Reactie CTIVD en TIB

op het concept wetsvoorstel Wet ter bescherming nationale veiligheid door inlichtingen- en veiligheidsdiensten (Wbnv) (consultatieversie 28 augustus 2026)

4 september 2026

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Toetsingscommissie Inzet Bevoegdheden

REACTIE CTIVD EN TIB

op het concept wetsvoorstel Wet ter bescherming nationale veiligheid door inlichtingen- en veiligheidsdiensten (Wbnv) (consultatieversie 28 augustus 2026)

Inhoudsopgave

REACTIE CTIVD EN TIB

op het concept wetsvoorstel Wet ter bescherming nationale veiligheid door inlichtingen- en veiligheidsdiensten (Wbnv) (consultatieversie 28 augustus 2026)

1. Hoofdboodschap

Essentie: Wetsvoorstel niet in balans: bevoegdheden uitgebreid, waarborgen verminderd

Het voorstel voor de nieuwe *Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten* is niet in balans: de diensten krijgen veel nieuwe bevoegdheden en meer ruimte om (persoons)gegevens te verzamelen en verder te verwerken. Tegelijkertijd worden voorwaarden die het handelen van de diensten begrenzen en onafhankelijke toetsing en toezicht verminderd. Dit vergroot het risico op onrechtmatigheden. Uitbreiding van bevoegdheden van de diensten en democratische rechtsstatelijke waarborgen zijn communicerende vaten: ze moeten gelijke tred met elkaar houden om fundamentele rechten van personen effectief te beschermen. Daarvan is nu geen sprake.

Juiste balans tussen bevoegdheden en waarborgen essentieel

De CTIVD en de TIB zien dat de geopolitieke situatie ingrijpend is veranderd en dat Nederland met toenemende en ernstige dreigingen wordt geconfronteerd. Deze dreigingen richten zich niet alleen tegen onze nationale veiligheid maar ook tegen onze democratische rechtsstaat en de fundamentele waarden waarop deze berust. Juist wanneer deze dreigingen toenemen, mogen we niet uit het oog verliezen wat we willen beschermen: niet alleen de nationale veiligheid, maar ook onze democratische rechtsstaat. Het doel van sterke en goed toegeruste inlichtingen- en veiligheidsdiensten is immers onze vrije en democratische samenleving te beschermen. Dat uitgangspunt is van bijzonder belang bij de herziening van de wet.

CTIVD en TIB

De CTIVD houdt onafhankelijk toezicht op de rechtmatigheid van het handelen van de AIVD en de MIVD en behandelt klachten over de diensten. Zij bewaakt de balans tussen nationale veiligheid en fundamentele rechten.

De TIB toetst vooraf of de toestemming voor de inzet van een aantal bijzondere bevoegdheden door de AIVD en de MIVD rechtmatig is. Het oordeel van de TIB is bindend.

Het wettelijk kader waarbinnen de AIVD en de MIVD hun taken uitvoeren en de bevoegdheden die hen daarbij worden toegekend, moet in dit licht voldoen aan de democratische en rechtsstatelijke waarden die Nederland wil beschermen. Dat vereist dat de wet niet alleen bepaalt welke bevoegdheden de diensten nodig hebben om dreigingen het hoofd te bieden, maar ook zorgvuldig afbakent binnen welke democratische en rechtsstatelijke grenzen die bevoegdheden worden uitgeoefend en hoe toezicht wordt gehouden op de naleving daarvan. Die waarborgen zijn cruciaal voor verantwoording

en democratische controle en beschermen personen tegen bedoeld of onbedoeld onrechtmatig of disproportioneel gebruik van de vergaande bevoegdheden van de diensten. Zoals het Europees Hof voor de Rechten van de Mens (EHRM) overwoog: *"In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse."*

Deze waarborgen zijn bovendien essentieel voor het maatschappelijk vertrouwen in de diensten. Juist omdat hun werk grotendeels in het geheim plaatsvindt, moeten zij het mogelijk maken de diensten en de verantwoordelijke ministers effectief te controleren en ter verantwoording te roepen; daarmee vormen zij een belangrijke voorwaarde voor de maatschappelijke legitimiteit en *license to operate* van de diensten.

Dat vraagt ook om een geïnformeerd politiek en maatschappelijk debat. Daarom vinden de CTIVD en de TIB het van belang het parlement en de samenleving, ook met deze inbreng in het consultatieproces van de wet, inzicht te geven in de voorgestelde uitbreidingen van bevoegdheden, de daaraan verbonden risico's en de gevolgen voor het democratische en rechtsstatelijke waarborgenstelsel. Beide colleges hebben overigens tijdens de voorbereiding van het wetsvoorstel ook al advies gegeven, waarbij enige voorstellen zijn overgenomen maar de meeste niet.

Waar mogelijk doen de CTIVD en de TIB in deze consultatie-reactie opnieuw voorstellen ter verbetering van de wet. Het is uiteindelijk uiteraard aan het parlement om te beoordelen welke nieuwe bevoegdheden noodzakelijk zijn en welke *checks and balances* daarbij vereist zijn. Voor die parlementaire afweging worden hieronder verhelderende informatie, adviezen, kritische vragen en afwegingskaders gegeven.

Beoordeling wetsvoorstel door CTIVD en TIB

De CTIVD en de TIB hebben het wetsvoorstel beoordeeld aan de hand van vier dimensies van het democratische en rechtsstatelijke waarborgenstelsel (zie separaat kader): internationale en wettelijke normstelling, politieke en democratische waarborgen, interne normering en controle en onafhankelijke externe toetsing en toezicht. De CTIVD en de TIB doen deze beoordeling vanuit hun onafhankelijke positie en bijzondere kennis van de praktijk van de inlichtingen- en veiligheidsdiensten.

Internationale en wettelijke normstelling. Op verschillende onderdelen roept het wetsvoorstel vragen op over de noodzakelijkheid, proportionaliteit en voorzienbaarheid van de voorgestelde bevoegdheden. Dit geldt bijvoorbeeld voor het brede opponentenregime, de ruime algemene bevoegdheden, de verwerving en verwerking van bulkgegevens, de verlenging van toestemmingsduur en bewaartermijnen, de verplichting tot afdracht van gegevens door vele private en (semi-) overheidspartijen, de brede bevoegdheid tot gebruik van OSINT, Artificial Intelligence (AI) en automatisering en de vermenging van het civiele en militaire inlichtingendomein. Ook wordt het uitgangspunt dat de zwaarte van de waarborgen moet aansluiten bij de daadwerkelijke inbreuk op fundamentele rechten niet consequent toegepast.

Politieke en democratische waarborgen. De nieuwe mandateringsregeling maakt het mogelijk dat toestemmingen voor vrijwel alle ingrijpende bevoegdheden en samenwerkingsrelaties lager binnen de diensten worden verleend. De minister heeft daarbij een eigenstandige controlerende taak ten aanzien van de diensten, die met de nieuwe wet kan worden gedelegeerd aan de dienstleiding zelf. Daarmee wordt een deel van de controle binnen de dienst belegd (de dienst controleert zichzelf) en neemt de actieve betrokkenheid en de controlemogelijkheden van de verantwoordelijke minister af. Ook dreigt de parlementaire controle op de minister daarmee meer op afstand te worden gezet. De beperkte mogelijkheid van de toezichthouder om het parlement rechtstreeks te informeren is

vanuit democratisch perspectief een tekortkoming. De vraag of de waarborgen voor de bijzondere voorziening voor de inzet van bijzondere bevoegdheden tegen leden van Eerste en Tweede Kamer, afdoende zijn, laten de CTIVD en de TIB aan het parlement.

De nieuwe wet roept in bredere zin de vraag op in hoeverre het wettelijke stelsel, ook onder uitzonderlijke of veranderende politieke omstandigheden, voldoende bescherming biedt tegen misbruik van de vergaande bevoegdheden van de diensten. De voorgestelde regeling van het staatsnoodrecht maakt deze vraag nog pregnanter.

Interne normering en controle. Op verschillende terreinen worden bevoegdheden verruimd zonder dat daar voldoende voorwaarden, beperkingen, procedures en interne controles tegenover staan. Dat geldt onder meer voor het brede opponentenregime, waarbij tegen personen die aan een aangewezen organisatie worden gelieerd gedurende langere tijd vergaande bevoegdheden kunnen worden ingezet, terwijl voor de verdere verwerking van aldus verworven gegevens onvoldoende specifieke waarborgen gelden. Ook bij gegevensverwerking ter ondersteuning van de taakuitvoering (TOTU), de verwerking van bulkgegevens, automatisering en samenwerking met externe partijen worden bevoegdheden verruimd zonder dat daar steeds passende interne waarborgen tegenover staan. Met de wettelijke verankering van de compliance- en auditfuncties is een eerste stap gezet, maar de wet dient ook vast te leggen dat die functies daadwerkelijk met impact, effectief en onafhankelijk hun rol binnen de diensten kunnen spelen. Zeker met een wet die de bevoegdheden van de diensten vergroot, is een versterking van deze interne waarborgen noodzakelijk.

Onafhankelijke externe toetsing en toezicht. Op belangrijke onderdelen wordt de voorafgaande onafhankelijke toetsing verminderd of naar een later moment in het besluitvormingsproces verschoven. Dat geldt onder meer voor het opponentenregime en voor hacken. Ook bij nieuwe en verruimde vormen van samenwerking en gegevensverstrekking ontbreekt externe toetsing of bindend toezicht. Tegelijkertijd wordt het nieuwe College Toetsing en Toezicht op verschillende punten beperkt in zijn functioneren, onder meer door een beperkte mogelijkheid tot bindende beslissingen, onvoldoende mogelijkheden voor een geïntegreerde en dynamische werkwijze en onvoldoende wettelijk verzekerde personele en financiële middelen.

Conclusie

De afzonderlijke wijzigingen moeten niet alleen op zichzelf worden beoordeeld. In hun onderlinge samenhang en cumulatieve effect ontstaat het volgende beeld: op belangrijke terreinen worden de bevoegdheden en mogelijkheden van de diensten uitgebreid, terwijl democratische en rechtsstatelijke waarborgen worden verminderd. Dit leidt er naar het oordeel van de CTIVD en de TIB toe dat de nieuwe wet niet in balans is, zowel op onderdelen als geheel.

Het stelsel van democratische en rechtsstatelijke waarborgen als beoordelingskader voor het wetsvoorstel

De democratische en rechtsstatelijke waarborgen rond de inlichtingen- en veiligheidsdiensten zijn essentieel voor een zorgvuldige inzet van hun vergaande bevoegdheden en voor het maatschappelijk vertrouwen in de diensten. Burgers moeten erop kunnen vertrouwen dat de inzet van deze bevoegdheden niet verder gaat dan noodzakelijk is en dat zij zoveel mogelijk worden beschermd tegen misbruik en tegen onbedoeld of disproportioneel handelen.

Tegelijkertijd moeten deze waarborgen het, ondanks het geheime karakter van het werk van de diensten, mogelijk maken om de diensten en de verantwoordelijke ministers ter verantwoording te roepen en hun handelen effectief te controleren. Zij vormen daarmee een belangrijke voorwaarde voor de maatschappelijke legitimiteit en het draagvlak – de *license to operate* – van de diensten.

Een democratische rechtsstaat kent daarbij geen enkele afzonderlijke waarborg die op zichzelf voldoende bescherming biedt. Het gaat om een samenhangend stelsel waarin verschillende vormen van normstelling, verantwoordelijkheid, interne beheersing en onafhankelijke controle elkaar aanvullen. Voor de beoordeling van het wetsvoorstel onderscheiden de CTIVD en de TIB de volgende vier samenhangende pijlers.

A. Internationale en wettelijke normstelling

De wetgeving over de inlichtingen- en veiligheidsdiensten moet passen binnen de internationale en constitutionele normen waaraan Nederland is gebonden. Mensenrechtenverdragen, relevante jurisprudentie en constitutionele grondrechten en beginselen stellen eisen aan de wijze waarop de wetgever bevoegdheden en het toezicht daarop vormgeeft. Daaruit volgen onder meer eisen van legaliteit, kenbaarheid, voorzienbaarheid, noodzakelijkheid en proportionaliteit.

Deze hogere normen vormen het uitgangspunt voor de beoordeling van de vraag welke bevoegdheden in een democratische rechtsstaat aan de diensten kunnen worden toegekend en welke waarborgen daarbij noodzakelijk zijn. De volgende drie dimensies komen hier mede uit voort.

B. Politieke en democratische waarborgen

De verantwoordelijke ministers moeten daadwerkelijk verantwoordelijk en aanspreekbaar blijven voor het handelen van de diensten. Dat vereist voldoende betrokkenheid bij ingrijpende besluiten en voldoende informatie om de ministeriële verantwoordelijkheid ook daadwerkelijk te kunnen dragen.

Daarnaast moet het parlement zijn democratische controlerende taak effectief kunnen uitoefenen. Daarbij is van belang dat het parlement binnen de grenzen van noodzakelijke geheimhouding voldoende wordt geïnformeerd en dat onafhankelijk toezicht niet onnodig afhankelijk is van de betrokken ministers bij de communicatie met het parlement. Ook de mogelijkheid om in uitzonderlijke omstandigheden van het reguliere wettelijke kader af te wijken, bijvoorbeeld door de inzet van staatsnoodrecht, raakt rechtstreeks aan deze democratische waarborgen.

C. Interne normering, regels en controle
De hogere democratische en rechtsstatelijke normen moeten worden vertaald in concrete beleidsregels en procedures.

Daartoe behoren onder meer regels over autorisatie en besluitvorming, de toepassing van bevoegdheden, gegevensverwerking, bewaring en vernietiging van gegevens, verslaglegging en *logging*, interne juridische advisering, werkcultuur en functiescheiding. Ook een goed gepositioneerde compliance- en auditfunctie zijn essentieel. Deze interne normering en controle vormen een belangrijke verdedigingslinie tegen onrechtmatig of disproportioneel handelen. Zij moeten niet worden gezien als een administratieve last, maar als een wezenlijk onderdeel van de rechtsstatelijke uitoefening van de taken van de diensten (hetgeen ook geldt voor externe toetsing en toezicht).

D. Onafhankelijke externe toetsing en toezicht
Juist omdat inlichtingen- en veiligheidsdiensten grotendeels in het geheim opereren en hun handelen daardoor slechts beperkt zichtbaar is voor betrokken burgers, publiek en politiek, heeft onafhankelijke externe toetsing en toezicht in dit domein een bijzonder gewicht.

De wet moet daarom voorzien in een toezichts- en toetsingsstelsel dat voldoende onafhankelijk, deskundig, flexibel en daadkrachtig is en dat de relevante onderdelen van het handelen van de diensten effectief kan bestrijken. Daarbij is van belang dat toetsing vooraf en toezicht tijdens en achteraf op samenhangende wijze kunnen functioneren en dat de toezichthouder over voldoende bevoegdheden, informatie, capaciteit en middelen (personeel en financieel) beschikt.

Effectief extern toezicht vormt daarmee de onafhankelijke controle op de vraag of de diensten en de verantwoordelijke ministers handelen binnen de normen en regels die in een democratische rechtsstaat aan geheime bevoegdheidsuitoefening worden gesteld.

Opbouw consultatiereactie

1. Het handelen van de diensten laat zich grofweg onderscheiden in drie fases. Die fases komen in een versimpelde weergave op het volgende neer:
   1) Allereerst de gegevensverzameling, waarbij bevoegdheden worden ingezet.
   2) Vervolgens de verdere gegevensverwerking, waarin de analyse en verrijking van die gegevens plaatsvindt.
   3) En vervolgens de verstrekking van gegevens aan enerzijds afnemers, dan wel aan andere partijen, waarbij de verstrekking van gegevens op zichzelf weer ten dienste kan staan van de gegevensverzameling. Ook kan in deze fase op andere manieren worden samengewerkt met externe partijen waarbij gegevens worden gedeeld.
2. In de voorstellen die zien op deze drie fases signaleren de CTIVD en de TIB een verruiming van mogelijkheden voor de diensten zonder dat daar passende waarborgen tegenover staan.
3. Hieronder zullen wij dit aan de hand van deze drie fases toelichten. We starten met opmerkingen over de gegevensverzameling. Vervolgens behandelen we opmerkingen die zien op de gegevensverwerking en gaan we in op de gegevensverstrekking en samenwerking. Daarna beoordelen wij het voorgestelde stelsel van toets, toezicht, klacht en beroep. Tot slot laten wij ons nog uit over het staatsnoodrecht en het overgangsrecht.
4. Onze opmerkingen moeten daarbij ook in onderlinge samenhang worden bezien. De optelsom van constateringen leidt er naar het oordeel van de CTIVD en de TIB toe dat het wetsvoorstel niet in balans is, zowel op onderdelen als het geheel.

A Stelsel van verwerving

2. Opponenten-toestemmingsprocedure

Essentie:

De 'opponenten-toestemmingsprocedure' is een grofmazig instrument dat geen recht doet aan de nuances die een noodzakelijkheids- en proportionaliteitstoets bij de inzet van bevoegdheden vraagt. De groep van organisaties waarop het regime van toepassing kan zijn, is zeer ruim geformuleerd. Bovendien is de impact van een aanwijzing bijzonder groot. Als een organisatie als opponent is gekwalificeerd en individuele personen op enige wijze zijn gelieerd aan deze organisatie, dan mogen de diensten zonder voorafgaande onafhankelijke toetsing voor maximaal een jaar nagenoeg alle (bijzondere) bevoegdheden tegen hen inzetten. De CTIVD en de TIB achten een afweging op organisatieniveau, zoals nu in het opponentenregime wordt voorgesteld, niet in overeenstemming met de normen van het Europees Verdrag voor de Rechten van de Mens. Daarom is een heroverweging van de invoering van dit regime op zijn plaats.

Nadere toelichting

5. Het wetsvoorstel introduceert een regime dat wordt aangeduid als de opponenten-toestemmingsprocedure. Dit regime geldt naast het reguliere regime. In het reguliere systeem krijgen de diensten aanzienlijk meer bevoegdheden en ruimte om gegevens te verzamelen, terwijl waarborgen aanmerkelijk worden beperkt. In dit nieuwe opponentenregime worden de wettelijke mogelijkheden voor de diensten nog verder verruimd.
6. Het opponentenregime stelt regels voor het doen van onderzoek naar organisaties met offensieve doelen gericht op Nederland. Het gaat dan om het aanwijzen van civiele organisaties (art. 55 lid 1 en 2) of militaire organisaties (art. 56) die horen bij een land dat doelen nastreeft of activiteiten onderneemt die gericht zijn tegen Nederland of tegen Nederlandse belangen. Daaronder vallen ook Nederlandse bondgenoten. Ook kan het gaan om terroristische organisaties die niet horen bij een land (niet-statelijke actor) (art. 55 lid 3). Voor onderzoek van de diensten naar deze organisaties of naar personen die verbonden zijn aan deze organisaties (zogenaamde gelieerde personen) geldt een lichtere toestemmingsprocedure dan voor andere onderzoeken waarop het reguliere regime van toepassing is. De afweging waarop de toestemming berust, is beperkter van omvang en de toestemming hoeft minder vaak te worden herhaald.
7. In het reguliere regime geldt dat voorafgaand aan elke inzet van een bevoegdheid de noodzaak, proportionaliteit en subsidiariteit moeten worden afgewogen en gemotiveerd. Dit betekent bijvoorbeeld dat voordat de diensten de internetaansluiting van een persoon kunnen tappen eerst moet worden beoordeeld of dit noodzakelijk is, of de inbreuk op de levenssfeer van de persoon in kwestie in verhouding staat tot het doel van die inbreuk en of er geen andere, lichtere middelen zijn om de beoogde inlichtingen te verkrijgen. Deze waarborgen, die gestoeld zijn op het Europees Verdrag voor de Rechten van de Mens, zijn erop gericht te voorkomen dat diensten hun verstrekkende bevoegdheden te lichtvaardig inzetten. Voor een aantal bijzondere bevoegdheden geldt aanvullend dat deze van tevoren moeten worden voorgelegd ter toetsing aan het nieuwe College van Toetsing en Toezicht (CTT) (art. 47 sub a-m).
8. In het opponentenregime krijgen deze waarborgen een andere invulling. Als een organisatie als opponent is gekwalificeerd en personen zijn gelieerd aan deze organisaties zijn de noodzaak en proportionaliteit van de inzet van bevoegdheden een gegeven. Dit betekent dat bij de inzet van een (bijzondere) bevoegdheid tegenover een persoon of organisatie die onder het opponentenregime valt niet meer per inzet wordt getoetst of die inzet noodzakelijk, proportioneel en subsidiair is. Als een persoon of organisatie op de lijst staat, kunnen bijna alle bijzondere bevoegdheden gedurende een jaar tegen hem worden ingezet zonder dat een voorafgaande externe toets per bevoegdheid plaatsvindt.

