Eindbalans Wiv 2017: een werkbare wet

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

EINDBALANS WIV 2017: EEN WERKBARE WET

In een wet die het handelen van inlichtingen- en veiligheidsdiensten reguleert, dient de bescherming van de nationale veiligheid in balans te zijn met de bescherming van de grondrechten van de burger, zoals het recht op privacy en de bescherming van persoonsgegevens. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) beantwoordt in deze nota de vraag of de binnenkort in te voeren Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) op dit punt in balans is.

Achtergrond

In het jaar 2017 is veel gebeurd rondom de totstandkoming van de Wiv 2017. Het voorstel voor deze wet is door de Tweede Kamer aangenomen op 14 februari 2017 en door de Eerste Kamer op 11 juli 2017. De CTIVD heeft het parlementaire en maatschappelijke debat inhoudelijk gevoed met o.a. de publicatie van haar "Standpunt" in januari 2017, waarin werd voortgebouwd op haar "Zienswijze" op het wetsvoorstel van november 2016, en een brief aan de Eerste Kamer in maart 2017.[1] Zij plaatste kritische kanttekeningen bij de mate waarin de wet voorzag in waarborgen tegen ongeoorloofd gebruik van bevoegdheden en de in mogelijkheden voor effectief toezicht op het handelen van de inlichtingen- en veiligheidsdiensten. Op 25 augustus 2017 werd de Wiv 2017 in het Staatsblad gepubliceerd. De invoering van de wet staat nu voor mei 2018. In het op 10 oktober 2017 gepresenteerde regeerakkoord is onder meer opgenomen: "Van het willekeurig en massaal verzamelen van gegevens van burgers in Nederland of het buitenland ('sleepnet') kan, mag en zal geen sprake zijn. Daarom zal het kabinet bij de uitvoering strikt de hand houden aan de extra waarborgen in deze wet." Op 15 december 2017 stuurde de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK), namens het kabinet, een brief aan de Tweede Kamer waarin m.b.t. de Wiv 2017 aanvullende waarborgen zijn opgenomen. Het maatschappelijk debat over de Wiv 2017 is begin 2018 opnieuw volop op gang gekomen. Dit debat heeft een nieuwe dimensie gekregen doordat een raadgevend referendum over de Wiv 2017 werd aangevraagd, dat op 21 maart 2018 zal plaatsvinden.

Tegen deze achtergrond geeft de CTID in deze nota antwoord op de vraag of de uitbreiding van bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD; tezamen: de diensten) thans in balans is met de daarmee verbonden noodzakelijke waarborgen voor de rechtsbescherming van de burger en de mogelijkheden voor effectief toezicht. Zij bouwt daarbij voort op de door haar eerder uitgebrachte adviezen die gericht waren op versterking van de wet. Daarbij komen twee onderwerpen aan bod waar de inmenging in de grondrechten van de burgers zich sterk doet voelen: (1) de nieuwe bevoegdheid van het in bulk tappen van de kabel en (2) de samenwerking met buitenlandse diensten. Toereikende waarborgen voor rechtsbescherming en mogelijkheden voor effectief toezicht moeten dáár dan ook aanwezig zijn. Daarnaast besteedt de nota aandacht aan (3) de wettelijke zorgplicht van de diensten voor de kwaliteit van de gegevensverwerking, omdat dit een belangrijke waarborg voor de gegevensbescherming vormt. Aan het slot beantwoordt de CTIVD de vraag of de Wiv 2017 in balans is (4).

[1] Alle beschikbaar op www.ctivd.nl

(1) Het in bulk tappen van de kabel

In de Wiv 2017 krijgen de AIVD en de MIVD de bevoegdheid communicatie over de kabel onderzoeksopdrachtgericht te intercepteren. Het is een aanvulling op de bevoegdheid tot ongerichte interceptie van ethercommunicatie; een bevoegdheid die de AIVD en de MIVD nu reeds hebben op grond van de huidige Wiv 2002. De CTIVD gaat hieronder vraagsgewijs in op de noodzaak en de betekenis van de bevoegdheid en de wijze waarop de Wiv 2017 deze inkadert.