9. De betrokken ministers (de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie) zijn samen bevoegd om een organisatie aan te wijzen waarop het opponentenregime van toepassing is. Het besluit om een organisatie aan te wijzen moet wel worden voorgelegd aan het CTT. Als de diensten bevoegdheden willen inzetten tegenover een persoon die betrokken zou zijn bij een organisatie die op de lijst staat, moeten zij motiveren waaruit die betrokkenheid bestaat. Het CTT kan vervolgens bindend toezicht uitoefenen op het liëren van die persoon aan de betreffende organisatie (art. 58 lid 4 jo. art. 188 lid 1 onder b). Deze bevoegdheid voor het CTT is in het wetsvoorstel toegevoegd na input van de CTIVD en de TIB. Wij blijven echter van mening dat deze waarborgen onvoldoende zijn. Zowel de toetsing van het aanwijzingsbesluit als het bindend toezicht op het liëren van personen door het CTT is beperkt. In de toetsing mag het CTT alleen beoordelen of de aanwijzing van de organisatie in overeenstemming is met de in art. 55 neergelegde eisen (art. 57). Omdat de wet ruim is geformuleerd, zal een aanwijzing al snel aan de wettelijke eisen voldoen. Het bindend toezicht beperkt zich tot de vraag of een persoon op enigerlei wijze met een aangewezen organisatie kan worden verbonden
10. Volgens de memorie van toelichting is de groep van organisaties waarvoor de opponenten-toestemmingsprocedure geldt wettelijk afgebakend en gaat het om de volgende vier groepen: 1) organisaties van landen die doelen nastreven of activiteiten verrichten gericht tegen Nederland of de Nederlandse belangen, 2) terroristische organisaties die op een EU-terrorismelijst zijn geplaatst, 3) in de wet genoemde militaire organisaties, en 4) daarmee gelijk te stellen paramilitaire organisaties of groeperingen die in staat zijn duurzame gewapende strijd te leveren.
11. De CTIVD en de TIB constateren, onder verwijzing naar met name 1) en 4), dat de groep van organisaties waarvoor het regime kan gaan gelden juist zeer ruim is geformuleerd. Bovendien is de impact van een aanwijzing zeer groot. De noodzaak om een aantal bijzondere bevoegdheden tegenover een persoon in te zetten wordt al geacht aanwezig te zijn zodra die persoon op enige wijze verbonden is aan een aangewezen organisatie. Oftewel: als de persoon verbonden kan worden aan zo'n organisatie dan is er ook altijd een reden om verschillende bevoegdheden op hem of haar in te zetten, zo wordt in de toelichting geredeneerd. Het maakt daarbij geen verschil op welke manier die persoon verbonden is of welke functie de persoon binnen die organisatie bekleedt. Daarbij komt dat door de huidige formulering een groot deel van de inwoners van een land, of personen behorend tot de diaspora van dat land, onder de werking van het regime kunnen komen, zeker als dat land een *'whole of society-approach*' kent. Ten aanzien van de onder 2) genoemde terroristische organisaties signaleren de CTIVD en de TIB de wereldwijde tendens dat terrorismewetgeving wordt opgerekt en dat ook dit begrip én aangewezen organisaties kunnen uitdijen. Daarnaast is ook bij de aanwijzing van militaire organisaties sprake van een zeer ruime definitie, waardoor ook organisaties daaronder vallen die (al dan niet bewust) wezenlijke werkzaamheden verrichten voor een uiteindelijk militair doel. De term 'wezenlijk' is onduidelijk en heeft het risico in zich van een glijdende schaal, omdat veel organisaties daaronder kunnen worden geschaard.
12. Als laatste merken de CTIVD en de TIB op dat de 'stomme tap', oftewel de *real time* verzameling van verkeers- en locatiegegevens (voorgesteld art. 89), niet wordt uitgezonderd van gebruik binnen het opponentenregime (voorgesteld art. 58 lid 1). Op grond van jurisprudentie van het Hof van Justitie van de Europese Unie (HvJ EU) is een bindende ex ante-toets voor de inzet van deze bevoegdheid noodzakelijk. Een bindende toets op de aanwijzing van de organisatie binnen het opponentenregime en bindend toezicht op het liëren van personen aan zo'n organisatie compenseren niet voor het gebrek aan individuele toetsing op de inzet van de bevoegdheid. Hoe de bindende toets en het bindend toezicht nu zijn vormgegeven, is er namelijk geen inhoudelijke toets op de noodzaak, proportionaliteit en subsidiariteit van de inzet van een specifieke bevoegdheid.
13. Op grond van het voorgaande menen wij dat een heroverweging van de introductie van het opponenten-regime in het wetsvoorstel op zijn plaats is. We vragen aandacht voor de vermeende noodzaak voor het inrichten van dit nieuwe regime. Voor welk (uitvoerings)probleem is dit regime de oplossing, en zijn er geen andere, lichtere methodes om dat doel te bereiken?

3. Mandatering

14. De CTIVD en de TIB spreken hun zorgen uit over de zeer ruime mogelijkheid tot mandatering en vervolgens ondermandatering van toestemming voor de inzet van (bijzondere) bevoegdheden door de diensten. Het is de minister toegestaan om in vrijwel alle gevallen waarin de wet vereist dat hij toestemming verleent voor een activiteit of uitoefening van een bevoegdheid de besluitvorming kan overdragen naar de dienstleiding (art. 27). Ondermandatering betekent dat de minister zelfs kan toestaan dat de besluitvorming binnen de dienst naar een lager niveau kan worden verschoven (art. 31). De minister kan hiertoe een openbare mandaatregeling opstellen of in individuele gevallen mandaat verlenen (art. 28). De minister kan dus ook bepalen dat (in welke gevallen) ondermandaat mogelijk is (art. 31 lid 1). In de gevallen dat de wet bepaalt dat het diensthoofd toestemming kan verlenen, is hij gemachtigd om mandaat voor besluitvorming te verlenen aan iemand binnen de dienst die onder zijn verantwoordelijkheid werkzaam is (art. 31 lid 2).
15. De mogelijkheid tot mandaat en ondermandaat is heel ruim gesteld. Het wetsvoorstel benoemt alleen enkele gevallen waarin het de minister *niet* is toegestaan mandaat te verlenen (art. 27 lid 2 en 3).[1] Voor veel inbreukmakende bevoegdheden is (onder)mandatering opengesteld, zoals alle bijzondere operationele bevoegdheden, het aangaan van samenwerkingsrelaties, automatisering, etc. Op pagina 48 van de memorie van toelichting merkt de regering op dat zij het feit dat de aanwijzingsbevoegdheid in het opponenten-toestemmingsregime niet kan worden gemandateerd als een belangrijke waarborg ziet. Het feit dat de aanwijzing van een organisatie slechts door de ministers kan plaatsvinden, is een uitdrukking van het gewicht van dit besluit. Wij zijn het met de regering eens dat dit een belangrijke waarborg is en daarom is het zorgelijk dat deze belangrijke waarborg in andere gevallen waarbij sprake is van vergaande inbreuken op fundamentele rechten niet wordt doorgevoerd.
16. Ondanks het feit dat elk handelen van de diensten onder ministeriële verantwoordelijkheid plaatsvindt, is het feit dat de betrokken minister niet actief betrokken is bij besluitvorming over de inzet van bijzondere bevoegdheden of samenwerking met militaire, buitenlandse en private partijen een belangrijke waarborg minder. Het tegenargument dat de mogelijkheid van mandaat een belangrijke waarborg tegen autocratische leiders vormt, nu de toestemming in veel gevallen niet meer bij de minister(s) ligt maar juist bij de diensten, vinden wij niet overtuigend. De wet bepaalt immers dat de beslissing over (onder)mandaatverlening door de ministers moet worden genomen door middel van het opstellen van een mandateringsbesluit (art. 28), die te allen tijde door hen kan worden aangepast of ingetrokken (art. 30) en zelfs bij mandaatverlening de minister(s) zelf bevoegd blijft om de toestemmingsverlening uit te voeren (art. 27 lid 5). Ons punt is dat de wet een te ruime mogelijkheid biedt tot mandaatverlening.
17. De ruime mandateringsmogelijkheid betekent dat sommige beslissingen door het diensthoofd zelfs tot een teamhoofd ondergemandateerd kunnen worden. De besluitvorming tot inzet van bijzondere bevoegdheden vindt in zo'n geval zeer dicht op het operationele proces plaats. Hoe dichter de besluitvorming plaatsvindt in de operatie, hoe minder de inzet van de bevoegdheid objectief en kritisch wordt bekeken. Hierdoor wordt ook het gat tussen besluitvorming en verantwoordelijke voor die besluitvorming zeer groot.

---

1 Dit betreft in lid 2: opstellen van de Geïntegreerde Aanwijzing (art. 7), aanwijzen van civiele organisaties met offensieve doelen en activiteiten in het opponentenregime (art. 55 lid 1), aanwijzen van militaire organisaties met offensieve doelen en activiteiten (art. 56 lid 1), verstrekken gegevens wegens zwaarwegende noodzaak aan buitenlandse dienst, entiteit of samenwerkingsverband (art. 141 lid 2), staatsnoodrecht (hfd 11). Nieuw toegevoegd ten opzichte van eerdere versies is art. 141. En in lid 3 zijn uitgesloten: verzoeken voor de inzet van operationele bevoegdheden tegen bijzondere categorieën van personen (o.g.v. art. 43 lid 1) of in tweede instantie aan de Raad van State als de rechtbank heeft afgewezen (o.g.v. art. 217 lid 1); instellen beroep tegen bindende oordelen van afdeling toetsing CTT, afdeling toezicht CTT of afdeling klacht CTT (o.g.v. art. 207 lid 1); verzoeken om voorlopige voorziening (o.g.v. art. 213 lid 1).

18. Een gevolg van dit wetsvoorstel is dat bijvoorbeeld de meest ingrijpende strategische hackoperaties kunnen worden uitgevoerd op basis van toestemming die via ondermandaat is verleend. Een voorafgaande, bindende toets ontbreekt. Het is bepaald zorgelijk dat dit wetsvoorstel ertoe leidt dat dergelijke hackoperaties kunnen plaatsvinden zonder een onafhankelijke voorafgaande toetsing door het CTT en daarnaast buiten het zicht van de verantwoordelijk minister. Ook voor vergaande samenwerkingen met buitenlandse entiteiten (ruimer dan buitenlandse inlichtingen- en veiligheidsdiensten) en private partijen waarbij gegevens uit het inlichtingen- en veiligheidsdomein gaan, is volgens het wetsvoorstel toegestaan dat de minister zijn toestemmingsbevoegdheid overdraagt aan de dienstleiding of zelfs lager in de organisatie belegd.
19. De inbreng van de CTIVD en de TIB in het voorbereidingstraject heeft ertoe geleid dat in de wet is geregeld dat het diensthoofd geen ondermandaat mag verlenen voor de inzet van bijzondere bevoegdheden onder het opponentenregime die in de reguliere toestemmingsprocedure ex ante getoetst zouden worden. Dit staat in art. 58 lid 3 en vormt een uitzondering op art. 31 lid 2 op grond waarvan het diensthoofd zijn toestemmingsbevoegdheid mag mandateren aan een lager geplaatste medewerker. Voor het overige heeft onze inbreng niet geleid tot andere beperkingen van mandaat of ondermandaat.
20. De CTIVD en de TIB vinden het belangrijk dat in de wet een ruimere grens wordt gesteld aan de mogelijkheid tot mandatering dan wel ondermandatering, bijvoorbeeld door in het wetsvoorstel meer ingrijpende bevoegdheden of samenwerkingen uit te zonderen van de mogelijkheid tot mandaat door de minister(s).

4. Algemene bevoegdheden

21. Om hun taken uit te kunnen voeren beschikken de diensten over wettelijke bevoegdheden. Deze bevoegdheden zijn onderverdeeld in algemene en bijzondere bevoegdheden; een systematiek die in de Wiv 2017 ook wordt gehanteerd. De CTIVD en de TIB hebben kritische kanttekeningen bij de wijze waarop een aantal bevoegdheden is gecategoriseerd, de invulling die daaraan is gegeven en de reikwijdte van de toepassing die daarmee ontstaat.
22. Het verschil tussen algemene en bijzondere bevoegdheden is dat voor de inzet van bijzondere bevoegdheden meer waarborgen gelden. Dat is in de Wiv 2017 zo en dat verandert niet met dit wetsvoorstel. Bijzondere bevoegdheden worden namelijk geacht meer inbreuk te maken op de persoonlijke levenssfeer van betrokkenen en zijn daarom aan strengere wettelijke eisen gebonden. De ervaring leert dat algemene bevoegdheden in de praktijk helemaal niet minder ingrijpend hoeven te zijn dan bijzondere bevoegdheden. Deze categorisering rechtvaardigt in die gevallen niet dat de voorwaarden en waarborgen die horen bij de inzet van algemene bevoegdheden worden afgeschaft, afgeschaald of beperkt. De met algemene bevoegdheden verkregen informatie komt beschikbaar voor alle taken van de diensten. Veel dienstmedewerkers hebben toegang tot die gegevens, waardoor de inbreuk op de persoonlijke levenssfeer van personen wier persoonsgegevens met algemene bevoegdheden zijn verworven groter is.
23. Een aantal (elementen van) huidige bijzondere bevoegdheden is in het wetsvoorstel als algemene bevoegdheid aangemerkt. Deze verschuiving van bijzondere bevoegdheid naar algemene bevoegdheid brengt een vermindering van waarborgen met zich mee. Dit geldt bijvoorbeeld voor het inzetten van technische middelen (voorheen onderdeel van een specifieke bijzondere bevoegdheid, zoals hacken en tappen), het aannemen van een identiteit of hoedanigheid (voorheen onderdeel van de agentenbevoegdheid) en kortstondige observatie, een bevoegdheid die nu onder de bredere observatie bevoegdheid van art. 40 Wiv 2017 valt en daarmee een bijzondere bevoegdheid is. Kortstondig observeren wordt nu aangemerkt als een algemene bevoegdheid waardoor dus de waarborgen die gelden voor bijzondere bevoegdheden niet meer van toepassing zijn. Hierbij komt dat niet helder is afgebakend wanneer sprake is van kortstondige observatie. In de memorie van toelichting wordt onvoldoende aandacht besteed aan de inbreuk op de persoonlijke levenssfeer en de vermindering van waarborgen die deze keuze van het verschuiven van bijzondere naar algemene bevoegdheden met zich meebrengt.

4.1 OSINT-bevoegdheid

24. Ook is een ruime reikwijdte van bestaande algemene bevoegdheden in dit voorstel vastgelegd, zoals de OSINT- en de informantenbevoegdheid. De OSINT (Open Source Intelligence)-bevoegdheid houdt in dat de diensten bevoegd zijn tot het verzamelen van gegevens uit *"voor eenieder toegankelijke informatiebronnen"*. De aard en omvang van de informatie die hieronder valt heeft de laatste jaren een grote vlucht genomen, waardoor deze niet meer de lading dekt die men in het maatschappelijk verkeer hieraan zou geven. De omvang van de bevoegdheid is niet (meer) voorzienbaar voor de burger.
25. De CTIVD en de TIB zijn zeer kritisch op de toelichting op dit artikel. De memorie van toelichting schetst het beeld dat met de OSINT-bevoegdheid slechts een geringe inbreuk op fundamentele rechten wordt gemaakt. De CTIVD en de TIB zien dat anders. Er is steeds meer informatie over personen beschikbaar op het internet. Sommige gegevens zijn door personen zelf online gezet met het doel om die informatie publiek te maken. Steeds meer informatie wordt echter buiten de invloedssfeer van de betreffende persoon om 'openbaar' gemaakt.[2] Denk aan advertentieprofielen,

2 Zie het recente toezichtrapport **nr. 84** (juli 2026) van de CTIVD over de verwerking van bulkdatasets door de AIVD en de MIVD.

informatie uit cookies en gestolen en gelekte datasets (zie CTIVD-rapport **nr. 74** (feb. 2022) over automated OSINT).[3] Daarnaast kan het gaan om gegevens die ooit vrijwillig online zijn gezet, maar die de persoon later doelbewust offline heeft geprobeerd te halen. Ook deze gegevens zijn vaak nog terug te vinden. Bij deze gegevens kan het bijvoorbeeld gaan om locatiegegevens en gegevens over het mobiele apparaat van een persoon. Al deze gegevens kunnen door de diensten worden gecombineerd, waardoor zij een zeer volledig beeld van een persoon kunnen krijgen. Hierdoor kan een grote inbreuk op de persoonlijke levenssfeer van personen worden gemaakt. De memorie van toelichting miskent dit risico.

26. Zo blijkt uit de memorie van toelichting dat onder de OSINT-bevoegdheid ook bronnen vallen waarvoor technische kennis of financiële middelen nodig zijn om toegang te hebben. Ook gegevens(sets) die op het *dark web* staan, vallen onder de OSINT-bevoegdheid. Afgezien van het feit dat er vraagtekens te zetten zijn bij de stelling dat financiële middelen in potentie voor iedereen beschikbaar zijn, is hiervan het gevolg dat de diensten via de OSINT-bevoegdheid kunnen betalen voor het verkrijgen van gehackte databestanden die op het *dark web* worden aangeboden. Hiermee dragen de diensten bij aan het verdienmodel van de hackersgroepen die betrokken zijn bij grootschalige datalekken. De CTIVD en de TIB laten de discussie over de wenselijkheid daarvan graag aan het parlement over, maar wijzen er wel op dat het niet passend is om een dergelijke verwerving aan te duiden als algemene bevoegdheid gelet op de grote inbreuk die dit voor betrokkenen van wie de gegevens zich in die databestanden bevinden met zich meebrengt. Een dergelijke ingrijpende bevoegdheid zou in de visie van de CTIVD en de TIB met meer waarborgen moeten zijn omgeven dan nu voor algemene bevoegdheden is ingericht.
27. Ook speelt hierbij dat het wetsvoorstel OSINT als één bevoegdheid aanmerkt, terwijl deze bevoegdheid een veelheid aan verschijningsvormen kent. De memorie van toelichting licht bijvoorbeeld op pagina 73 toe dat de inzet van de OSINT-bevoegdheid kan worden gebruikt bij het verkennen van geautomatiseerde werken, dat onderdeel is van de bijzondere bevoegdheid hacken.[4] Het is daarnaast een verschil of een enkele zoekslag wordt gedaan in gegevens van de Kamer van Koophandel of dat door middel van specialistische software of webapplicaties meerdere (wellicht honderden) grote databestanden worden doorzocht en gecombineerd (*automated OSINT*). Die laatste vorm van open bronnenonderzoek is daarmee niet te vergelijken met een meer simpele naslag die van oudsher onder deze bevoegdheid werd geschaard. De CTIVD heeft in haar toezichtrapport **nr. 74** (feb. 2022) aandacht besteed aan de bevoegdheid van *automated OSINT* en de risico's die daarmee gepaard kunnen gaan. Het is, gelet op de grote verscheidenheid aan vormen van open bronnenonderzoek passender als deze bevoegdheid niet geheel als algemene bevoegdheid wordt aangemerkt. Voor meer uitgebreidere – en daarmee meer inbreukmakende – varianten is een categorisering als bijzondere bevoegdheid passender. Hierdoor worden die varianten omgeven met meer passende waarborgen dan nu in het voorstel is geregeld.

---

3 Voor nadere uitleg zie het rapport 'Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?', Charlotte Dietrich & Thorsten Wetzling, 17 november 2022.

4 Memorie van toelichting, p. 73: "Een verkenning van een geautomatiseerd werk vindt plaats om de capaciteit en de technische haalbaarheid te beoordelen door een beeld te verkrijgen van de eigenschappen van een geautomatiseerd werk, zoals de geïnstalleerde software, de aanwezige netwerkverbindingen en de hardware. Met behulp van deze informatie kunnen de diensten efficiënter en zorgvuldiger overgaan tot het binnendringen in een geautomatiseerd werk. De verkenning wordt ook gebruikt om een actueel beeld te krijgen van het digitale landschap van het geautomatiseerde werk. Dat gaat er dan om met wat voor andere geautomatiseerde werken wordt gecommuniceerd en waarvoor deze dienen. Op die manier kan worden geduid of het geautomatiseerde werk relevantie heeft voor het onderzoek van de dienst. Hiervoor gebruikt de dienst toepassingen, zoals IP- en poortscansoftware en registratiemiddelen, waarmee inzicht kan worden verkregen van het communicatienetwerk van een geautomatiseerd werk. Een voorbeeld zou kunnen zijn dat hiermee kan worden nagegaan of een desktop pc van een relevante buitenlandse actor, onderdeel uitmaakt van een militaire radarinstallatie van een straaljager die communiceert met een grondstation. De kenmerken die in deze fase door de diensten worden vastgelegd zullen veelal bestaan uit vrijelijk te onderkennen gegevens over technische eigenschappen, zoals het IP-adres, de beschikbaarheid van poorten en de functie van het werk, zoals mailserver of router. Voor deze vrijelijk te onderkennen gegevens kan art. 55 (voor eenieder toegankelijke informatiebronnen) worden gebruikt."

4.2 Informantenbevoegdheid

28. Ook de informantenbevoegdheid (voorgesteld art. 63) heeft een ruime invulling. Dat komt omdat de diensten met deze bevoegdheid ook geautomatiseerd (bulk)datasets van Nederlandse medeoverheden kunnen verwerven. Het gaat dan bijvoorbeeld over passagiersgegevens van vliegtuigmaatschappijen, gegevens uit het register van de Kamer van Koophandel en gegevens uit de Basisregistratie Personen. De Evaluatiecommissie Wiv 2017[5] heeft hierover geconstateerd dat bij het verwerven van bulkdata via de informantenbevoegdheid een gebrek aan voorzienbaarheid is. Zij beveelt aan om een eenduidige en voorzienbare grondslag voor het verwerven van bulkdata van Nederlandse medeoverheden te creëren. Dit komt ook ten goede aan de waarborgen behorende bij de verwerving van bulkdatasets. Het verwerven daarvan door middel van een bijzondere bevoegdheid, zoals de hackbevoegdheid, is met meer waarborgen omkleed. Dat verschil is wel te verklaren als er alleen wordt gekeken naar de inbreuk van de bevoegdheid. Het vragen van gegevens op basis van vrijwilligheid aan personen/organisaties (informantenbevoegdheid) is minder ingrijpend dan het ongezien inbreken in de systemen van personen of organisaties. Maar het verschil is niet goed te verklaren als wordt gekeken naar de aard en omvang van de gegevens. In beide gevallen wordt bulkdata verworven, wat betekent dat er inbreuk wordt gemaakt op de privacy van mensen die niet het onderwerp van onderzoek van de diensten zijn of zullen worden, aldus de Evaluatiecommissie Wiv 2017. De CTIVD en de TIB zijn het hiermee eens. Het geautomatiseerd verwerven van bulkdatasets van Nederlandse medeoverheden maakt een veel grotere inbreuk dan het “normaal” bevragen van een persoon als informant. Een eigen wettelijke grondslag met bijbehorende passende waarborgen voor het geautomatiseerd verwerven van bulkdatasets via Nederlandse medeoverheden is naar het oordeel van de CTIVD en de TIB gerechtvaardigd.

5 ECW-rapport, *Kamerstukken II* 2020/21, 88, bijlage 965058.

5. Bijzondere bevoegdheden

5.1 De hackbevoegdheid

29. De hackbevoegdheid is een van de bevoegdheden van de diensten die de meeste inbreuk maakt op fundamentele rechten, met name het recht op eerbiediging van de persoonlijke levenssfeer. De CTIVD en de TIB vinden dat een dergelijk vergaande inbreuk vooraf moet worden getoetst door een onafhankelijke instantie.
30. Tegenwoordig heeft vrijwel ieder persoon en iedere organisatie in Nederland en daarbuiten ten minste één 'geautomatiseerd werk' in bezit en gebruik. Denk aan een mobiele telefoon, laptop, wifi-netwerk en tablet, maar ook aan de server van 112, pacemakers en de besturing van (drink)watersystemen. Een groot deel van het (sociale) leven van personen is op de een of andere manier opgeslagen op deze apparaten. Daarnaast zijn bijna alle organisaties afhankelijk van geautomatiseerde werken voor het functioneren van hun systemen. Het inbreken in zo'n geautomatiseerd werk en het vervolgens uitwinnen van gegevens die daarop zijn opgeslagen maken daarom een grote inbreuk op de persoonlijke levenssfeer. Ook bestaat soms het (technische) risico dat er iets misgaat in de werking van een systeem. De ex ante-toets hierop zou wat de CTIVD en de TIB betreft moeten plaatsvinden vóór het binnendringen. Wij wijzen in dit verband ook op de jurisprudentie van het Hof van Justitie van de Europese Unie (HvJEU) dat een bindende ex ante-toets noodzakelijk acht voor de zogenoemde 'stomme tap', oftewel de toegang tot real time verkeers- en locatiegegevens. Dat is een minder inbreukmakende bevoegdheid van de diensten dan de hackbevoegdheid.
31. In de Wiv 2017 is de hackbevoegdheid geregeld in één artikel, namelijk art. 45 Wiv 2017. Het wetsvoorstel knipt deze bijzondere bevoegdheid op in drie wetsartikelen waarin bevoegdheden voor drie fases van de hackbevoegdheid worden gecreëerd. De eerste fase is het 'vooronderzoek', de tweede fase het 'positioneren en treffen van voorbereidingen in een binnengedrongen automatisch werk' en de laatste fase de 'uitwinning van een binnengedrongen geautomatiseerd werk'. De regering stelt dat de inbreuk in fase 1 en fase 2 relatief gering is. De echte inbreuk zit in de uitwinning van gegevens, aldus de regering. Daarom wordt voorgesteld dat er pas voor de uitwinning onder het reguliere regime – en dus niet onder het opponentenregime – een externe toets door het CTT noodzakelijk is. Dat fase 3 vaak de grootste inbreuk op de persoonlijke levenssfeer zal maken, neemt niet weg dat ook het binnendringen en positioneren een grote inbreuk maken. Daarnaast zijn er (technische) risico's verbonden aan het binnendringen en positioneren.
32. In de memorie van toelichting maakt de regering de analogie van het doorzoeken van een loods. De CTIVD en de TIB zijn van oordeel dat de analogie van het doorzoeken van een woning beter past bij de inbreuk die de hackbevoegdheid maakt. Mobiele telefoons geven immers zicht op een groot deel van het privéleven van een persoon. In de eerste fase wordt ingebroken in de woning, al dan niet geruisloos. In de tweede fase doorzoeken de diensten de woning voor relevante informatie en bekijken of het nut heeft om een verzoek in te dienen om gegevens mee te nemen. Tot slot wordt in fase 3 die relevante informatie meegenomen. Dit voorbeeld laat zien dat ook de eerste twee fases al een grote inbreuk maken op de persoonlijke levenssfeer van personen. Dit geldt des te meer voor het inzetten van de hackbevoegdheid tegen non-targets (d.w.z. niet zelf in onderzoek bij de dienst, maar wel noodzakelijk voor het onderzoek, bijvoorbeeld vanwege contact met target). Tegenover deze inbreuk moet in de visie van de CTIVD en de TIB in alle gevallen de waarborg van een ex ante-toets staan, zodat onafhankelijk wordt beoordeeld of de diensten wel mogen binnendringen.

33. Dat fases 1 en 2 geen onafhankelijke ex ante-toets kennen, brengt nog een groot risico met zich mee. Het is voorstelbaar dat het doel van het binnendringen niet het uitwinnen van dat geautomatiseerde werk is, maar dat het doel een digitale verstoringsactie is (voorgestelde art. 76 en 77 in samenhang met art. 97). In zo'n geval is op geen enkel moment een ex ante-toets voorzien.
34. De CTIVD en de TIB voorzien met een ex ante-toets tussen fases 2 en 3 een nieuw knelpunt in de uitvoering van de hackbevoegdheid. In het voorgestelde systeem moet er tijdens het proces van hacken nog toestemming worden gevraagd aan de afdeling toetsing van het CTT. Voor de snelheid en de effectiviteit van het proces is het logischer om vooraf toestemming te vragen voor het binnendringen van een geautomatiseerd werk dan om na het binnendringen toestemming te vragen voor het uitwinnen van dat apparaat of netwerk.
35. Ten aanzien van de inhoud van het toestemmingsverzoek worden in de voorgestelde regeling slechts beperkte waarborgen voorgesteld. Zo hoeven technische kenmerken, zoals een IP-adres, niet meer te worden vermeld in (verlengings)toestemmingsverzoeken. Hierdoor is het voor de afdeling toetsing niet inzichtelijk op hoeveel kenmerken een toestemmingsverzoek ziet. Deze kennis is wel van belang voor de beoordeling van met name de proportionaliteit van de inzet van de hackbevoegdheid. Het maakt uit of de dienst van plan is op drie, dertig, of driehonderd kenmerken de bevoegdheid in te zetten. De afdeling toetsing heeft geen toegang tot loggingsgegevens en kan niet controleren op hoeveel en op welke kenmerken wordt ingezet. Voor effectief toezicht op de hackbevoegdheid is noodzakelijk dat de (geautomatiseerde) logging goed is ingeregeld en dat de afdeling toezicht daar volledige toegang toe heeft.
36. Daarnaast hoeven technische risico's van een hack niet meer te worden omschreven. Wij vinden wel dat technische risico's separaat moeten worden meegewogen bij de beslissing over te gaan tot een hack. In het kader van het toetsen van de noodzaak, proportionaliteit en subsidiariteit is het van belang dat de diensten daarover zelf een afweging maken die ook voor de interne compliance en het CTT inzichtelijk is. Het meewegen van technische risico's in het toestemmingsverzoek is daarom nog steeds noodzakelijk.
37. Tot slot hebben de CTIVD en de TIB nog de volgende opmerkingen over de hackbevoegdheid.
    - Zoals in de memorie van toelichting wordt geschreven, is het mogelijk dat de drie fases door elkaar lopen. Ook in de eerste twee fases kunnen gegevens worden verzameld die noodzakelijk zijn voor het doel van die fases, zo blijkt uit de toelichting. Uit het wetsvoorstel en de toelichting daarop wordt niet duidelijk wat er moet gebeuren met de in fase 1 en fase 2 verworven gegevens als het toestemmingsverzoek voor fase 3 onrechtmatig wordt bevonden door de minister (of (onder)gemandateerde) of de afdeling toetsing van het CTT.
    - Art. 76, derde lid, dat van overeenkomstige toepassing wordt verklaard in art. 77 en 78, stelt dat het diensthoofd voor de dienst werkzame personen aanwijst die de hackbevoegdheid mogen uitoefenen. In het huidige art. 45, zesde lid, staat dat het diensthoofd aan hem ondergeschikte ambtenaren aanwijst. Wij vragen ons af of met deze definitiewijziging een uitbreiding is beoogd van de kring van personen die de hackbevoegdheid mogen uitoefenen. Als dit het geval is, verdient dit nadere uitleg in de memorie van toelichting. Wij zien risico's in een uitbreiding van de kring van personen, met name als die uitbreiding inhoudt dat personen die niet bij de dienst werkzaam zijn de hackbevoegdheid mogen uitvoeren.

5.2 Medewerkingsplicht online platforms

38. In de Wiv 2017 is al een medewerkingsplicht voor communicatieaanbieders geregeld. Dit houdt in dat deze aanbieders verplicht zijn medewerking te verlenen en te voldoen aan de vordering van gegevens. Deze medewerkingsplicht wordt in het wetsvoorstel uitgebreid naar online platforms (art. 91, derde lid; ziet op vordering van gegevens ex art. 85 en 87-90) en kredietinstellingen en financiële instellingen (art. 92). (Onder andere) deze organisaties konden op grond van de Wiv

2017 al door de diensten worden bevraagd op grond van de informantenbevoegdheid (art. 39 Wiv 2017). De vrijwilligheid van de medewerking komt met de voorgestelde artikelen te vervallen.

39. De CTIVD en de TIB voorzien een grote uitbreiding van de medewerkingsplicht, met name in het geval van de online platforms. De definitie van een online platform is breed en onvoldoende afgebakend. Veel verschillende organisaties kunnen hieronder vallen, ook organisaties waarvan het aanbieden aan anderen van de mogelijkheid om met elkaar te communiceren met behulp van een geautomatiseerd werk, niet het hoofddoel is (Cybercrimeverdrag). Voor de voorzienbaarheid van de wet, voor zowel de betreffende organisaties als de personen die met of via die organisaties op enige wijze communiceren, is het van belang dat de definitie van een online platform meer invulling krijgt en beter wordt afgebakend. De impact van deze uitbreiding is namelijk groot omdat iedereen klant of gebruiker is van de bedrijven waar het hier over gaat.

5.3 Bulkverwerving

40. Deze paragraaf gaat over bulkgegevens en bulkdatasets. Bulkgegevens zijn een verzameling persoonsgegevens die betrekking heeft op een groot aantal personen waarvan het merendeel van de personen geen onderwerp van onderzoek van een dienst is en dat ook niet zal worden. In bulkdatasets staan dus gegevens van mensen die géén dreiging vormen voor de nationale veiligheid. Een dataset met passagiersgegevens van vliegtuigen is een voorbeeld van een bulkdataset. Bulkinterceptie is een manier om bulkgegevens te verzamelen, maar ook met andere bevoegdheden kunnen de diensten bulkgegevens verwerven. Bulkinterceptie en het gebruik van bulkdatasets zijn belangrijk voor het werk van de diensten. Tegelijkertijd moeten de diensten extra zorgvuldig omgaan met bulkgegevens, omdat het voor een groot deel gaat om gegevens van personen die niet in onderzoek bij de diensten zijn. Daarom is het belangrijk dat voor de verwerving en verwerking van bulkgegevens passende waarborgen worden ingeregeld, zodat misbruik en onrechtmatig gebruik van die gegevens wordt voorkomen.

Bulkinterceptie

41. De CTIVD en de TIB constateren dat het wetsvoorstel de bestaande praktijk van onderzoeksopdrachtgerichte (OOG) interceptie, in de nieuwe wet bulkinterceptie, op verschillende punten beter weerspiegelt en verduidelijkt. Tegelijkertijd constateren de CTIVD en de TIB dat het wetsvoorstel de bevoegdheid op verschillende punten aanzienlijk verruimt zonder passende waarborgen. De verruimingen doen ook afbreuk aan de voorzienbaarheid van het wetsvoorstel.
42. Bulkinterceptie is in de Wiv 2017 en de Tijdelijke wet beschreven als OOG-interceptie. Dit betreft communicatie via internetkabels en satellieten. Bulkinterceptie omvat (lang) niet alle verwerving van bulkgegevens. Bulkdatasets kunnen ook worden verworven met andere bevoegdheden, zoals OSINT, de informantenbevoegdheid, de agentenbevoegdheid en de hackbevoegdheid. Het nieuwe wetsvoorstel kent geen bulkverwervingsartikelen, behalve bulkinterceptie.
43. Enkele voorbeelden van verruimingen in het wetsvoorstel:
    – Door het loslaten van het criterium van onderzoeksopdrachtgerichtheid, kunnen de diensten breder gegevens intercepteren dan voorheen. Interceptie hoeft namelijk niet langer gekoppeld te zijn aan een specifieke onderzoeksopdracht. Daarnaast kunnen de diensten gegevens intercepteren voor onderzoek A en die vervolgens gebruiken in onderzoek B. Dit gebeurt ook al onder de huidige Wiv (zie in dit kader ook het **CTIVD-rapport nr. 85** (2026) over de werking en waarde van het filterkader bij OOG-interceptie). De potentiële inbreuk hiervan wordt echter groter nu er op grond van het wetsvoorstel kan worden geïntercepteerd zonder dat daarbij een koppeling hoeft te worden gemaakt met een concrete onderzoeksopdracht. Deze breder geïntercepteerde gegevens kunnen vervolgens voor alle onderzoeken en ter ondersteuning van de taakuitvoering worden gebruikt. De CTIVD en de TIB vragen zich af hoe de diensten met deze

ruime mogelijkheid de noodzaak, proportionaliteit en subsidiariteit van bulkinterceptie willen onderbouwen.

- Daarnaast kunnen de diensten op basis van het wetsvoorstel volstaan met een meer abstracte omschrijving van de gegevensstromen die worden geïntercepteerd. Hierdoor kunnen meer verschillende gegevensstromen worden geïntercepteerd op basis van één toestemmingsverzoek. Dit levert de diensten weliswaar operationele wendbaarheid op, maar dit maakt de inzet van de bevoegdheid nóg minder gericht. Dat de diensten onder de Wiv 2017 moeten motiveren welke gegevensstromen worden geïntercepteerd en dat zij daarvoor toestemming moeten krijgen is een waarborg tegen onnodige verzameling van gegevens en dus tegen onnodige inbreuk op de persoonlijke levenssfeer van personen.
- Op basis van de toelichting op het wetsvoorstel is onduidelijk in hoeverre bulkinterceptie ook kan worden toegepast op Nederland-Nederland verkeer. Weliswaar benoemt de toelichting dat bulkinterceptie *"niet gericht [is] op het intercepteren van uitsluitend nationaal verkeer"*, maar niet uit te sluiten is dat verkeer met oorsprong en bestemming in Nederland wordt verworven. Of dit gebeurt, is afhankelijk van de breedte van de onderschepte gegevensstroom en de aard van de gegevens. Gezien het potentieel inbreukmakende karakter, dient de wetgever duidelijkheid te bieden over de vraag wat de diensten mogen met Nederland-Nederland verkeer dat zij onderscheppen. Bijvoorbeeld in het geval dat zij dergelijk verkeer onderscheppen ondanks dat de bulkinterceptie hier niet primair op gericht is en er een indicatie is dat de gegevens van waarde kunnen zijn voor onderzoeken van de diensten. Hierover moet het wetsvoorstel transparanter zijn. In termen van beperkingen kan er over worden gedacht of de diensten dergelijke gegevens met buitenlandse diensten mogen delen.

44. Zoals we hiervoor al hebben uiteengezet, kunnen de diensten op basis van het wetsvoorstel meer gegevens intercepteren op meer verschillende gegevensstromen. Daarnaast kunnen deze gegevens in het kader van alle inlichtingenonderzoeken worden bevraagd. Deze verruimingen vergroten de potentiële inbreuk van bulkinterceptie op de privélevens van personen. De verruimingen moeten daarom gepaard gaan met een toename van waarborgen.
45. De CTIVD en de TIB kunnen echter op basis van het wetsvoorstel niet goed beoordelen of sprake is van voldoende waarborgen. Dit komt onder andere door de technische en juridische complexiteit van het onderwerp. Hoe juridische bepalingen uiteindelijk worden vertaald in de technische uitvoeringspraktijk laat zich hierdoor moeilijk voorspellen. Deze vertaling wordt nog bemoeilijkt door het feit dat in het wetsvoorstel open normen staan, zoals 'bevragingskenmerk'. Het is onduidelijk wanneer dat 'voldoende vernauwend' is. Dit doet af aan de voorzienbaarheid van het wetsvoorstel. Daarnaast geldt dat het daadwerkelijke effect van veel waarborgen nog moet blijken, bijvoorbeeld door middel van toezichtonderzoek. De waarborg die functiescheiding moet bieden, zal in de toekomst in elk geval nog voor de inwerkingtreding van de nieuwe wet onderwerp zijn van onderzoek door de CTIVD.
46. Ook is onduidelijk hoeveel zicht het CTT concreet kan hebben op de uitoefening van bulkinterceptie. De verwachting is dat dit zicht met name bij de ex ante-toets beperkter wordt. Dit komt onder andere door de meer abstracte omschrijving van gegevensstromen in het toestemmingsverzoek en omdat ook andere onderdelen niet meer onderhevig zijn aan ex ante-toetsing, zoals bijvoorbeeld technisch onderzoek aan geïntercepteerde gegevens.
47. Tot slot vragen de CTIVD en de TIB zich af of de voorgestelde regeling voor bulkinterceptie voldoet aan de eisen die het EHRM daaraan stelt. In zijn arrest *Big Brother Watch* schrijft het EHRM dat het onafhankelijke autorisatieorgaan moet worden geïnformeerd over de doelstellingen van de interceptie en de verwachte communicatieroutes ('fibers' of kanalen) die zullen worden geïntercepteerd. Op die manier kan het autorisatieorgaan de noodzakelijkheid en proportionaliteit van de bulkinterceptie beoordelen en bekijken of de juiste keuzes zijn gemaakt.