Noodzaak

Waarom is het in bulk tappen van de kabel van belang?
De CTIVD onderkent de noodzaak van de uitbreiding van de bevoegdheden van de AIVD en de MIVD zoals voorzien in de Wiv 2017. De uitbreiding is noodzakelijk om, gegeven de aard en de omvang van de bedreigingen voor onze nationale veiligheid, bestaande inlichtingenmatig blinde vlekken zoveel mogelijk weg te nemen en daarmee de slagkracht van onze inlichtingen- en veiligheidsdiensten te vergroten. Het ontstaan van deze blinde vlekken kent verschillende verklaringen. Zo zijn als gevolg van technologische ontwikkelingen de communicatietoepassingen (bijvoorbeeld het gebruik van berichtenapps) en – infrastructuur (bijvoorbeeld de uitbreiding van het glasvezelnetwerk) sinds de invoering van de huidige Wiv 2002 aanzienlijk veranderd. Personen die in onderzoek zijn van de diensten kunnen van steeds nieuwe communicatietoepassingen op het internet gebruikmaken. De diensten kunnen deze communicatie met alleen de inzet van gerichte bevoegdheden, zoals een telefoontap, onvoldoende effectief onderzoeken. Het tijdig onderkennen, herleiden en tegengaan van nieuwe cyberdreigingen en – aanvallen is evenmin goed mogelijk met de inzet van gerichte bevoegdheden alleen. Ook daarvoor is noodzakelijk dat de diensten op grotere schaal technisch onderzoek kunnen doen. Bovendien is het voor onze nationale veiligheid van belang dat de diensten blijvend in staat zijn onbekende dreigingen tijdig te onderkennen. Het in bulk verzamelen van communicatie die over kabels verloopt is daarvoor noodzakelijk.

Waarborgen

Is sprake van het grootschalig verzamelen van gegevens?
Ja. De bevoegdheid tot het in bulk tappen van de kabel stelt de AIVD en de MIVD in staat grootschalig (persoons)gegevens te verzamelen. Naar verwachting zal bij het in bulk aftappen van de kabel ca. 98% van de getapte gegevens direct worden vernietigd, omdat op voorhand kan worden vastgesteld dat deze gegevens niet terzake doen. Voor verdere verwerking zal dus rond de 2% worden opgeslagen.[2] Maar ook bij die 2% zal het nog steeds om zeer omvangrijke hoeveelheden (persoons)gegevens gaan. Deze opgeslagen gegevens zijn potentieel van waarde voor de onderzoeksopdrachten waarvoor de dienst de bevoegdheid heeft ingezet. Analyse en selectie zal vervolgens moeten uitwijzen welke gegevens van die 2% te relateren zijn aan personen, organisaties en onderwerpen waarnaar de diensten onderzoek

[2] Memorie van Toelichting bij het wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20.. (Wiv 20..), *Kamerstukken II* 2016/17, 34588 nr. 3, p. 146. De genoemde percentages gelden niet voor ether communicatie (niet-kabelgebonden).

verrichten. Daarvan zal slechts een deel uiteindelijk relevant blijken te zijn en worden gebruikt voor de onderzoeksopdrachten van de AIVD en de MIVD. Alle overige data moeten worden verwijderd, dan wel vernietigd. Hetzij terstond, hetzij binnen 3 jaar. In zoverre gaat de metafoor van het sleepnet dus maar gedeeltelijk op: er is wel sprake van het grootschalig verzamelen van (persoons)gegevens, maar niet van het grootschalig gebruik daarvan. De Wiv 2017 staat bovendien willekeurig gebruik van gegevens niet toe (zie hierna).

Mogen de diensten willekeurig communicatie verzamelen en opslaan?
Nee, de bevoegdheid van de diensten communicatie te verzamelen en op te slaan wordt ingeperkt door de Wiv 2017. De wet en de toelichting hierop bieden in dit verband de volgende waarborgen:

1. De diensten moeten bij het in bulk tappen de keuze maken welke kabels en fibers zij willen tappen. Deze keuze moet gemotiveerd voor toestemming worden voorgelegd aan de betrokken minister(s). De Toetsingscommissie Inzet Bevoegdheden (TIB) toetst vervolgens bindend een door de minister verleende toestemming op rechtmatigheid. Als de TIB de toestemming niet rechtmatig acht, mag de bevoegdheid niet worden ingezet.