6. Verwerving ter ondersteuning van de taakuitvoering

48. Met het voorgestelde art. 38 creëert de regering drie extra mogelijkheden om bijzondere bevoegdheden in te zetten ter ondersteuning van de taakuitvoering (art. 38, tweede lid, onder a, b en d). Dit is een ruime uitbreiding van de mogelijkheden van de diensten. De CTIVD en de TIB zijn met name kritisch op de voorgestelde uitbreiding onder b: de inzet van bijzondere bevoegdheden om capaciteiten die de diensten nodig hebben voor de taakuitvoering te ontwikkelen en te onderhouden.
49. Bijzondere bevoegdheden zijn bevoegdheden die een (grote) inbreuk kunnen maken op de persoonlijke levenssfeer van personen. Daarom moet de inzet daarvan niet alleen noodzakelijk, proportioneel en subsidiair zijn voor de bescherming van de nationale veiligheid en de democratische rechtsorde, maar gelden daarvoor ook aanvullende waarborgen.
50. In de Wiv 2017 zijn twee uitzonderingen gemaakt voor de inzet van bijzondere bevoegdheden in andere gevallen dan de taakuitvoering. Daar zijn strenge aanvullende waarborgen voor opgetuigd, namelijk een verkorte toestemmingsduur van een maand en een meldplicht bij de CTIVD. Deze waarborgen zijn er met een goede reden: in principe zetten de diensten (bijzondere) bevoegdheden alleen in voor hun taakuitvoering. Omdat deze bevoegdheden vergaande inbreuken maken op fundamentele rechten van personen, zijn de taken van de diensten limitatief in de wet opgenomen en worden zij alleen uitgeoefend in het belang van de nationale veiligheid. Dit betekent dat bevoegdheden alleen mogen worden ingezet als de nationale veiligheid in het geding is. De inzet van *bijzondere* bevoegdheden is in eerste instantie alleen aangewezen voor de inlichtingentaken van de AIVD en de MIVD (voorgestelde art. 2, tweede lid, onder a en b, en 3, tweede lid, onder a en b). Met de inzet van (bijzondere) bevoegdheden ter ondersteuning van de taakuitvoering wordt die directe link met de nationale veiligheid losgelaten. De CTIVD en de TIB menen daarom dat uiterst terughoudend moet worden omgegaan met het creëren van rechtsgrondslagen hiervoor. In uitzonderingsgevallen mogen bijzondere bevoegdheden ter ondersteuning van de taakuitvoering worden ingezet. Voor zover de voorgestelde uitzondering onder b al noodzakelijk zou zijn, moet die gepaard gaan met een verruiming van de waarborgen. Het wetsvoorstel voorziet niet in die waarborgen. In tegendeel, de waarborgen worden afgeschaald. Het is de CTIVD en de TIB niet duidelijk waarom het voor de diensten toegestaan zou moeten zijn om met 'echte' data te oefenen en niet kan worden volstaan met een testomgeving.
51. Anders dan in de Wiv 2017 zijn er geen (extra) waarborgen ingebouwd bij de inzet van bijzondere bevoegdheden ter ondersteuning van de taakuitvoering. De toestemmingverlening kan worden (onder)gemandateerd, de toestemmingstermijn is niet ingekort en er is geen meldplicht bij het CTT.
52. De noodzaak van het opnemen van de mogelijkheid om gegevens te verwerven ten behoeve van het ontwikkelen en onderhouden van capaciteiten die de diensten nodig hebben voor hun taakuitvoering is onvoldoende onderbouwd. De voorbeelden die de memorie van toelichting geeft – het op peil houden van de vaardigheden van medewerkers en het testen van een richtmicrofoon – overtuigen niet. Het is immers mogelijk om onder deze bepaling ook veel en meer inbreukmakende operaties uit te voeren gericht op personen en organisaties.
53. Deze kritiek geldt ook voor de onder a gecreëerde grondslag, de inzet van bijzondere bevoegdheden om de uitoefening van operationele bevoegdheden mogelijk te maken. Hoewel het voorstelbaar is dat er gevallen zijn waarin een vroegtijdige inzet van bijzondere bevoegdheden noodzakelijk is, moet worden afgewogen of het noodzakelijk is hier een speciale grondslag voor te creëren en deze situatie niet te koppelen aan de taakuitvoering van de diensten. In veel gevallen zal ook die vroegtijdige inzet plaatsvinden in het kader van een onderzoeksopdracht en zal die binnen de taakuitvoering (kunnen) vallen. Door deze grondslag te creëren, bestaat ook het risico dat er al bijzondere bevoegdheden worden ingezet ter ondersteuning van de inzet van een bijzondere bevoegdheid die later niet noodzakelijk, proportioneel en/of subsidiair blijkt te zijn.

B Stelsel van verdere verwerking

7. Verwerking algemeen

54. Het (verder) verwerken van persoonsgegevens maakt inbreuk op de persoonlijke levenssfeer van personen. Daarom moet de wet waarborgen introduceren die ervoor zorgen dat die inbreuk alleen plaatsvindt als die noodzakelijk is en zo klein mogelijk wordt gehouden. Een belangrijke waarborg is dat gegevens worden verwijderd en vernietigd als ze niet (meer) van betekenis zijn voor het werk van de diensten.
55. De regering introduceert met het wetsvoorstel een nieuw stelsel voor de verdere verwerking van gegevens. Dit stelsel kent verschillende soorten gegevens die eigen regels en waarborgen krijgen. Een aantal regels gelden in het algemeen. In de eerste plaats zijn dit de algemene normen die worden gesteld aan de uitoefening van bevoegdheden en de gegevensverwerking (paragrafen 3.1, 3.2 en 3.3), zoals bijvoorbeeld de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit en doelbinding. Daarnaast kent hoofdstuk 6 over de verdere verwerking van gegevens een aantal algemene normen. Gegevens die, gelet op het doel waarvoor zij worden verwerkt, geen betekenis hebben of hun betekenis hebben verloren, worden verwijderd (art. 98). Dit is een algemene plicht tot datareductie. Verder wordt in het algemeen een bewaartermijn voor gegevens ten aanzien van informanten en agenten gecreëerd (art. 99). Tot slot is er een algemene regeling voor de omgang met onvoorzien verzamelde vertrouwelijke gegevens van journalisten en advocaten (art. 100). Met deze laatste regeling is een al eerder gedane aanbeveling van de CTIVD opgevolgd. Deze regeling is breder dan die in de Wiv 2017, omdat die geldt voor gegevens verzameld met bijzondere én algemene bevoegdheden en ook de vertrouwelijke gegevens van journalisten hieronder vallen.
56. Het wetsvoorstel vereist toestemming van de rechtbank voor inzet van operationele bevoegdheden jegens leden van de Eerste en Tweede Kamer van de Staten-Generaal, als ook jegens leden of medewerkers van het CTT (art. 42). Dit vereiste geldt overigens op grond van lid 2 niet op de uitoefening van algemene bevoegdheden in de uitvoering van de taken van de diensten, bedoeld in art. 2 lid 2 onder d, e, en f, en art. 3 lid 2 onder d, e, en f. Deze waarborg van rechterlijke toestemming is nieuw ten opzichte van de Wiv 2017. Het is aan de wetgever om te bepalen of sprake is van voldoende waarborgen in deze gevallen.
57. Voor een aantal categorieën gegevens zijn deze algemene regels de enige toepasselijke regels voor de verdere verwerking ervan. Dit geldt voor:
    - Alle gegevens die geen persoonsgegevens zijn;
    - Alle specifieke persoonsgegevens die met algemene bevoegdheden zijn verworven voor de taakuitvoering;
    - Alle specifieke persoonsgegevens die zijn opgenomen in een dossier.
    - Alle persoonsgegevens, inclusief bulkgegevens, die met algemene bevoegdheden zijn verworven ter ondersteuning van de taakuitvoering.
58. Voor deze gegevens gelden bijvoorbeeld geen bewaartermijnen, verplichte (her)beoordelingen of de gegevens nog betekenis hebben of toegangsregimes (waardoor het aantal medewerkers van de diensten dat toegang heeft tot de gegevens wordt beperkt). Ten aanzien van persoonsgegevens geldt weliswaar de algemene norm dat gegevens moeten worden verwijderd als zij hun betekenis hebben verloren, maar het risico bestaat dat deze gegevens blijven rondzwerven in de systemen van de diensten als er geen beoordelingstermijn wordt gesteld. Daarom zijn de CTIVD en de TIB van oordeel dat er een periodieke beoordeling van gegevens(sets) verplicht moet worden gesteld als extra waarborg voor gegevensreductie.

59. De CTIVD en de TIB constateren verder dat deze voorgestelde regeling niet overeenkomt met het in de memorie van toelichting genoemde uitgangspunt dat de wijze waarop gegevens zijn verzameld niet bepalend is voor de wijze waarop deze gegevens (verder) worden verwerkt. Voor persoonsgegevens, niet zijnde bulkgegevens, maakt het in het voorgestelde stelsel namelijk wél uit of die met algemene of bijzondere bevoegdheden zijn verworven. Het maakt ook uit voor de waarborgen of gegevens zijn verworven voor de taakuitvoering of ter ondersteuning van de taakuitvoering. Deze criteria (algemene/bijzondere bevoegdheden of voor (de ondersteuning van) de taakuitvoering) bepalen niet of de inhoud van de persoonsgegevens zelf inbreuk makend is of niet, zoals de regering zelf ook stelt. Het verwerken van (*real time*) locatiegegevens zal bijvoorbeeld meer inbreuk maken op de persoonlijke levenssfeer van een persoon dan het verwerken van een geboortedatum. Beide soorten gegevens kunnen met zowel algemene als bijzondere bevoegdheden en zowel voor de taakuitvoering als ter ondersteuning van de taakuitvoering worden verworven. Toch wordt aan de hand van deze criteria onderscheid gemaakt in de regels en waarborgen voor het (verder) verwerken ervan. Wij betwijfelen daarom of aan het – wat ons betreft juiste – uitgangspunt van de regering recht wordt gedaan met het voorgestelde stelsel van verdere verwerking van gegevens.
60. De CTIVD en de TIB willen aandacht vragen voor de definitie van persoonsgegevens. Deze lijkt evident, maar in de praktijk kan er discussie bestaan over de vraag of iets een persoonsgegeven is. Als een niet-persoonsgegeven wordt gecombineerd met (andere) persoonsgegevens, kan dat eerste gegeven alsnog betrekking hebben op een persoon en dus een persoonsgegeven worden. De aanduiding van een gegeven als persoonsgegeven is in dit wetsvoorstel extra relevant omdat de regels en waarborgen daarvan afhangen. Een heldere definitie ontbreekt echter in dit wetsvoorstel.
61. Naast de algemene regels voor gegevensverwerking introduceert de regering drie bijzondere verwerkingsregimes, namelijk de (verdere) verwerking van specifieke gegevens, bulkgegevens en gegevens ter ondersteuning van de taakuitvoering. Het verwerken van bulkgegevens wordt besproken in paragraaf 6 en het verwerken ter ondersteuning van de taakuitvoering komt in paragraaf 8 aan bod. Hieronder gaan wij in op de verwerking van specifieke gegevens.

8. Specifieke verwerkingsregimes

8.1 Specifieke gegevens

62. Specifieke gegevens zijn alle persoonsgegevens die geen bulkgegevens zijn, aldus de memorie van toelichting. Aan die definitie voegen wij nog toe dat specifieke gegevens alleen de persoonsgegevens zijn die met de uitoefening van bijzondere bevoegdheden zijn verworven in het kader van de taakuitvoering van de diensten. Zoals hiervoor al is opgemerkt, wordt hiermee niet voldaan aan het uitgangspunt van de regering dat gegevens worden verwerkt op basis van de inbreuk en niet op basis van de manier van verwerven van de gegevens. De CTIVD en de TIB pleiten ervoor om ook persoonsgegevens die met algemene bevoegdheden zijn verworven in dit verwerkingsregime op te nemen. Ook de verdere verwerking van deze persoonsgegevens kan namelijk inbreuk makend zijn.
63. Daarnaast zien de CTIVD en de TIB een vermindering van waarborgen in de werkwijze van het verder verwerken van specifieke gegevens. Het wetsvoorstel voorziet niet meer in een relevantiebeoordeling binnen een bepaalde termijn (max. anderhalf jaar) van gegevens die met bijzondere bevoegdheden zijn verworven, waarna niet beoordeelde gegevens moeten worden vernietigd. De huidige relevantiebeoordeling kan zowel plaatsvinden voor het onderzoek waarvoor de gegevens zijn verworven als voor enig ander lopend onderzoek binnen de taken van de diensten waarvoor bijzondere bevoegdheden mogen worden ingezet. Pas als gegevens relevant zijn bevonden en in het betekenisregime komen, komen ze beschikbaar voor alle taken van de diensten. Als voorbeeld: Het wetsvoorstel voorziet in een mogelijkheid om die gesprekken integraal geautomatiseerd uit te werken, te verwerken en de inhoud daarvan vast te leggen en gedurende jaren te bewaren en doorzoekbaar te houden. De gehele inhoud van de inzet van bijzondere bevoegdheden komt in het wetsvoorstel ook beschikbaar voor andere taken van de diensten; ook voor de taken waarvoor het niet is toegestaan bijzondere bevoegdheden in te zetten.
64. Het wetsvoorstel stelt een bewaartermijn aan persoonsgegevens die ten behoeve van “kortlopende” onderzoeken zijn verworven. Ook moeten persoonsgegevens die in langlopende onderzoeken zijn verworven, periodiek worden beoordeeld of zij nog steeds van betekenis zijn. Wat ons betreft zou een herbeoordelingsplicht ook moeten gelden voor gegevens die in een dossier zijn opgenomen. Ook is niet duidelijk op basis van welk criterium of beoordeling gegevens in een dossier kunnen worden opgenomen.
65. De mogelijkheid om specifieke gegevens ook te gebruiken in andere onderzoeken dan waarvoor zij in eerste instantie zijn verworven verdient nadere onderbouwing. Kunnen specifieke gegevens die zijn verworven ten behoeve van onderzoek A in een dossier uit onderzoek B worden geplaatst of kunnen die specifieke gegevens helemaal worden overgeheveld naar onderzoek B? In dat laatste geval voorzien wij uitvoeringsproblemen met het bijhouden van bewaartermijnen.

8.2 Verdere verwerking van bulkgegevens

66. De regering schrijft in de memorie van toelichting dat het uitgangspunt bij de verwerking van bulkgegevens is dat de wijze van verwerving van deze gegevens niet bepalend is voor de wijze van verwerking. Er wordt dus niet langer onderscheid gemaakt tussen bulkdatasets die met algemene of bijzondere bevoegdheden zijn verworven. Ook zijn de diensten niet langer verplicht om een indeling van de gegevens te maken op basis van een inhoudelijke beoordeling. De praktijk heeft uitgewezen, aldus de regering, dat het niet altijd eenvoudig is om een indeling van de bulkdatasets te maken op basis van de mate van inbreuk op het recht op privacy.

67. De CTIVD en de TIB zijn voorstanders van het wél op inhoud beoordelen van bulkdatasets, omdat op die manier de daadwerkelijke inbreuk van verwerking én bijbehorende waarborgen kunnen worden vastgesteld. Wij lichten dit hieronder nader toe.
68. Op dit moment moeten de diensten op grond van de Tijdelijke regeling verdere verwerking bulkdatasets (hierna: Tijdelijke regeling) en de Tijdelijke wet (Tw) aan alle bulkdatasets, behalve de sets die door middel van OOG-interceptie (art. 48 Wiv 2017) zijn verworven, een toegangsregime toewijzen. De diensten beoordelen in welke mate de verdere verwerking van een bulkdataset een beperking oplevert van het recht op bescherming van de persoonlijke levenssfeer (art. 8 EVRM). Dit doen zij aan de hand van in ieder geval de volgende criteria: a) de mate waarin een bulkdataset inzicht geeft in bepaalde aspecten van het privéleven, waaronder identificerende gegevens, locaties, netwerk en vertrouwelijke inhoudelijke gegevens, en b) de mate waarin een bulkdataset voor eenieder toegankelijk is. De diensten scoren iedere bulkdataset op deze criteria en wijzen een toegangsregime toe aan de bulkdataset. Daarbij wordt onderscheid gemaakt tussen drie toegangsregimes: 'standaard', 'beperkt' of 'strikt beperkt'. Afhankelijk van het toegewezen toegangsregime hebben meer of minder dienstmedewerkers toegang tot (de gegevens in) de bulkdataset en wordt een (langere of kortere) termijn voor periodieke beoordeling vastgesteld waarop de diensten (opnieuw) beoordelen of de bulkdataset moet worden verwijderd.
69. Naar het oordeel van de CTIVD werkt de werkwijze die voortvloeit uit de Tijdelijke regeling goed. Bulkdatasets worden inhoudelijk beoordeeld op de mate van inbreuk. Deze beoordeling is belangrijk voor het toewijzen van passende waarborgen voor de verdere verwerking van deze bulkgegevens. Met de Tijdelijke regeling is een goed gedifferentieerd waarborgenstelsel ontstaan. Dat het 'niet altijd eenvoudig is', aldus de regering, om bulkdatasets in te delen op grond van de mate van inbreuk op het recht op privacy is onvoldoende onderbouwing om deze regeling los te laten. Het voorgestelde stelsel van indeling in regimes leidt niet tot een beoordeling op basis van de mate van inbreuk. Daarom is het onvoldoende in staat om in passende waarborgen te voorzien.
70. Het wetsvoorstel voorziet in een indeling van bulkdatasets in vier regimes: het AMvB-regime, het standaardregime, het regime voor bijzondere bulkgegevens en het regime voor de verwerking van bulkdatasets ter ondersteuning van de taakuitvoering (zie paragraaf 7.3). De indeling in regimes is deels gebaseerd op de mate van verwerving of hangt daarmee samen. Daarom voldoet het wetsvoorstel niet aan het uitgangspunt van de regering dat de verdere verwerking van bulkdatasets niet afhangt van de wijze van verwerving (algemene of bijzondere bevoegdheden). In de praktijk zullen AMvB-sets vooral door middel van algemene bevoegdheden worden verworven. Uit het recente toezichtrapport **nr. 84** (juli 2026) van de CTIVD over de verwerking van bulkdatasets blijkt dat bulkdatasets die met algemene bevoegdheden worden verworven in de praktijk zelfs vaker gevoelige gegevens bevatten dan bulkdatasets die met bijzondere bevoegdheden zijn verworven. Daarnaast is er (weer) een speciale regeling voor bijzondere bulkdatasets, waaronder met name sets vallen die zijn verworven door middel van bulkinterceptie. Ook bulkdatasets die ter ondersteuning van de taakuitvoering zijn verworven, krijgen een eigen regeling met minder waarborgen dan bulkdatasets die voor de taakuitvoering zijn verworven. Het waarborgenstelsel wordt bepaald aan de hand van andere, minder relevante criteria dan de mate van inbreuk van een bulkdataset. De CTIVD en de TIB adviseren de werkwijze van de huidige Tijdelijke regeling in stand te houden. Hieronder bespreken we onze zorgen ten aanzien van twee bulkregimes (het AMvB-regime en het standaardregime).

Het AMvB-regime

71. Op grond van het voorgestelde art. 107 kunnen categorieën bulkgegevens waarvan de verdere verwerking door de diensten geen onevenredige gevolgen heeft voor betrokkenen in vergelijking met het belang van de taakuitvoering door de diensten als zodanig worden aangewezen. De term 'onevenredige gevolgen' is een breed begrip. De CTIVD en de TIB voorzien dat de inkleding van dit begrip voor discussie zal zorgen, mede gelet op de uitleg van het begrip in de memorie van

toelichting. De memorie van toelichting kleedt dit begrip namelijk in door de kenbaarheid van dergelijke gegevens binnen de overheid en de mogelijkheid voor de diensten om daarover te beschikken centraal te stellen. De voorzienbaarheid dat de diensten over bepaalde bulkdatasets beschikken lijkt ons nauwelijks relevant voor de vraag of de verdere verwerking daarvan 'onevenredige gevolgen' heeft voor betrokkenen. Dat laatste hangt wat ons betreft met name af van de aard (en inhoud) van de gegevens in de bulkdatasets.

72. In de artikelsgewijze toelichting bij art. 107 wordt als voorbeeld van een mogelijke AMvB-bulkdataset een set met de justitiële gegevens van personen, oftewel het strafblad, genoemd. De regering schrijft: "Justitiële gegevens zijn in de AVG genoemd als bijzondere persoonsgegevens. In algemene zin heeft de verwerking hiervan een aanzienlijke impact op de privacy van betrokkene." Hier sluiten de CTIVD en de TIB zich bij aan. De regering vervolgt echter dat het verwerken door de diensten van deze gegevens slechts beperkte gevolgen heeft voor betrokkene, omdat andere overheidsorganisaties, zoals politie, justitie en reclassering ook toegang hebben tot justitiële gegevens. Wij kunnen deze redenering niet volgen, omdat er significante verschillen zijn tussen verwerking door deze overheidsorganisaties ten opzichte van verwerking door de diensten. De diensten kunnen deze gegevens immers combineren met veel andere gegevens waarover zij kunnen beschikken. Hierdoor zijn zij in staat op gedetailleerd niveau een inkijk te krijgen in iemands leven. Deze gegevens worden door de diensten verwerkt in een geheime context. Er is geen controle door een rechter. Daarnaast gelden er bewaartermijnen voor de verwerking van gegevens door de politie. Het verwerken van justitiële gegevens van betrokkenen door de diensten heeft dus wel degelijk extra impact op zijn privacy.
73. De waarborgen bij het verwerken van AMvB-bulkdatasets worden afgeschaald met het argument dat voorzienbaar is dat de diensten beschikken over deze bulkgegevens. Nogmaals, dit is niet het relevante criterium voor het bepalen van de inbreuk op fundamentele rechten die wordt gemaakt door het verwerken van bulkgegevens. Er is geen bewaartermijn of herbeoordelingstermijn: zolang de categorie waartoe een bulkdataset behoort, is opgenomen in de AMvB mag die set worden bewaard. Daarnaast zijn AMvB-sets voor alle dienstmedewerkers toegankelijk (zolang noodzakelijk voor de aan hen opgedragen taak), zonder dat zij toestemming hoeven te vragen voor het gebruik van de bulkdataset. Deze bulkdatasets zijn te raadplegen voor alle taken van de diensten. Dat de afdeling toezicht van het CTT bindend toezicht heeft op de aanwijzing van AMvB-sets is een belangrijke waarborg, maar dat corrigeert het onderliggende systeem onvoldoende. Ook als een bulkdataset naar het oordeel van de afdeling toezicht geen 'onevenredige gevolgen' heeft voor betrokkenen en dus rechtmatig als AMvB-set is aangemerkt, is bijvoorbeeld een herbeoordelingsplicht alsnog een belangrijke waarborg. De CTIVD en de TIB zijn daarom van oordeel dat onvoldoende is onderbouwd waarom bij de verdere verwerking van AMvB-sets minder waarborgen nodig zijn.

Het standaardregime

74. Alle bulkdatasets die in het kader van de taakuitvoering worden verworven en niet in het AMvB-regime of in het bijzondere bulkregime worden verwerkt, vallen onder het standaardregime. In het standaardregime zullen daarom bulkdatasets worden verwerkt, die in verschillende mate inbreuk maken op fundamentele rechten. Toch kiest de regering ervoor om voor al deze bulkdatasets één regeling te treffen. De waarborgen die hiertegenover staan, sluiten aan bij de waarborgen die nu gelden voor het standaard toegangsregime, oftewel het regime met bulkdatasets met de (relatief) geringste inbreuk. Dit geldt voor de toegang tot gegevens uit een bulkdataset (voorgesteld art. 104, eerste lid), voor de bewaartermijn (voorgesteld art. 105) en voor de herbeoordelingsplicht (voorgesteld art. 106). Voor de bulkdatasets die nu vallen binnen het beperkte en strikt beperkte toegangsregime en onder de nieuwe wet in het standaardregime komen, zullen de waarborgen verminderen, terwijl de feitelijke inbreuk van het verwerken van die bulkgegevens gelijk blijft. Het bevragen van een bulkdataset die in het standaardregime valt is een algemene bevoegdheid,

dus dienstmedewerkers hoeven daarvoor niet om toestemming te verzoeken. De CTIVD en de TIB bevelen aan om ook in het standaardregime de inhoudelijke beoordeling van de gegevens te behouden en op basis daarvan een waarborgenstelsel in te richten, zoals nu ook gebeurt onder de Tijdelijke regeling.

75. Het wetsvoorstel handhaaft bindend toezicht door de onafhankelijke toezichthouder op het verlengen van bewaartermijnen. De CTIVD heeft goede ervaringen met de huidige regeling uit de Tijdelijke wet cyberonderzoeken en bulkdatasets (Tw). In februari 2026 heeft de CTIVD in het kader van de Invoeringstoets Tw aan de Tweede Kamer medegedeeld dat enkel de mogelijkheid van een bindend (onrechtmatigheids)oordeel al tot normconform gedrag heeft geleid, zonder dat de CTIVD daadwerkelijk van haar bevoegdheid gebruik hoefde te maken.

8.3 Verdere verwerking van gegevens ter ondersteuning van de taakuitvoering

76. (Bulk)gegevens die ten behoeve van de ondersteuning van de taakuitvoering zijn verworven, krijgen eigen regels voor de verwerking ervan. De regels die gelden voor gegevens die ten behoeve van de taakuitvoering zijn verworven, zijn niet van toepassing, met uitzondering van de algemene regels van het voorgestelde art. 98. In de memorie van toelichting wordt niet gemotiveerd waarom gegevens die ter ondersteuning van de taakuitvoering dienen andere regels met minder waarborgen voor de verdere verwerking ervan moeten krijgen. Ten aanzien van bulkgegevens behelst dit een afwijking van het uitgangspunt ‘bulk is bulk’. De regering maakt de noodzaak (en proportionaliteit) van deze afwijking niet duidelijk.
77. Een goed ingerichte functiescheiding zou een belangrijke waarborg kunnen zijn. De voorgestelde inrichting van die functiescheiding doet daar echter aan af. Ten eerste geldt de functiescheiding slechts voor gegevens die met bijzondere bevoegdheden zijn verworven. Voor gegevens die met algemene bevoegdheden zijn verworven ter ondersteuning van de taakuitvoering geldt deze beperking niet. Dienstmedewerkers die in de functiescheiding werken, kunnen ook bij een inlichtingenteam werken, dienstmedewerkers uit inlichtingenteams kunnen collega’s in de functiescheiding ondersteunen en bijstaan en dienstmedewerkers uit inlichtingenteams die meedoen aan een opleiding kunnen ook bij deze gegevens. Al deze uitzonderingen op de functiescheiding kleden de waarborgfunctie ervan uit en zorgen ervoor dat deze waarborg onvoldoende effect heeft.
78. Als de noodzaak van het inrichten van een apart verwerkingsregime ten aanzien van bulkgegevens ter ondersteuning van de taakuitvoering wordt aangenomen, stellen de CTIVD en de TIB voor om ook hierin te werken met een categorisering van bulkdatasets aan de hand van de inbreuk die de gegevens in die set maken. In een bulkdataset zitten persoonsgegevens van personen die niet in onderzoek zijn van de diensten. Als deze gegevens bijvoorbeeld worden gebruikt voor het trainen van applicaties, wordt er ook inbreuk gemaakt op de persoonlijke levenssfeer van de betrokkenen. De gegevens van die persoon zitten immers in systemen van de overheid en zijn volledig buiten zijn eigen controle.
79. De CTIVD en de TIB vragen uitdrukkelijk aandacht voor het feit dat er geen bewaartermijn is gesteld aan het verwerken van (bulk)gegevens ter ondersteuning van de taakuitvoering. Deze gegevens vallen weliswaar onder de algemene norm dat gegevens moeten worden verwijderd als zij hun betekenis hebben verloren, maar het risico bestaat dat deze gegevens blijven rondzwerven in de systemen van de diensten als er geen beoordelingstermijn wordt gesteld. Daarom zijn wij van oordeel dat een periodieke beoordeling van gegevens(sets) verplicht moet worden gesteld als extra waarborg voor gegevensreductie.

80. Tot slot voorzien wij uitvoeringsproblemen bij het bepaalde in art. 113. Met de voorgestelde wettekst worden verschillende typen (persoons)gegevens en bulkdatasets geïntroduceerd met eigen verschillende bewaartermijnen (en andere gebruiksregels). Deze verschillen moeten niet alleen juridisch worden onderscheiden, maar ook worden vertaald naar en geïmplementeerd in de datahuishouding van de diensten, denk aan ICT-systemen, autorisatiebeheer en logging. Op deze punten bestaan al uitvoeringsproblemen, zoals een versnipperd datalandschap, onvoldoende herleidbaarheid van autorisaties en verschillen in de wijze waarop bewaartermijnen worden bewaakt en gegevens worden verwijderd (zie toezichtrapport **nr. 84** (juli 2026)) van de CTIVD). Het uitvoeren van onder andere art. 113 vergroot daarom aanzienlijk het risico op het gebruik van persoonsgegevens (in bulkdatasets) buiten de wettelijke bewaartermijnen, onbevoegde toegang tot de persoonsgegevens en gebrekkige herleidbaarheid en controleerbaarheid van het gebruik van persoonsgegevens.

9. Automatisering

81. Onder de Wiv 2017 is er veel discussie over de definitie en invulling van geautomatiseerde data-analyse (GDA). Daarom heeft de regering ervoor gekozen om in het wetsvoorstel een nieuwe bepaling op te nemen die automatisering door de diensten integraal moet reguleren. Automatiseringstoepassingen, zoals AI, ontwikkelen zich in hoog tempo. Het gebruik van AI kan bovendien (zeer) risicovol zijn. Large Language Models (LLM) kunnen bijvoorbeeld feiten verzinnen (hallucinaties) en kunnen afhankelijk van de gegevensinput vooroordelen in zich hebben. De toeslagenaffaire is een goed voorbeeld van hoe ernstig personen kunnen worden benadeeld door verkeerd gebruik van algoritmes. Ook het gebruik van AI door de diensten kan grote gevolgen hebben voor personen als de risico's onvoldoende worden gemitigeerd.
82. Daarom is het aan de ene kant noodzakelijk om hiervoor gedegen wetgeving en juridische kaders te ontwikkelen, waarin voldoende waarborgen zijn opgenomen om misbruik en fouten tegen te gaan. De diensten moeten er ook voor zorgen dat de verslaglegging voldoende is om verantwoording af te kunnen leggen aan de interne compliance-afdeling en het CTT.
83. Aan de andere kant is het een uitdaging om een goed juridisch kader te schrijven dat voorzienbaar en bruikbaar is en ook genoeg ruimte houdt om te kunnen anticiperen op technologische ontwikkelingen, zoals quantumtechnologie. In de EU is in 2024 de "AI Act", oftewel de AI-verordening, in werking getreden. Hierin worden regels gesteld over het gebruik van AI. Het wetsvoorstel volgt niet het systeem van de AI Act. Anders dan de AI Act heeft de regering geen risicocategorieën geïntroduceerd. De CTIVD en de TIB adviseren om deze categorieën over te nemen in de nieuwe wet, zodat per risicocategorie voldoende waarborgen kunnen worden ingericht. Ten aanzien van het voorliggende voorstel hebben wij verder de volgende opmerkingen en bedenkingen.
84. In het wetsvoorstel wordt ten aanzien van automatisering een aantal ruime, minimaal gedefinieerde begrippen gebruikt. Zo is niet duidelijk wat 'onevenredige gevolgen' inhoudt, waartegen die gevolgen moeten worden afgezet en wie bepaalt wat onevenredige gevolgen zijn. In het voorgestelde art. 33 wordt het begrip 'risicotoepassing' geïntroduceerd. Op grond van dit artikel moet iedere automatiseringstoepassing worden beoordeeld op het zijn van risicotoepassing. Daarvan is sprake 'indien de resultaten van de toepassing voorafgaand aan het gebruik niet kenbaar zijn'. Wij voorzien dat er discussie zal ontstaan over wanneer de uitkomst van een automatiseringstoepassing kenbaar zal zijn. Bovendien wordt hierop in het tweede lid meteen een brede uitzondering gemaakt. Van een risicotoepassing is geen sprake 'indien het gebruik van de toepassing in het maatschappelijk verkeer gebruikelijk is'. Het gebruik in het maatschappelijk verkeer is echter geen graadmeter voor de inbreuk die een risicotoepassing kan maken op fundamentele rechten. (AI-)chatbots, zoals ChatGPT, zijn inmiddels redelijk ingeburgerd, maar kennen nog steeds grote risico's. Dat het gebruik ervan 'normaal' is, betekent niet dat de diensten weten hoe het LLM achter de chatbot werkt en of de output betrouwbaar en correct is. Daarnaast is het gebruik van zo'n chatbot in het maatschappelijk verkeer waarschijnlijk onschuldiger dan wanneer de diensten daarvan gebruik maken. De diensten hebben immers ontzettend veel gegevens beschikbaar en kunnen die gegevens met elkaar combineren.
85. Als een toepassing als risicotoepassing wordt aangemerkt, moeten de diensten maatregelen nemen om de onbedoelde gevolgen daarvan te voorkomen (voorgesteld art. 34). De mate van betrouwbaarheid van de toepassing moet worden onderzocht, de toepassing moet zijn voorzien van voldoende instructies voor gebruikers en de minister (of (onder)gemandateerde) moet toestemming hebben verleend voor het gebruik van de toepassing. De voorgestelde risicobeheersing werkt als een hefboom. Is aan deze voorwaarden voldaan, dan mag de risicotoepassing volgens de memorie van toelichting in verschillende contexten worden gebruikt.
86. Daarmee wordt miskend dat verschillende contexten verschillende risico's met zich mee kunnen brengen. Het risico dat kleeft aan (de gevoeligheid van) gegevens die je invoert in de

risicotoepassing of de gevolgen die de uitkomst van de toepassing hebben, worden hier bijvoorbeeld niet meegewogen. Daarnaast is de context van het in gebruik nemen van de risicotoepassing van groot belang voor de beoordeling van de betrouwbaarheid daarvan. Door een algemene toestemming te geven voor het in gebruik nemen van een risicotoepassing wordt dus geen recht gedaan aan andere factoren die een belangrijke invloed hebben op de risico's van de toepassing.

87. De CTIVD en de TIB zijn van oordeel dat een systeem met risicocategorieën zoals opgenomen in de EU AI Act meer recht doet aan de verschillende maten van inbreuk die risicotoepassingen in verschillende omstandigheden kunnen maken. Bij het indelen in categorieën kunnen bijvoorbeeld factoren als gevoeligheid van de inputgegevens, betrouwbaarheid van de toepassing, mogelijke gevolgen voor betrokkenen en kenbaarheid van de uitkomst worden meegewogen. Een risicotoepassing wordt dan niet in het algemeen goedgekeurd, maar krijgt passende waarborgen afhankelijk van het risico. Voor toepassingen die een laag risico met zich meebrengen, hoeven de diensten dan bijvoorbeeld geen extra toestemming te verzoeken aan de minister. Bepaalde toepassingen met een hoog risico zouden bijvoorbeeld kunnen worden uitgesloten van het inlichtingenproces.
88. De uitzondering in art. 34 vijfde lid is te kort door de bocht. Ook voor het trainen van modellen en het overigens ontwikkelen van capaciteiten kan een betrouwbaarheidsbeoordeling nodig zijn. De omstandigheid dat de risicotoepassing wordt gebruikt voor de ontwikkeling van capaciteiten kan worden meegewogen bij de indeling in risicocategorieën.

C Stelsel van verstrekking en samenwerking

10. Samenwerking/externe verstrekking

10.1 Algemeen

89. Hoewel de CTIVD en de TIB zien dat samenwerking met andere partijen essentieel kan zijn voor een goede taakuitvoering door de diensten, vinden wij dat de verruimingen in dit hoofdstuk van het wetsvoorstel met onvoldoende waarborgen gepaard gaan. De wijze waarop deze bepalingen nu zijn geformuleerd houdt aanzienlijke risico's in voor fundamentele rechten.
90. Het wetsvoorstel bevat een veelheid aan grondslagen voor samenwerking van de diensten met andere partijen, zowel met nationale/internationale als met publieke/private partijen en zowel bi- als multilateraal. Wij zien bij het onderwerp samenwerking verruimingen over de gehele linie. Het betreft een potentieel oneindige hoeveelheid partijen waarmee kan worden samengewerkt. Zo rekt het wetsvoorstel het internationale speelveld op door te spreken over 'buitenlandse militaire inlichtingen- en veiligheids*entiteiten*' en 'buitenlandse inlichtingen- en veiligheidsdiensten' in plaats van over 'inlichtingen- en veiligheidsdiensten van andere landen'. Samenwerking met nationale overheidsinstanties wordt verruimd, door meer partijen op te nemen en de mogelijkheid te bieden bij AMvB de groep verder uit te breiden. De MIVD wordt op dit punt gelijkgetrokken met de AIVD en dat betreft een forse uitbreiding. Vergaand in het wetsvoorstel is de samenwerking met private partijen. Deze partijen zijn niet beperkt. Dit kan verschillende vormen aannemen: bilateraal (een op een), in groepsverband met meerdere private partijen, maar ook in hybride constructies met deelnemers uit buitenland, binnenland, overheid en het private domein. Voor de MIVD voorziet het wetsvoorstel in extra samenwerkingsbepalingen met de krijgsmacht en andere defensieonderdelen. Daarnaast is het de diensten toegestaan ruwe, onbewerkte, (bulk) gegevens aan de krijgsmacht of andere defensieonderdelen te verstrekken.
91. De risico's van samenwerking met externe partijen, zoals overheidsinstanties, private partijen en buitenlandse diensten, worden in het wetsvoorstel slechts zeer beperkt afgewogen. De CTIVD en de TIB wijzen erop dat altijd voorafgaand aan de samenwerking en aan de verstrekking van gegevens een weging plaats zou moeten vinden of die samenwerking wel gerechtvaardigd is. Een dergelijke afweging dient niet alleen plaats te vinden bij structurele samenwerking waarbij persoonsgegevens kunnen worden uitgewisseld, zoals het wetsvoorstel voorschrijft. Hierdoor wordt allereerst voorbijgegaan aan het feit dat ook het delen van andere dan persoonsgegevens een risico met zich mee kan brengen. Daarnaast kan het delen van gegevens toch resulteren in de herleidbaarheid van natuurlijke personen, bijvoorbeeld als de ontvanger van gegevens door de informatie die hij al tot zijn beschikking heeft die personen kan identificeren. Oftewel, het kan zijn dat de diensten persoonsgegevens delen zonder dat zij zich daarvan bewust zijn.
92. Voor het risico van gegevensdeling hoeft het niet uit te maken of deze plaatsvindt in een incidentele of structurele samenwerking. Voor de inbreuk op de persoonlijke levenssfeer van een persoon maakt het immers geen verschil of zijn gegevens zijn gedeeld met een partij waarmee een enkele keer wordt samengewerkt of waarmee een meer duurzame samenwerkingsrelatie bestaat. Bepalend voor die inbreuk is vooral om welke partij het gaat en wat die partij met de (persoons)gegevens gaat doen.
93. Ten overvloede merken we op dat de waarborg van de weging verder aan betekenis inboet door het overgangsrecht dat in het wetsvoorstel is opgenomen. Hierin is bepaald dat voor bestaande samenwerkingsrelaties en -verbanden de weging op grond van de nieuwe wet met vijf jaar wordt uitgesteld en voor nieuwe samenwerkingsrelaties – en verbanden met twee jaar. Dus de plicht om vooraf af te wegen wat de risico's en geschiktheid van private partijen en hybride constructies zijn om persoonsgegevens mee te kunnen delen, hoeft pas in een beperkt aantal gevallen en op zijn vroegst twee jaar na inwerkingtreding van de wet plaats te vinden. Ondertussen is er geen

belemmering om dergelijke samenwerkingen al wel te laten plaatsvinden, met alle risico's van dien.

94. Andere waarborgen dan de weging bevat het wetsvoorstel niet. Weliswaar staat in alle bepalingen dat de minister toestemming voor de samenwerkingen moet geven, maar deze toestemming kan aan het diensthoofd of lager in de organisatie worden belegd. Ook voorziet het wetsvoorstel niet in bindende toetsing of toezicht.
95. Een belangrijk risico aan gegevensdeling bij samenwerking is dat gegevens van de diensten, denk aan staatsgeheime of gevoelige informatie, buiten het op de diensten toepasselijke wettelijke kader, nu het domein van de Wbnv, worden gebracht. Hiermee bedoelen we dat die informatie ter beschikking komt van organisaties en personen die niet gebonden zijn aan de wettelijke eisen die de toekomstige wet voor de inlichtingen- en veiligheidsdiensten stelt. De waarborgen die daarin staan, gelden niet. Die verstrekking brengt dan ook risico's met zich mee. Verstrekking betekent ook dat een en ander buiten het zicht van het CTT zal plaatsvinden.
96. Deze risico's hebben zich in de praktijk ook verwezenlijkt en kunnen verstrekkende gevolgen hebben. Als voorbeeld wijzen wij op de toezichtrapporten **nrs. 81** en **82** (nov. 2025) van de CTIVD over de zogeheten NCTV-casus.
97. Het is daarom belangrijk dat altijd vooraf zeer zorgvuldig wordt nagedacht over de manier waarop wordt samengewerkt en welke informatie met welke partijen moet en kan worden gedeeld. Bij die afweging moet ook in ogenschouw worden genomen dat door verstrekking van gegevens de diensten de controle over de staatsgeheime informatie en soms gevoelige (persoons)gegevens verliezen. Ontvangende partijen zijn vaak gebonden aan andere wetgeving die niet per definitie is toegespitst op dit soort informatie.
98. Door de voorgestelde systematiek wordt de kring van organisaties die kan gaan beschikken over 'informatie van de AIVD en/of de MIVD' zeer groot en ook zeer gefragmenteerd. Het gaat om heel verschillende soorten organisaties en partijen waarmee de diensten kunnen gaan samenwerken. Door de omvang van mogelijke samenwerkingspartners neemt het risico toe dat staatsgeheime informatie tot de beschikking komt van personen zonder dat daarvoor een concrete noodzaak bestaat (wat in strijd is met het *'need to know'*-principe).
99. Ook wordt het door het wetsvoorstel zeer complex voor de diensten om zicht te houden op welke gegevens met welke partijen worden gedeeld. Hierdoor hebben de diensten slechts beperkt zicht op wat deze partijen vervolgens met die gegevens doen. Dit roept de vraag op hoe de diensten invulling geven aan de zorgplicht die zij hebben op grond van het voorgestelde art. 23. De diensten moeten wel aantekening houden van de verstrekking van persoonsgegevens. Maar voor andere gegevens geldt die verplichting niet. De zorgplicht ziet op geheimhouding van alle daarvoor in aanmerking komende gegevens en strekt zich dus verder uit dan over persoonsgegevens alleen.
100. De samenwerkingsbepalingen leiden bovendien tot toezichtleemtes ('oversight gaps'). Het CTT kan geen zicht houden op gegevens die worden verstrekt als de diensten deze verstrekkingen niet vastleggen, nog afgezien van het feit dat dan het kwaad al geschied is. Ook heeft het CTT geen zicht op wat de ontvangende partij doet met de ontvangen informatie. Als de ontvangst en verdere verwerking door de ontvangende partij onderworpen is aan een ander wettelijk regime waarop toezicht wordt gehouden door een andere toezichthouder, betekent dit niet per definitie dat geen sprake is van reguleringstekorten en toezichtleemtes.
101. Hoewel de CTIVD en de TIB dus de noodzaak tot samenwerking en tot verstrekking van gegevens aan andere partijen zien, is het belangrijk dat die gegevensverstrekking slechts plaatsvindt als dat noodzakelijk is. Daarbij is het belangrijk dat voorafgaand aan een samenwerking zorgvuldig wordt afgewogen wat een noodzakelijke en passende samenwerking is met die andere partij gelet op de doelstellingen die de partij nastreeft en de context waarbinnen die partij opereert. De waarborgen die nu in de bepalingen over samenwerking en gegevensverstrekking zijn opgenomen voldoen daarvoor niet. Het wetsvoorstel zou meer mogelijkheden tot samenwerking tussen het CTT en toezichthouders op ontvangende partijen in zowel de publieke als de private sector moeten bieden en in bindend toezicht moeten voorzien.

102. Hierna volgt per categorie van samenwerking (met andere overheidsinstanties, met private partijen, met internationale diensten en militaire entiteiten) een specifieke toelichting van de risico's en tekortkomingen in het wetsvoorstel.

10.2 Samenwerking met andere overheidsinstanties

103. De kring van overheidsorganen en -instanties die voor de diensten werkzaamheden kunnen verrichten, waar de diensten samenwerkingsverbanden mee kunnen aangaan en die verplicht kunnen worden gegevens aan de diensten te verstrekken, wordt uitgebreid, met name ook voor de MIVD. In toezichtrapport **nr. 76** (feb. 2024) heeft de CTIVD al kritisch gerapporteerd over de manier waarop de diensten sturing geven aan en controle uitoefenen over de inlichtingendiensten van de politie en de KMar. De CTIVD en de TIB maken zich zorgen over de aansturing en controle vanuit de diensten over deze werkzaamheden die in de loop van de tijd alleen maar zullen toenemen. Daarbij komt dat niet wordt voorzien in bindend toezicht door het CTT.
104. In art. 126 (AIVD) en art. 128 (MIVD) van het wetsvoorstel staat een grote groep (voornamelijk civiele) overheidsorganen/-instanties genoemd die (structureel) werkzaamheden verrichten ten behoeve van de beide diensten (hiervoor worden medewerkers van deze instanties aangewezen door de betrokken minister; dit is niet uitgezonderd in de mandaatverlening van art. 27 lid 2/3). Voor de MIVD is dit grotendeels nieuw omdat de Wiv 2017 dit alleen regelt met betrekking tot de KMar. Op dit punt wordt de MIVD gelijkgetrokken met de AIVD zonder dat hiervoor duidelijke argumentatie wordt gegeven, anders dan een algemene verwijzing naar de veranderde geopolitieke situatie en de toegenomen dreiging. De groep van overheidsorganen/-instanties kan ook nog bij AMvB worden uitgebreid. Het parlement wordt hiervan op de hoogte gesteld.
105. Met dit wetsvoorstel wordt de kring van overheidsorganen en -instanties waaraan de diensten sturing moeten geven aanzienlijk groter. Ook vindt een uitbreiding plaats voor de MIVD ten aanzien van voornamelijk civiele instanties. Daardoor neemt het risico op samenloop/vermenging tussen de werkzaamheden voor de AIVD en de MIVD toe, waar dit eerder niet gebeurde omdat dit niet passend was gelet op de verschillen tussen het civiele en het militaire domein. De aansturing en controle vanuit die diensten aan de (voornamelijk civiele) instanties wordt dan steeds belangrijker, maar hierin schuilen serieuze risico's, zoals wij in toezichtrapport **nr. 76** (feb. 2024) al constateerden, omdat de diensten op afstand staan en de instanties steeds meer verzelfstandigen in hun taakuitvoering.
106. Naast deze vormen van structurele samenwerking, die voor de MIVD grotendeels nieuw zijn, voorziet het wetsvoorstel ook al in andere vormen van samenwerking, zoals op incidentele basis of in hybride verbanden. Wij wijzen bijvoorbeeld op art. 136 op basis waarvan de krijgsmacht en andere defensieonderdelen zoals de KMar, desgevraagd incidentele ondersteuning kunnen verlenen aan de MIVD, dus zonder dat dit een structureel karakter heeft en hiervoor ambtenaren (door de minister) moeten worden aangewezen. Deze ondersteuning kan in ieder geval bestaan uit het verlenen van technische en andere vormen van ondersteuning en het in gezamenlijkheid ontwikkelen van technische- en analysecapaciteiten. Op grond van art. 137 kan de MIVD deze vormen van ondersteuning omgekeerd ook leveren aan de krijgsmacht en andere defensieonderdelen zoals de KMar.
107. Ook kunnen beide diensten samenwerkingsverbanden met meerdere (voornamelijk civiele) overheidsorganen/-instanties aangaan waarbij gegevens van de diensten worden gedeeld. Deze grondslagen zijn nieuw (art. 127: AIVD en 129: MIVD). Ook hier kan de groep van instanties bij AMvB worden uitgebreid.
108. Daarnaast kunnen meer overheidsinstanties worden verplicht gegevens te delen met de diensten. Dit staat in art. 132. Hoewel dit al bestaat in art. 94 Wiv 2017, zijn er organisaties toegevoegd (IND, DJI, NCSC en FIU) en wordt ook een grondslag toegevoegd om bij AMvB andere overheidsorganisaties aan te wijzen die gegevens moeten leveren aan de diensten.

10.3 Verstrekking van onbewerkte gegevens aan de krijgsmacht en defensieonderdelen

109. Verder vragen we aandacht voor de verstrekking van gegevens aan de krijgsmacht en defensieonderdelen. Deze mogelijkheid is in het voorgestelde art. 116 zeer ruim geformuleerd. De verstrekking vindt plaats direct na het verzamelen van de gegevens door de AIVD of de MIVD, zonder verdere verwerking of duiding door de dienst. Het gaat dus om ruwe, onbewerkte, gegevens. Het ongezien en zonder duiding verstrekken van gegevens houdt risico's in. Hierbij moet de minister van BZK of Defensie de afweging maken of er gezien de taakuitvoering van de diensten een noodzaak is voor de directe verstrekking aan de krijgsmacht of een ander defensieonderdeel.
110. Een algemeen risico hierbij is dat door verstrekking aan de krijgsmacht of andere defensieonderdelen dergelijke gegevens buiten het domein van de Wbnv worden gebracht en mogelijk kunnen worden gebruikt voor doeleinden waarvoor deze niet zijn verkregen. Het gaat hier immers wel om instanties met handelingsbevoegdheid. Er staat dat de betrokken minister, die verantwoordelijk is voor de AIVD of de MIVD, toestemming moet geven voor de verstrekking. Dat lijkt bij zo'n risicovolle verstrekking een belangrijke waarborg, maar nu deze bepaling niet is uitgezonderd bij de in het wetsvoorstel voorgestelde ruime mandateringsmogelijkheid (art. 27 lid 2 en 3), staat het de minister(s) vrij ervoor te kiezen de toestemming bij het diensthoofd te beleggen of zelfs te beslissen dat toestemming ook lager in de dienstorganisatie kan plaatsvinden (ondermandatering; art. 31).
111. De directe verstrekking kan ook zien op bulkgegevens (art. 116 lid 2). Bij bulkgegevens gelden twee vereisten: 'de verstrekking [vindt] alleen plaats als sprake is van zwaarwegende noodzaak en voor zover die de gereedstelling, gereedheid en inzet van de krijgsmacht, bedoeld in art. 3, tweede lid en onder a, b en c, aangaat'. Op basis van deze formulering in de wet is niet direct duidelijk voor wie die zwaarwegende noodzaak er moet zijn en ook niet waar het woordje 'die' bij het tweede vereiste betrekking op heeft. Ook hier speelt de vraag of deze ruime vorm van verstrekking noodzakelijk is. Bij bulkgegevens gaat het immers om grote hoeveelheden gegevens waarbij het merendeel van de gegevens betrekking heeft op personen die niet onder de aandacht van de diensten staan. Geautomatiseerde verstrekking van volledige (bulk)datasets aan de krijgsmacht zou niet mogelijk moeten zijn. De inbreng van de CTIVD en de TIB in de voorbereidingsfase van het wetsvoorstel heeft ertoe geleid dat de verstrekking van bulkgegevens in ieder geval beperkt moet blijven tot de taakuitvoering van de MIVD (art. 116 lid 2; taken in art. 3 lid 2 onder a, b en c), en niet ook tot de taakuitvoering van de AIVD zoals eerder opgenomen. Dat geldt nog wel voor de verstrekking op grond van het eerste lid. Ook is een meldplicht van een verstrekking van bulkgegevens aan het CTT toegevoegd. Er wordt niet voorzien in bindend toezicht van het CTT, hetgeen wel geëigend is. Ook kan de toestemming van de minister door hem worden gemandateerd aan het diensthoofd (art. 27) dan wel worden ondergemandateerd aan iemand lager in de organisatie (art. 31).

10.4 Publiek-private samenwerking

112. Nieuw in het wetsvoorstel zijn grondslagen voor bilaterale en multilaterale samenwerking van de AIVD en de MIVD met private partijen, in art. 144 resp. art. 145. De risico's van samenwerking met private partijen, bijvoorbeeld buitenlandse commerciële bedrijven, worden in de visie van de CTIVD en de TIB onvoldoende belicht en worden in de wettelijke weging niet afgedekt door de opgenomen criteria als doelstelling, professionaliteit en betrouwbaarheid van de partij. Een belangrijk risico betreft het buiten domein van de Wbnv brengen van inlichtingen en persoonsgegevens en het buiten de controle en zicht van de AIVD of de MIVD gebruiken van deze gegevens voor andere doeleinden dan het belang van nationale veiligheid.

113. Voor het aangaan van bilaterale en multilaterale samenwerking met private partijen is niet vereist dat dit plaatsvindt in het kader van de taakuitvoering van de dienst(en). De samenwerking kan verschillende (vergaande) vormen aannemen, zoals in lid 2 wordt benoemd, te weten de uitwisseling van gegevens, gezamenlijke analyse van gegevens en wederzijdse technische of operationele ondersteuning. Een weging van de risico's en de noodzaak van de samenwerking hoeft alleen plaats te vinden als de samenwerking beoogd wordt structureel van aard te zijn én voorzien wordt dat persoonsgegevens door de dienst verstrekt zullen worden (dus niet bij andere gegevens of andere activiteiten of het ontvangen van gegevens). De kring van private partijen is onbeperkt, dus ook buitenlandse bedrijven kunnen eronder vallen. Daarbij komt dat de toestemming van de minister niet is uitgesloten van (onder)mandatering op grond van art. 27 lid 2/3.

10.5 Internationale samenwerking

114. Bij samenwerking met internationale partijen zien de CTIVD en de TIB in het wetsvoorstel uitbreidingen die risico's met zich meebrengen en niet voorzien zijn van voldoende waarborgen.
115. Het wetsvoorstel bevat een grondslag voor bilaterale samenwerking (art. 138) als ook (nieuw) voor multilaterale samenwerking (art. 139), dus met meer dan één partij tegelijkertijd. Op zich gebeurt dit nu ook al, dus de voorzienbaarheid vereist dat het wetsvoorstel hier een grondslag voor creëert. De CTIVD heeft hierop in toezichtrapport **nr. 73** (okt. 2021) over de samenwerking met buitenlandse diensten met een verhoogd risicoprofiel ook gewezen. Dit betreft het voorzien in een zelfstandige weging van de risico's van een multilateraal samenwerkingsverband. Het wetsvoorstel voorziet in weging van samenwerkingen die worden vastgelegd in wegingsnotities (bilateraal) of overzichtsnotities (multilateraal). Ten opzichte van de Wiv 2017 wordt dit voor zowel bilaterale relaties als multilaterale verbanden beperkt tot het geval dat de relatie of het verband structureel zal zijn én voorzien wordt dat *persoons*gegevens zullen worden gedeeld. Deze beperkingen beogen de situaties waarin wegings- of overzichtsnotities moeten worden opgesteld te verminderen, terwijl een weging van de risico's voor het aangaan en onderhouden van dit soort relaties juist belangrijk is om te bepalen of en zo ja, in hoeverre kan worden samengewerkt en onder welke voorwaarden, bijv. mitigerende maatregelen, dit moet plaatsvinden.
116. Het wetsvoorstel doet het in deze bepalingen (art. 138 lid 5 en art. 139 lid 5) ook voorkomen dat de minister van BZK (AIVD) of Defensie (MIVD) toestemming moet geven voor het aangaan van een bilaterale relatie dan wel het oprichten/deelnemen aan een multilateraal verband. Toch is dat niet per se het geval. Nu deze bepalingen niet zijn uitgezonderd bij de in het wetsvoorstel voorgestelde ruime mandateringsmogelijkheid (art. 27 lid 2 en 3), staat het de minister(s) vrij ervoor te kiezen de toestemming bij het diensthoofd te beleggen of zelfs te beslissen dat toestemming ook lager in de dienstorganisatie kan plaatsvinden (ondermandatering; art. 31). Zeker bij samenwerkingen met buitenlandse diensten met een verhoogd risicoprofiel als ook bij (bepaalde) samenwerkingsverbanden met meerdere buitenlandse partijen waar intensief gegevens worden gedeeld of ondersteuning aan elkaar wordt verleend, is de vraag of afwezigheid van ministeriële betrokkenheid wenselijk is.
117. Hier wordt ook opgemerkt dat de scope van deze bepalingen groter is geworden. In het wetsvoorstel staat dat beide diensten bilaterale en multilaterale relaties aangaan met 'buitenlandse inlichtingen- en veiligheidsdiensten'. Dit heeft een ruimere reikwijdte dan het in de Wiv 2017 gangbare 'inlichtingen- en veiligheidsdiensten van andere landen'. Voor de MIVD wordt de scope nog groter door te bepalen dat deze dienst ook bilaterale relaties en multilaterale verbanden mag oprichten of eraan deelnemen met buitenlandse militaire inlichtingen- en veiligheids*entiteiten*. Volgens de memorie van toelichting is gekozen voor het begrip 'buitenlandse inlichtingen- en veiligheidsdiensten' in plaats van "inlichtingen- en veiligheidsdiensten van andere landen", zoals in art. 88 Wiv 2017, om de samenwerkingsgrondslag en bijbehorend waarborgenkader voor

meer partijen van toepassing te verklaren. Ook buitenlandse militaire inlichtingendiensten en SIGINT-diensten vallen onder het begrip buitenlandse inlichtingen- en veiligheidsdienst. Met deze wijziging wordt beoogd buiten twijfel te stellen dat de diensten onder de juiste voorwaarden kunnen samenwerken met entiteiten met overeenkomstige taken, waaronder ook niet-erkende staten of groeperingen die niet als vertegenwoordiger van een staat zijn erkend, maar die wel bepaalde statelijke activiteiten uitoefenen. Voor de MIVD in het bijzonder is er daarom voor gekozen de term militaire inlichtingen- en veiligheidsentiteiten expliciet in dit artikel op te nemen, om betere aansluiting te vinden bij de militaire praktijk, waaronder missieondersteuning. De CTIVD heeft er eerder voor gepleit dat een grondslag wordt opgenomen voor de samenwerking met niet-statelijke actoren die inlichtingen- en veiligheidstaken uitvoeren, maar daarbij dan wel te voorzien in een passend waarborgenkader. De voorgestelde terminologie is naar onze opvatting te ruim gesteld en de waarborgen onvoldoende, nu de toestemming van de minister ten aanzien van gevoelige onderdelen (denk aan samenwerking met risicodiensten of niet-statelijke actoren) niet van mandatering is uitgezonderd, er een oneigenlijke drempelwaarde wordt ingericht voor het opstellen van wegingsnotities, en er geen bindend toezicht ten aanzien van gevoelige onderdelen is voorzien.

118. Op basis van art. 140 mogen de diensten in een bilaterale of multilaterale samenwerking met buitenlandse diensten (art. 138 resp. art. 140) gegevens uitwisselen (lid 1 onder a). Hierbij is niet meer vereist dat dit plaatsvindt in het kader van de taakuitvoering van de AIVD of de MIVD. Deze verwijdering is vreemd nu lid 1 onder b erin voorziet dat de AIVD of de MIVD, gegevens mogen verstrekken ten behoeve van door de buitenlandse dienst te behartigen belangen, tenzij deze belangen onverenigbaar zijn met de door de dienst te behartigen belangen of de taakuitvoering van de dienst zich tegen verstrekking verzet. Onder deze bevoegdheid tot gegevensuitwisseling valt ook het verstrekken en ontvangen van bulkgegevens. De memorie van toelichting (p. 82) licht toe dat het kan gaan om bijzondere bulkgegevens verzameld met bulkinterceptie. Een voorbeeld van internationale samenwerking bij bulkinterceptie is een bi- of multilateraal samenwerkingsverband waarbij het gezamenlijke belang is om onderzoek te kunnen doen naar een specifieke buitenlandse statelijke actor. In het samenwerkingsverband kan afgesproken worden dat een dienst specifieke gegevensstromen met bulkinterceptie verzamelt en verstrekt, en vervolgens bulkgegevens weer ontvangt van de andere diensten. Zo kan samengewerkt worden zodat de AIVD en de MIVD kunnen beschikken over noodzakelijke bulkgegevens, die zij bijvoorbeeld vanwege de geografische ligging van Nederland of om andere redenen niet zelfstandig kunnen verzamelen. De memorie van toelichting wijst erop dat uit de weging moet blijken dat de verstrekking van bulkgegevens kan plaatsvinden. De weging moet volgens de wet plaatsvinden als een samenwerking structureel van aard zal zijn en persoonsgegevens gedeeld zullen worden. De vraag is of die weging in voldoende mate ziet op de risico's van bulkgegevens, waarvan de diensten niet precies weten wat voor gegevens ze verstrekken. Lid 2 vereist verder dat de minister voor de verstrekking van bulk toestemming geeft, al kan dat voor de duur van een jaar voor opeenvolgende verstrekkingen van gelijksoortige aard plaatsvinden. Ook is de toestemming van de minister niet uitgezonderd van mandatering op grond van art. 27 lid 2/3 en ondermandatering in art. 31. Alleen als de dienst(en) vanwege een zwaarwegende noodzaak gegevens willen verstrekken aan een buitenlandse dienst of entiteit waarmee geen samenwerkingsrelatie bestaat (art. 138), of de weging van de relatie (art. 138 lid 3) of het samenwerkingsverband (art. 139 lid 3) geen ruimte laat voor de verstrekking van dergelijke gegevens, kan dit toch plaatsvinden met toestemming van de minister. Deze toestemming kan op grond van art. 27 lid 2 *niet* worden gemandateerd aan het diensthoofd.

119. Op grond van art. 146 mogen de AIVD en de MIVD zelfs gemixte nationale en internationale multilaterale samenwerkingsverbanden oprichten en eraan deelnemen, bestaande uit een mix van nationale overheidsorganen en overheidsinstanties, buitenlandse inlichtingen- of veiligheidsdiensten (138 lid 1 of 139 lid 1) en nationale of buitenlandse private partijen (art.144 lid 1 of 145 lid 1). Hierbij kunnen vergaande samenwerkingsactiviteiten plaatsvinden,

zoals gegevensuitwisseling, gezamenlijke analyse van gegevens en wederzijdse technische of operationele ondersteuning. Daarnaast is de MIVD nog bevoegd tot het oprichten van of deelnemen aan samenwerkingsverbanden met een mix van buitenlandse militaire inlichtingen- en veiligheidsentiteiten (138 lid 2 of 139 lid2) en de krijgsmacht en andere defensieonderdelen. Ook de toestemmingsbevoegdheid van de minister hiervoor kan worden (onder)gemandateerd.

10.6 Overgangsrecht

120. Het wetsvoorstel regelt ook overgangsrecht ten aanzien van samenwerking (art. 242). Dit beoogt na inwerkingtreding van de nieuwe wet een vloeiende overgang van de nieuwe regels naar de praktijk te bewerkstellingen. Dit resulteert erin dat de verplichting tot het uitvoeren van een weging voor al bestaande bilaterale relaties (opstellen wegingsnotitie op grond van art. 138 lid 3) of voor reeds bestaande multilaterale verbanden (opstellen overzichtsnotitie op grond van art. 139 lid 3) na inwerkingtreding van de wet met vijf jaar wordt uitgesteld. Mogelijk kan deze beperking aan waarde worden ondervangen doordat in de memorie van toelichting staat dat gedurende deze vijf jaar het diensthoofd er zorg voor draagt dat als omstandigheden daartoe aanleiding geven de deelname aan een samenwerkingsrelatie of -verband geheel of gedeeltelijk opnieuw wordt gewogen of dat een overzichtsnotitie wordt opgesteld (art. 138 lid 6 en art. 139 lid 6). Risicovol vinden wij het tweede deel van het overgangsrecht in art. 242 op grond waarvan de nieuw voorgestelde wegingsnotities en overzichtsnotities voor publiek-, private en multilaterale samenwerking, bedoeld in de art. 144 lid 3, 145 lid 3 en art. 146 lid 3, pas voor het eerst uiterlijk twee jaar na inwerkingtreding van de wet worden opgesteld. Dit betekent dat twee jaar van de bevoegdheid gebruik mag worden gemaakt voordat de bijbehorende waarborgen in werking treden. Een dergelijk lange overgangstermijn vinden de CTIVD en de TIB onwenselijk. Juist bij een nieuwe bevoegdheid moeten de diensten behoudend te werk gaan.

D. Stelsel van compliance, audit, toetsing, toezicht, klacht en misstanden

11. Compliance en audit

11.1 Wettelijke grondslag

121. De CTIVD en de TIB onderschrijven de noodzaak en het belang van interne controle en toetsing binnen de beide diensten. Dit kan vorm krijgen via compliance en auditfunctionaliteiten. Het is een belangrijke eerste stap dat beide functionaliteiten in het wetsvoorstel een wettelijke verankering krijgen (art. 14).

11.2 Onafhankelijke inbedding en borging taakuitvoering in de wet en praktijk

122. Dit laat onverlet dat het wetsvoorstel en de toelichting daarop weinig houvast bieden voor de inrichting en taakuitvoering hiervan. Met de wettelijke verankering van de compliance- en auditfuncties is een eerste stap gezet, maar de wet dient ook vast te leggen dat die functies daadwerkelijk met impact, effectief en onafhankelijk hun rol binnen de diensten kunnen spelen. Zeker met een wet die de bevoegdheden van de diensten vergroot, is een versterking van deze interne waarborgen noodzakelijk. De CTIVD en de TIB constateren dat de diensten na de inwerkingtreding van de huidige Wiv 2017, waarin een zorgplicht is opgenomen voor een zorgvuldige en rechtmatige gegevensverwerking, aanzienlijke stappen hebben gezet op het gebied van het inrichten dan wel professionaliseren van de compliance en auditfuncties. Desondanks wijst de huidige toezichtpraktijk ook uit dat de beide organisaties nog flinke stappen te zetten hebben op dit gebied, met name ten aanzien van de onafhankelijke inbedding en taakuitvoering van deze functionaliteiten. Ook wijzen wij erop dat deze functionaliteiten niet alleen een wettelijke grondslag moeten hebben, maar daarnaast een specifieke controlerende rol moeten krijgen bij de uitvoering van de taken van de diensten. Het wetsvoorstel bedeelt op veel punten een grote(re) rol toe aan interne toestemmingsverlening en controle, maar regelt geen expliciete rol voor de compliance en auditfunctionaliteiten. Daarbij tekenen wij ook aan dat goed intern toezicht weliswaar een voorwaarde vormt voor een volwassen organisatie en voor goed extern toezicht, maar dat dit geen substituut vormt voor externe toetsing en toezicht. Nu is in het wetsvoorstel een tendens waarneembaar van het afschalen van externe toetsing en toezicht ten behoeve van interne toestemmingsverlening en controle, alsof het inwisselbare grootheden betreft.

12. CTT: toetsing, toezicht, klacht en misstanden

123. De betrokkenheid en inbreng van de CTIVD en de TIB in de voorbereidingsfase van het wetstraject heeft tot een aantal veranderingen in het wetsvoorstel geleid waardoor de positie van de toezichthouder is versterkt in vergelijking tot eerdere conceptteksten. Dit laat onverlet dat op een aantal fundamentele punten de positie van de toezichthouder nog onvoldoende stevig is. We geven eerst een overzicht van de door ons bereikte verbeteringen. Daarna gaan we in op de fundamentele punten die nog aandacht behoeven.

12.1 Enkele positieve elementen

124. De CTIVD en de TIB hebben al eerder hun voorkeur uitgesproken voor de oprichting van een nieuw, onafhankelijk toezichthoudende instantie waarin de functies van toets, toezicht en klachtbehandeling worden geïntegreerd. Het 'één-toezichthoudermodel' draagt bij aan de noodzakelijke verdere professionalisering van het stelsel van toetsing en toezicht. Dit maakt het mogelijk de ex ante toetsing en het toezicht effectief op elkaar af te stemmen. Hierdoor kan beter worden ingespeeld op nieuwe ontwikkelingen en risico's in de dynamische operationele praktijk van de inlichtingen- en veiligheidsdiensten en een normatief kader voor de gehele keten worden opgesteld. In het wetsvoorstel is deze aanbeveling overgenomen. Het wetsvoorstel creëert een nieuwe toezichthouder, te weten het College van Toetsing en Toezicht (CTT) (art. 160). In het CTT worden zowel het ex ante toetsen van bepaalde activiteiten van de diensten, het houden van toezicht op de naleving van wet- en regelgeving en het behandelen van klachten en vermoedens van misstanden over de diensten belegd. Dit laat onverlet dat de voorgestelde inrichting van het CTT de beoogde synergie van het samenbrengen van toetsing en toezicht geheel tenietdoet. Hier komen wij later op terug.
125. Ook de onafhankelijkheid van het CTT wordt nu in de wet zelf verankerd (art. 160 lid 5). De onafhankelijkheid van het CTT komt, net als het geval is bij de CTIVD en de TIB, onder meer tot uiting in de benoemingsprocedure voor de leden van het CTT en de limitatieve regeling van ontslag- en schorsingsgronden. Op ons initiatief wordt het CTT direct betrokken in de benoemingsprocedure voor haar eigen (plv.) leden. Nieuw is ook dat een herbenoemingsprocedure is opgenomen.
126. In het wetsvoorstel is verder een consultatierecht voor het CTT verankerd ten aanzien van elke wijziging van de WBNV, Wvo of toepasselijke regelgeving. De CTIVD en de TIB hebben hier al langere tijd op aangedrongen, mede naar aanleiding van de wijziging en ratificatie van Conventie 108+, waarin voor nationale toezichthoudende instanties een consultatierecht over wetswijzigingen is opgenomen.

12.2 Fundamentele tekortkomingen bij regeling CTT

127. Voorgaande positieve elementen in het wetsvoorstel ten aanzien van het CTT laten onverlet dat op een aantal wezenlijke punten niet wordt voorzien in voldoende ruimte voor de toezichthouder om op een robuuste en slagvaardige manier het toezicht in te richten en uit te oefenen. De wendbaarheid en slagkracht die voor de diensten in het voorstel zijn opgenomen moeten onverkort ook voor het toezicht gelden. In het wetsvoorstel is echter een aantal keuzes gemaakt dat hieraan in de weg staat.

12.3 Scheiding tussen toetsing en toezicht binnen het CTT

128. Een belangrijk punt betreft de inrichting van het CTT (art. 164). In het wetsvoorstel wordt de interne communicatie en besluitvorming binnen het CTT uitgesloten op het niveau van werkzaamheden van de afdeling toetsing en toezicht. Waar in het wetsvoorstel veel verruiming wordt geboden aan de inrichting binnen de diensten, valt op dat de inrichting van de toezichthouder zeer precies en zeer beperkt wordt gedefinieerd. De CTIVD en de TIB gaan weliswaar op in één organisatie, maar de werkzaamheden binnen het CTT zijn organisatorisch gescheiden. Er lijkt bij de regering een zorg te bestaan dat de toetsing een te ruime toepassing krijgt en informatie van de afdeling toezicht in haar oordelen betrekt.
129. De CTIVD en de TIB zijn voorstander van een structuur waarbij er geen restricties zijn om op bestuursniveau complexere zaken te besluiten en waarbij informatiedeling tussen de afdeling wordt verruimd. Toetsing en toezicht vormen immers één keten, waarbij de ex ante toetsing en het ex durante/post toezicht in het verlengde van elkaar liggen en, gezien de dynamische en flexibele operationele praktijk van de diensten, communicerende vaten vormen. De synergie die beoogd wordt met het samenbrengen van toetsing en toezicht in één organisatie moet daarom ook in de praktijk een effectieve toepassing kunnen krijgen. Hiervoor is vereist dat er informatiedeling tussen toezicht en toetsing kan plaatsvinden en dat complexe toetsingskwesties naar een hoger (bestuurs)niveau binnen het CTT kan worden opgeschaald.
130. De besluitvorming in complexe zaken, die op bestuursniveau gewenst is, zal slechts in een beperkt percentage van de ex ante toetsing plaatsvinden, maar het is noodzakelijk dat hiervoor geen belemmeringen worden opgeworpen.
131. Bovendien kent het voorstel al verschillende waarborgen om zorgen over een te ruime toetsing te ondervangen:
    - Toetsing vindt slechts plaats op basis van het toestemmingsverzoek en eventueel van de diensten afkomstige aanvullende informatie
    - Toetsing is gebonden aan wettelijke termijnen
    - Tegen het bindend oordeel van afdeling toets voor de betrokken minister(s) staat beroep open bij de afdeling bestuursrechtspraak van de Raad van State, waarbij ook het toestemmingsverzoek leidend is.
132. Het wetsvoorstel regelt dat de voorzitter van het CTT tevens lid van de afdeling toezicht is. De CTIVD en de TIB zijn van oordeel dat het CTT zelf over de inrichting van het bestuur moet gaan. In de wet kan worden volstaan te bepalen dat de CTT een voorzitter heeft.
133. De positie van de afdeling klacht binnen het CTT is onvoldoende geregeld. Art. 160 biedt geen uitzicht op de positie van de afdeling klachtbehandeling voor zaken die wél het functioneren van die afdeling betreffen als de afdeling geen onderdeel uitmaakt van het bestuur. De memorie van toelichting laat het bij die enkele constatering en biedt ook geen waarborgen.

12.4 Beslistermijnen en medewerkingsplicht

134. Opvallend is dat de beslistermijnen voor toetsing in art. 48 van het wetsvoorstel uitdrukkelijk zijn bepaald op twee weken. Die termijn is onnodig belastend en zelfs contraproductief volgens de CTIVD en de TIB. In de huidige dagelijkse praktijk wordt in meer dan 90% van de gevallen een beslissing binnen die termijn genomen. Maar als dit een eis zal worden voor alle beslissingen, zal het wellicht nodig zijn om de ‘moeilijkste’ gevallen als eerste te beoordelen met als gevolg dat de ‘eenvoudiger’ gevallen langer op een beslissing moeten wachten. Dit onbedoelde effect zal dus mogelijk een vertragend effect op de keten van beoordeling hebben. De CTIVD en de TIB zijn een voorstander van het opnemen van een generieke termijn, bijvoorbeeld ‘zo spoedig mogelijk’ als termijn bij de beoordeling.

135. In art. 48, 57, 180 en 181 wordt bepaald dat de inlichtingen worden verstrekt en alle overige medewerking wordt verleend voor zover dat voor de afdeling toetsing, afdeling toezicht of van afdeling klachtbehandeling van het CTT redelijkerwijs noodzakelijk is. Dat roept de vraag op wie bepaalt wanneer inlichtingen redelijkerwijs noodzakelijk zijn voor het vormen van een oordeel door het CTT. Het CTT dient zelf degene te zijn om dit te beoordelen, terwijl de huidige tekst de beoordeling hiervan bij de minister of het diensthoofd legt. Deze beperking is in de visie van de CTIVD en de TIB ongewenst en onnodig beperkend. In het uiterste geval zou de minister of het diensthoofd kunnen weigeren gevraagde inlichtingen te verstrekken, terwijl de afdeling toetsing of de afdeling klachtbehandeling wel tot een oordeel moeten komen over de casus die voorligt en dat ook nog binnen een voorgeschreven termijn.

12.5 Bindend toezicht CTT

136. De ex ante toetsing van het CTT wordt in aanzienlijk minder situaties voorgeschreven dan nu in de Wiv 2017 en de Tijdelijke wet het geval is (art. 47).
137. Een ander elementair punt in het wetsvoorstel betreft de regeling van bindend toezicht. Dit is de mogelijkheid tot het opleggen van bindende oordelen en maatregelen. Het wetsvoorstel voorziet hier slechts zeer beperkt in (art. 188 lid 1). De CTIVD en de TIB blijven van mening dat dit een interventiemogelijkheid is die noodzakelijk is om enigszins evenwicht te bieden aan de vergaande verruiming van mogelijkheden die de diensten krijgen op grond van het wetsvoorstel. Hierbij tekenen wij nadrukkelijk aan dat bindend toezicht geen oplossing vormt voor de algehele verruiming van de taken en bevoegdheden van de diensten die in het wetsvoorstel wordt beoogd. Wij zijn van mening dat de voorgestelde verruiming over de gehele linie van het wetsvoorstel zonder adequate democratische waarborgen te ver gaat en dat ook in andere waarborgen, zoals striktere toestemmingsvereisten, kortere bewaartermijnen en datareductie, moet worden voorzien. Dat laat onverlet dat bindend toezicht een belangrijke waarborg vormt in het stelsel van *checks and balances*.
138. Nu wordt dit voor de afdeling toezicht van het CTT slechts voorzien in vijf gevallen: gedeeltelijk verbod volledige automatisering (art. 36), liëren van personen aan aangewezen organisaties in het opponentenregime (art. 58 lid 4), hacken voor zover het betreft het binnendringen in een geautomatiseerd werk door tussenkomst van het werk van een derde (art. 76 lid 1), bewaartermijn bulkgegevens (art. 105), aanwijzen bulkdatasets in AMvB (art. 107). Het is voor ons niet inzichtelijk op welke gronden deze gevallen wel van bindend toezicht zijn voorzien en andere gevallen niet. Dit zijn ook andere bevoegdheden dan nu voorzien in art. 12 van de Tijdelijke wet cyberonderzoeken en bulkdatasets, waarin naast verkennen en technische risico's bij de hackbevoegdheid, GDA op metadata uit OOG-interceptie en het vaststellen van een nieuwe bewaartermijn voor bulkdatasets, ook bindend toezicht is geregeld voor bijschrijven bij hacken, tappen en opvragen gegevens bij providers.
139. Tezamen vindt een vermindering van ex ante toetsing en toezicht plaats.
140. Bovendien is de mogelijkheid om een bindend oordeel te geven ook nog geclausuleerd geformuleerd in art. 188, vijfde lid waardoor het oordeel van het CTT in een individuele casus naar inschatting van de CTIVD en de TIB niet langer kan worden gezien als *effective remedy* (effectief rechtsmiddel) in de zin van art. 13 EVRM en de jurisprudentie van het Europees Hof voor de Rechten van de Mens tegen niet rechtmatig handelen van de diensten. Los daarvan leidt de beperking om daadwerkelijk gevolgen te verbinden aan een onrechtmatigheidsoordeel tot de onwenselijke situatie dat aanbeveling tot herstel van een onrechtmatige situatie niet meer onlosmakelijk een gevolg is van onrechtmatig handelen van de diensten. Wij zijn van mening dat een clausulering als art. 188 lid 5 niet in de wet zou moeten worden opgenomen.

12.6 Rechtstreekse communicatie CTT met parlement

141. Een belangrijk onderdeel van de onafhankelijkheid vinden wij ook dat het CTT zelfstandig, op een door haar gekozen moment, zonder tussenkomst van de betrokken minister(s), kan communiceren met het parlement. Het wetsvoorstel voorziet hier niet in, slechts als de minister nalatig is om een vastgestelde rapportage van het CTT binnen de voorgeschreven termijn door te sturen naar het parlement (art. 186 lid 5). Dit zogenoemde noodventiel bij een 'weigerachtige' minister is een verandering ten opzichte van de huidige Wiv 2017, waarin dit niet is geregeld, maar deze voorziening voorziet niet in de mogelijkheid van zelfstandige communicatie met het parlement. Het uitgangspunt in het wetsvoorstel blijft verzending door tussenkomst van de minister(s) met een beroep op de ministeriële verantwoordelijkheid.
142. De CTIVD en de TIB vinden het in het kader van goed, effectief en onafhankelijk toezicht van belang om rechtstreeks te kunnen communiceren met het parlement. Dit sluit ook aan bij wat gangbaar is in het bredere toezichtdomein. Ook sluit het aan bij de toenemende dynamische operationele praktijk van de diensten dat meer flexibiliteit en wendbaarheid vergt voor de diensten in wettelijke processen. De CTIVD en de TIB vinden het met het oog op de onafhankelijkheid van het CTT in dat kader van belang dat de besluitvorming over het moment van verzending van toezichtproducten aan de Tweede Kamer en/op de CIVD uiteindelijk bij het CTT ligt en niet bij de minister(s), zoals nu in het wetsvoorstel in art. 186 en 187 staat.
143. De CTIVD en de TIB menen dat ministeriële verantwoordelijkheid niet in de weg staat aan rechtstreekse communicatie van het CTT met het parlement. Immers het uitgangspunt hierbij blijft de borging van vereisten als procedurele voorzienbaarheid en hoor en wederhoor. Hieraan kan ook in een praktijk van rechtstreekse verzending aan het parlement invulling worden gegeven. Als de minister(s) tijdig op de hoogte wordt gesteld van de inhoud van bevindingen en oordelen en in de gelegenheid wordt gesteld hierop te reageren, blijven de minister conform hun verantwoordelijkheid in staat een reactie te geven op eventuele feitelijke onjuistheden en een controle te verrichten op de aanwezigheid van eventuele staatsgeheime informatie die niet in de openbaarheid gedeeld kan worden met het parlement dan wel eventueel informatie die vanwege het belang van de staat op grond van art. 68 Grondwet volgens de minister ook niet vertrouwelijk gedeeld kan worden met de CIVD, die juist voor dat doel door de Tweede Kamer in het leven is geroepen. Ook worden de ministers door het CTT tijdig op de hoogte gebracht van het moment van verzending aan het parlement in verband met hun beschikbaarheid en het tijdig kunnen voorbereiden en het tegelijkertijd kunnen toesturen van hun beleidsreactie. De ministeriële verantwoordelijkheid kan op deze wijze (feitelijk) geborgd en nageleefd worden en kan naar het oordeel van de CTIVD en de TIB daarom niet in de weg staan aan het belang van rechtstreekse communicatie van het CTT met het parlement.

12.7 Onafhankelijk budget en voldoende middelen en mensen

144. Het is belangrijk dat het CTT zal beschikken over een onafhankelijk budget, waarbij de mensen en middelen van de toezichthouder gelijke tred houden met de groei van de diensten. Ook de toename van de benodigde toezichtactiviteiten gezien de grote uitbreiding van de mogelijkheden van de diensten in het wetsvoorstel dient hierbij in ogenschouw te worden genomen. Daar wordt nu niet in voorzien.

12.8 Regeling kennisneming gegevens bij CTT

145. Nieuw in het wetsvoorstel is een inzageregeling voor gegevens die door het CTT zijn verwerkt, anders dan gegevens die door de diensten zijn verwerkt en op grond van de toetsingstaak (art. 48) dan wel de toezichttaak (art. 180 en 181) aan het CTT zijn verstrekt (art. 177). De CTIVD en de TIB hebben bezwaren tegen deze regeling, ondanks dat zij transparantie en het afleggen van verantwoording belangrijke kernwaarden voor hun organisaties vinden. Bij de totstandkoming van de Wiv 2017 en de nadien in werking getreden Wet open overheid werd het niet noodzakelijk geacht dat de CTIVD en de TIB onder de daarin geregelde inzageregeling vielen. Daarvoor golden belangrijke argumenten die ook gelijkelijk gelden voor het CTT. Bij dit wetsvoorstel wordt niet beargumenteerd waarom dit nu wel noodzakelijk is, anders dan de algemene onderbouwing dat inzage voor elke overheidsinstantie geldt.
146. De CTIVD en de TIB onderschrijven het belang van transparantie en het afleggen van verantwoording, maar toepassing van de inzagebepalingen uit het wetsvoorstel ten aanzien van gegevens die zijn verwerkt door het CTT, ook wanneer deze gegevens niet door of ten behoeve van de diensten verwerkte gegevens betreffen, stuit op bezwaren. Wanneer het desondanks noodzakelijk wordt geacht dat de inzageregeling van toepassing moet zijn op het CTT, dan zou in de wettekst expliciet moeten worden opgenomen dat het hier *uitsluitend* gaat om gegevens over haar bedrijfsvoering. Dit neemt niet weg dat ook dergelijke gegevens niet of in zeer beperkte mate openbaar kunnen worden gemaakt. Bij openbaar te maken gegevens moet slechts worden gedacht aan algemene informatie zoals functiebeschrijvingen etc. De toegevoegde waarde hiervan boven de reeds via andere wegen bekendgemaakte informatie is zeer beperkt.
147. Op veruit de meeste informatie die het CTT onder zich heeft rust in beginsel een geheimhoudingsplicht, omdat deze informatie door of ten behoeve van de diensten verwerkte gegevens betreft, dan wel rechtstreeks te relateren is aan deze gegevens. Voor deze gegevens geldt een apart openbaarmakingsregime in de huidige Wiv 2017 en op een vergelijkbare wijze in het wetsvoorstel via de diensten. De vraag is derhalve of dat uitgangspunt niet evenzeer zou moeten gelden voor door of ten behoeve van het CTT verwerkte gegevens, zoals memo's, vergaderverslagen, toetsingskaders. Gelet op de nauwe verwevenheid van deze gegevens met door of ten behoeve van de diensten verwerkte gegevens, moet deze vraag positief worden beantwoord. Dezelfde vraag is ten aanzien van de CTIVD en de TIB bij de Wiv 2017 ook positief beantwoord. Dit geldt ook voor gegevens van het CTT die uitsluitend zien op haar bedrijfsvoering. Een instantie die toezicht houdt op werkzaamheden van inlichtingen- en veiligheidsdiensten zal, alleen al gegeven haar toegang tot alles en iedereen binnen de diensten, net als de diensten zelf, in de belangstelling staan van buitenlandse, al dan niet statelijke actoren. Vanuit dat perspectief kan door het leggen van verbanden tussen en combineren van onder meer reiskosten, vergaderkosten, beveiligingskosten en (technische) kantoortoepassingen informatie worden gegenereerd die voornoemde actoren behulpzaam is bij activiteiten die negatieve implicaties kunnen hebben voor de nationale veiligheid. De (technische) beveiligingsmaatregelen die in dit verband ten behoeve van het CTT en haar werkzaamheden zijn getroffen, wijzen erop dat het hier niet gaat om een slechts denkbeeldige mogelijkheid.
148. De nieuwe wet bepaalt al op welke wijze en wat het CTT openbaar maakt. Het valt binnen de taakopvatting van het CTT dat zij binnen de kaders van deze wet zoveel mogelijk openbaar zal maken en publiceren op haar website, zoals dit nu ook geldt voor de CTIVD en in de vorm van een jaarverslag ook voor de TIB. Toepassing van de inzageregeling zou in de meeste gevallen een herhaling van zetten zijn. Gegevens die op grond van bepalingen uit het wetsvoorstel openbaar moeten en kunnen worden gemaakt, zullen vrijwel altijd gegevens zijn die volgens de wettelijke bepalingen uit het wetsvoorstel reeds openbaar zijn gemaakt. Het CTT stelt zich dan ook op het standpunt dat het niet zinvol is haar onder de reikwijdte van de inzageregeling te laten vallen. Voor het CTT geldt eenzelfde openbaarmakingsprocedure als nu voor de TIB en de CTIVD. Dit ziet allereerst op het uitbrengen van een jaarverslag. Voor het CTT wordt dit uitgebreid met

een openbaar jaarplan (art. 176). Voor het CTT geldt ook de wettelijke plicht om zoveel mogelijk in de openbaarheid te publiceren over haar bevindingen en werkzaamheden. De CTIVD doet dit via rapportages, zoals toezichtrapporten en brieven (gepubliceerd op www.ctivd.nl). Hierin worden naast bevindingen en oordelen, ook toetsingskaders opgenomen. Deze rapporten en brieven worden aan het parlement aangeboden en op de website van de CTIVD gepubliceerd. Waar geheimhouding hieraan in de weg staat (de wet verbiedt openbaarmaking van gegevens die zien op modus operandi, identiteit van bronnen en actueel kennisniveau), wordt de CIVD van de TK geïnformeerd (tenzij in heel uitzonderlijke gevallen art. 68 Grondwet hieraan in de weg zou staan) en wordt in algemene zin verslag gedaan in het jaarverslag. Daarnaast zal het CTT, net als de CTIVD en de TIB, een reglement van orde en een openbaar toezichtprotocol publiceren waarin vanuit het oogpunt van voorzienbaarheid en transparantie de procedures en producten van toezicht worden beschreven. Voor het CTT geldt op grond van de wet dat zij uit eigen beweging al openbaar maakt wat zij openbaar kan en mag maken. De wet telt grenzen aan openbaarmaking door het CTT, maar het is evenwel de taakopvatting van het CTT dat zij binnen deze grenzen maximale openbaarheid betracht.

149. Omdat het bij het CTT vaak gaat over informatie die volgens de wet geheim moet blijven, zal openbaarmaking op verzoek in veruit de meeste gevallen stranden op een van de uitzonderingsgronden die zijn opgenomen in het wetsvoorstel. Dit is niet wenselijk omdat daardoor onterecht het algemene beeld kan ontstaan van een toezichthouder die gegevens niet wil openbaren.
150. Daarnaast blijkt dat uitvoering van het wetsvoorstel betekent dat werkprocessen en systemen moeten worden aangepast. Het vraagt aanzienlijk meer capaciteit om de verzoeken om inzage te verwerken. Tegen deze achtergrond zullen de daarvoor benodigde extra investeringen en inspanningen, die voor een kleine organisatie als het CTT onvermijdelijk verbonden zijn met het voorgestelde openbaarmakingsregime, niet in verhouding staan met de zeer beperkte mate van openbaarheid die zij over door haar verwerkte gegevens zal kunnen geven. Dit geldt ook voor gegevens die uitsluitend gaan over haar bedrijfsvoering.

12.9 Toezicht-hiaat internationale context

151. De CTIVD en de TIB wijzen al enige jaren op het toezicht-hiaat in de internationale context. De CTIVD en de TIB spannen zich er al jaren voor in dat ook op toezichtgebied er internationaal meer samenwerking kan plaatsvinden. In het wetsvoorstel is hier geen aandacht voor. Voor de CTIVD en de TIB is niet duidelijk waarom het CTT niet onder dezelfde voorwaarden met de (internationale) toezichthouders zou kunnen samenwerken waar de diensten wel toe bevoegd zijn.
152. In de praktijk en in het wetsvoorstel zien we dat die internationale samenwerking tussen diensten en andere internationale partijen steeds intensiever wordt en innoveert. Dit kan vergaande vormen aannemen zoals verstrekkingen van grote hoeveelheden gegevens, het uitvoeren van gezamenlijke operaties en gezamenlijke verwerking van gegevens, ook met meerdere diensten tegelijk in samenwerkingsverbanden. Deze samenwerking en gegevensdeling met inlichtingen- en veiligheidsdiensten van andere landen gebeurt op basis van het vertrouwensbeginsel. Dit beginsel is een zeer belangrijke ongeschreven regel. In de politiek en in de maatschappij is begrip voor deze (internationale) samenwerking, maar er is ook veel onrust over, omdat niet kan worden gecontroleerd hoe deze samenwerkingen en gegevensdelingen plaatsvinden.
153. Daar staat tegenover dat het toezicht op inlichtingen- en veiligheidsdiensten een nationale aangelegenheid is op basis van nationale wetgeving. De CTIVD en de TIB hebben onder de huidige wet geen mandaat om staatsgeheime informatie te delen met andere internationale toezichthouders. Er is geen sprake van gezamenlijke toezichtactiviteiten of operationele samenwerking tussen nationale toezichthouders uit verschillende landen, zoals tussen inlichtingen- en veiligheidsdiensten bestaat. Hierdoor is wel gesproken over een zogenaamd

'toezicht-hiaat in de internationale context'. Dit ontstaat doordat het toezicht op de internationale samenwerking van de AIVD en de MIVD niet voorbij de nationale grenzen gaat. Het gevolg is dat het huidige wettelijke stelsel voor nationaal toezicht niet toereikend is om de diensten in een internationale context verantwoordelijk te houden.

154. Dit toezicht-hiaat bestaat al in de huidige praktijk, maar in het wetsvoorstel worden de samenwerkingsgrondslagen nog verder verruimd. Het wordt bijvoorbeeld mogelijk om niet alleen met inlichtingen- en veiligheidsdiensten van andere landen, maar ook met andere entiteiten die inlichtingenwerk doen samen te werken. Deze entiteiten, waarvan niet is te overzien welke partijen hieronder kunnen vallen, zitten niet per definitie in het inlichtingen- en veiligheidsdomein of zijn verbonden aan erkende staten, en zijn dus niet per definitie bekend met het vertrouwensbeginsel. Ook blijkt uit het coalitieakkoord van de regering Jetten dat het doel is de samenwerking tussen inlichtingen- en veiligheidsdiensten op Europees niveau te versterken, en zelfs een Europees equivalent van de bestaande Five Eyes op te richten om zo met een kopgroep van Europese landen intensief te kunnen samenwerken.
155. Het wetsvoorstel moet de internationale samenwerking met betere waarborgen omkleden. Een belangrijk onderdeel van goede waarborgen voor (internationale) samenwerking is het toezicht. Wij zijn gebonden aan nationale wetgeving en kunnen de bevindingen van ons toezicht niet delen en bediscussiëren met toezichthouders van andere landen. Wij kunnen daardoor bijvoorbeeld niet controleren in hoeverre er toezicht is ná de gegevensverstrekking van onze diensten aan diensten van andere landen. Dan wel of buitenlandse diensten de gegevens die zij verstrekken aan onze diensten volgens de voor hun wettelijke regels hebben verkregen. Daardoor zijn wij niet in staat te beoordelen welk niveau van bescherming van individuele rechten wordt geboden door de ontvangende dienst. Kennis hiervan is relevant voor de beoordeling van de proportionaliteit van gegevensuitwisseling. Dit is een voorbeeld van wat wij verstaan onder het toezichthiaat, of '*oversight gap*'.
156. Wij hebben dit onderzocht met vier andere toezichthouders en hebben daarover in 2018 gepubliceerd. Een belangrijke conclusie was dat voor een effectieve samenwerking tussen toezichthouders het nodig kan zijn om staatsgeheime gegevens te delen. Toezichthouders zouden bijvoorbeeld in ieder geval met elkaar moeten kunnen overleggen over concrete bilaterale en multilaterale samenwerkingsafspraken tussen de diensten waarop zij toezicht houden. Wij hebben een wettelijk mandaat nodig om dit te kunnen doen.
157. Zoals gezegd is toezicht een onderdeel van de waarborgen, maar niet zaligmakend. Zoals we in dit proces steeds naar voren hebben gebracht, zijn de bevoegdheden van de diensten in het wetsvoorstel verruimd zonder de waarborgen daarop mee te laten groeien. Daardoor heeft het hele wetsvoorstel, in onderlinge samenhang bezien, onvoldoende balans tussen de nationale veiligheid en fundamentele rechten. De (internationale) samenwerking is daar een onderdeel van.

12.10 Afdeling klachtbehandeling

158. De CTIVD en de TIB hebben ook een aantal opmerkingen die specifiek gelden voor de positie van de afdeling klachtbehandeling binnen het CTT.

Unus oordelen

159. De CTIVD en de TIB maken zich zorgen dat het wetsvoorstel slechts voorziet in één klachtlid en geen plaatsvervangende leden (art. 163 lid 1). In art. 193 ten opzichte van art. 118 Wiv 2017 is niet opgenomen dat een klacht behandeld wordt door de voorzitter van de afdeling en twee aangewezen leden. Het wordt niet duidelijk waarom er gekozen is voor unus-beslissingen binnen de afdeling klachtbehandeling, anders dan het relatief geringe aantallen klachten en vermoedens van misstanden dat de afdeling zou behandelen. Bij de afdeling toetsing is unus-beslissen het

uitgangspunt, maar voorziet het wetsvoorstel ook in de mogelijkheid tot meervoudig beslissen. Daarin voorziet het wetsvoorstel niet voor de afdeling klachtbehandeling. Daarmee miskent het wetsvoorstel dat een aantal klachten tot onderzoek leidt en vervolgens een oordeel dat eventueel bindend kan zijn. Daarvoor moet het mogelijk blijven om meervoudig te beslissen. Gezien de scheiding qua benoeming tussen de leden van de afdelingen van het CTT is het niet mogelijk dat de afdeling gebruik maakt van de leden van de afdeling toezicht. Er moet dus voorzien worden in meerdere (plaatsvervangende) leden voor de afdeling klachtbehandeling zodat de afdeling naast unus-beslissingen ook waar zij dat aangewezen acht, meervoudig kan besluiten.

Vastlegging interne klachtprocedure

160. Op de behandeling van klachten door de diensten zelf (eerstelijnsklachtbehandeling) is de Algemene wet bestuursrecht (Awb) van toepassing. Voor meldingen van vermoedens van misstanden geldt de Awb niet. De Wet bescherming klokkenluiders is niet van toepassing. Daarom is het opvallend dat in art. 200 de definitie van de interne procedure voor meldingen van vermoedens van misstanden uit het voormalige art. 125 Wiv 2017 is weggelaten. Over die interne procedure staat ook elders in de het wetsvoorstel niets. In de memorie van toelichting dient, anders dan onder de Wiv 2017, voldoende informatie te staan over de interne procedures voor behandeling van klachten en meldingen van vermoedens van misstanden. Dat ontbreekt. Bij de evaluatie van de Wiv 2017 heeft de CTIVD destijds aangegeven dat de bij AMvB vastgestelde regelingen van de beide diensten voor klachten en meldingen op orde waren. De afdeling klachtbehandeling oordeelt aan de hand van die regelingen ook over de juiste toepassing van interne klachtbehandeling en behandeling meldingen van vermoedens van misstanden. In een aantal gevallen luidde het: niet behoorlijk. Nu in het wetsvoorstel en de memorie van toelichting niets opgenomen is over de interne procedures ontbreekt een waarborg voor een blijvend goede regeling van de interne klachtbehandeling en de behandeling van vermoedens van misstanden.

13. Staatsnoodrecht

161. De buitengewone omstandigheden zien op situaties waarin (nog) niet een daadwerkelijke noodtoestand, zoals een gewapend conflict in de regio, is afgekondigd. De vraag is of het staatsnoodrecht de zogenoemde democratische stresstest kan doorstaan.
162. Op voorhand is niet in te schatten voor welke situaties een beroep zal worden gedaan op de bepalingen van staatsnoodrecht. Hoewel deze bepalingen geformuleerd zouden moeten zijn met het oog op voorzienbaarheid, brengt juist de ruime formulering onduidelijkheid en onvoorspelbaarheid in de toepassing met zich mee.
163. Dit moet ook worden bezien in het licht van het relatieve gemak, via een koninklijk besluit, waarmee het staatsnoodrecht kan worden ingeroepen, met de vergaande implicaties die het inhoudt. De controle van het parlement vindt pas later plaats bij de behandeling van het ingediende voorstel voor een voortduringswet.
164. Het wetsvoorstel zoals dat nu is geformuleerd biedt de diensten al een enorme mogelijkheid aan flexibiliteit met zo min mogelijk administratieve lastendruk. De CTIVD en de TIB vragen zich af of het staatsnoodrecht in verhouding staat tot de voorgestelde mogelijkheden van bijvoorbeeld spoedprocedures in het wetsvoorstel.
165. Hiervoor hebben wij uitgebreid uiteengezet dat het wetsvoorstel de waarborgen aanzienlijk vermindert. Het inroepen van het staatsnoodrecht biedt de betrokken ministers de mogelijkheid een aantal belangrijke waarborgen op te schorten (art. 224-225). Dit geldt bijvoorbeeld voor de verplichting van de diensten om jaarlijks verantwoording af te leggen aan het parlement. Ook de onafhankelijkheid van de toezichthouder kan worden ondermijnd. Zo kunnen de betrokken ministers zelf nieuwe leden van de toezichthouder benoemen zonder dat de wettelijke benoemingsprocedure wordt gevolgd. Ook hoeven deze leden niet meer aan de wettelijke benoemingsvereisten te voldoen. Bovendien kan de minister ingrijpen in de wijze waarop het CTT haar werk doet. De minister is bijvoorbeeld bevoegd om te bepalen dat het CTT alleen nog maar in enkelvoudige samenstelling (unus) over ex ante toetsingen kan besluiten, dat de rechtsmatigheidstoets wordt opgeschort of zelfs in zijn geheel vervalt. Ook waarborgen die van belang zijn voor het recht op een daadwerkelijk rechtsmiddel (‘*effective remedy*’) kunnen verder worden beperkt. Zo kan de notificatieplicht aan personen tegen wie bijzondere bevoegdheden zijn ingezet worden opgeschort en de beslistermijnen voor inzageverzoeken worden verlengd.

14. Overgangsrecht

166. In paragraaf 13.2 van het wetsvoorstel wordt de overgang van de Wiv 2017 naar het de nieuwe wet geregeld. Deze artikelen zijn niet eerder aan de CTIVD en de TIB voorgelegd.

Overgangsrecht m.b.t. gegevensverwerking

167. Het wetsvoorstel introduceert vergaande aanpassingen in het kader van gegevensverwerking, waarbij de wettelijke waarborgen achterblijven tegenover de uitbreiding van de bevoegdheden. Het wetsvoorstel bevat in het overgangsrecht een delegatiebepaling. Deze bepaling maakt het mogelijk om bij ministeriële regeling af te wijken van het wetsvoorstel indien de operationele continuïteit dit vereist. Het is knellend dat eenvoudig van de reeds ingeperkte bescherming in het wetsvoorstel kan worden afgeweken. Als deze afwijkingsbevoegdheid toch wordt opgenomen in een delegatiebepaling, dient dit te worden voorzien met een algemene maatregel van bestuur (AMvB) en een voorhangprocedure, aangezien de waarborging van de fundamentele rechten en parlementaire betrokkenheid hierdoor onder druk komen te staan.

Overgangsrecht m.b.t. nieuw op te richten CTT

168. Verder regelt het wetsvoorstel dat de afdeling toetsing, afdeling toezicht en afdeling klachtbehandeling kunnen blijven werken met de al opgestelde interne regelementen, tot deze vervangen zijn in het kader van het nieuwe wetsvoorstel. De afdelingen dienen de scheiding tussen taken in acht te nemen. Dit belemmert echter de efficiëntie bij het harmoniseren van de reglementen tot een eenduidige werkwijze.
169. Het wetsvoorstel voorziet in een bepaling die, bij onvoorziene omstandigheden, de mogelijkheid biedt om nadere regels te stellen bij ministeriële regeling door de minister-president in het kader van de overgang toetsingscommissie en commissie van toezicht. Ondanks dat de onafhankelijkheid van het CTT wordt gewaarborgd door deze verantwoordelijkheid bij de minister-president te beleggen, wordt in het artikel niet gesproken over de rol van het CTT in de totstandkoming van de ministeriële regeling en het eventueel volgende wetsvoorstel, anders dan het consultatierecht o.g.v. art. 179. Het is van belang om op te nemen in het wetsartikel dat het CTT bevoegd is om in gesprek te gaan met de minister-president dan wel de betrokken ministers (de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie) om aan te geven dat, in afwijking of aanvulling op het wetsvoorstel, een ministeriële regeling en eventueel een wetsvoorstel noodzakelijk is voor de uitvoering van haar taken in het kader van de overgang naar het nieuwe wetsvoorstel.
170. Tot slot, vragen we aandacht voor het aantal verzoeken die het CTT verwacht bij ingang van de nieuwe wet. Art. 48 lid 4 van het wetsvoorstel verplicht de afdeling toetsing om in ieder geval uiterlijk twee weken na ontvangst van het verzoek een oordeel uit te brengen. Het is voorzienbaar dat het voor de diensten voordeliger is om bepaalde verzoeken in te dienen onder de nieuwe wet in plaats van de Wiv 2017. Als gevolg hiervan bestaat het risico dat verzoeken en masse worden ingediend als de nieuwe wet in werking is getreden en de twee weken termijn daardoor voor het CTT niet haalbaar is. Daarom adviseren wij tot een redelijke overgangstermijn voor de ingang van art. 48 lid 4 van dit wetsvoorstel.

Overgangsrecht m.b.t. samenwerking

171. Het wetsvoorstel regelt ook overgangsrecht ten aanzien van samenwerkingsbepalingen van de diensten (art. 242). Dit beoogt na inwerkingtreding van de nieuwe wet een vloeiende overgang van de nieuwe regels naar de praktijk te bewerkstellingen.
172. Voor internationale samenwerking met buitenlandse diensten of militaire entiteiten resulteert dit erin dat de verplichting tot het uitvoeren van een weging voor al bestaande bilaterale relaties

(opstellen wegingsnotitie op grond van art. 138 lid 3) of voor reeds bestaande multilaterale verbanden (opstellen overzichtsnotitie op grond van art. 139 lid 3) na inwerkingtreding van de wet met vijf jaar wordt uitgesteld. Mogelijk kan deze beperking aan waarde worden ondervangen doordat in de memorie van toelichting staat dat gedurende deze vijf jaar het diensthoofd er zorg voor draagt dat indien omstandigheden daartoe aanleiding geven de deelname aan een samenwerkingsrelatie of -verband geheel of gedeeltelijk opnieuw wordt gewogen of dat een overzichtsnotitie wordt opgesteld (art. 138 lid 6 en art. 139 lid 6).

173. Risicovol vinden wij het tweede deel van het overgangsrecht in art. 242 op grond waarvan de nieuw voorgestelde wegingsnotities en overzichtsnotities voor publiek-, private en multilaterale samenwerking, bedoeld in de art. 144 lid 3, 145 lid 3 en art. 146 lid 3, pas voor het eerst uiterlijk twee jaar na inwerkingtreding van de wet worden opgesteld. Dit betekent dat twee jaar van de bevoegdheid gebruik mag worden gemaakt voordat de bijbehorende waarborgen in werking treding. Een dergelijk lange overgangstermijn vinden de CTIVD en de TIB voor dit soort risicovolle samenwerkingen onwenselijk.

Postbus 85556, 2508 CG Den Haag

T 070 315 58 20
E info@ctivd.nl | www.ctivd.nl