2. Daarbij geldt dat die motivering, waarin het doel van het onderzoek en in dat verband de noodzakelijkheid van de verwerving en opslag van de gegevens moet worden onderbouwd, dient aan te tonen dat een gerichtere inzet niet mogelijk is.[3]

3. Wanneer de diensten overgaan tot het feitelijke tappen van de kabel, zullen filters worden aangebracht. Deze filters bepalen welke gegevens gerelateerd zijn aan de onderzoeksopdrachten van de diensten en dus (voorlopig) mogen worden opgeslagen (2%). Ook bepalen deze filters welke gegevens direct moeten worden vernietigd (98%). De samenstelling van de filters is dus, naast de specifieke keuze voor bepaalde kabels en fibers, bepalend voor de mate waarin de verwerving is gericht op de onderzoeksopdrachten.

4. Na uiterlijk drie jaar moeten alle gegevens vernietigd zijn die voor het verstrijken van die termijn als niet relevant voor de taakuitvoering zijn beoordeeld respectievelijk in het geheel niet beoordeeld zijn.

Mogen de diensten die opgeslagen (persoons)gegevens willekeurig gebruiken?
Nee, er zijn in de wet waarborgen voor databeperking opgenomen, die zien op de verdere verwerking en het gebruik van de opgeslagen 2% (persoons)gegevens. De grootste inmenging in de rechten van de burger vindt plaats daar waar de diensten de opgeslagen persoonsgegevens verder verwerken, door het verkennen van de communicatie (search), het geautomatiseerd analyseren van de verworven metadata en het selecteren van inhoud. Vervolgens mogen zij uitsluitend de relevante uitkomsten daarvan gebruiken en langdurig bewaren. Dit maakt het essentieel dat na de verwerving de opgeslagen gegevens zo spoedig mogelijk worden gereduceerd tot die gegevens die de AIVD en de MIVD daadwerkelijk nodig hebben om hun taken goed uit te voeren (relevante gegevens). De CTIVD noemt dit **verantwoorde databeperking**.

---

[3] Motie nr. 66 van het lid Recourt (PvdA), *Kamerstukken II* 2016/17, 34588 nr. 66, waarin is opgenomen dat de de wettelijke eisen van noodzakelijkheid, proportionaliteit en subsidiariteit geïnterpreteerd worden en in de praktijk gebruikt worden als eisen die zullen leiden tot een zo gericht mogelijke inzet van bevoegdheden.

Welke waarborgen zijn er voor die verantwoorde databeperking?
In de nieuwe wet zijn de waarborgen voor verantwoorde databeperking in de loop van de parlementaire behandeling versterkt. Er is toegevoegd dat de inzet van bevoegdheden zo gericht mogelijk moet zijn en er is nadere betekenisvolle toelichting gegeven over hoe de wet in de praktijk uitgelegd moet worden, bijvoorbeeld over het begrip 'relevante gegevens'. Ook is door het kabinet in het regeerakkoord toegezegd dat "van het willekeurig en massaal verzamelen van persoonsgegevens geen sprake kan, mag en zal zijn". De Wiv 2017 biedt thans, met die context, toereikende waarborgen voor verantwoorde databeperking. Deze waarborgen zijn gelegen in de volgende twee elementen:

1. Voorafgaande toestemming en onafhankelijke toets voor verdere verwerking
   De diensten moeten niet alleen de verzameling zelf maar ook de verdere verwerking van de opgeslagen gegevens voor toestemming aan de betrokken minister voorleggen. Zo moet voorafgaand aan de verkenning van de communicatie (search), de geautomatiseerde analyse van verworven metadata en de selectie van gegevens m.b.t. personen, organisaties en onderwerpen vooraf gemotiveerd toestemming worden verkregen van de betrokken minister(s). De TIB toetst bindend de door de minister verleende toestemming. Ook hier geldt als een aanvullende waarborg dat de inzet van bevoegdheden zo gericht mogelijk moet zijn. Dit houdt o.m. in dat de diensten moeten aantonen dat een gerichtere inzet van bevoegdheden t.a.v. de desbetreffende personen, organisaties en onderwerpen niet mogelijk is. Dit criterium geldt dus behalve voor de verwerving, ook voor de inzet van de voor de privacy van burgers ingrijpende bevoegdheden van search, geautomatiseerde data-analyse en selectie.

2 De verplichting de opgeslagen gegevens op relevantie te beoordelen.
   De Wiv 2017 vereist dat de opgeslagen gegevens (die ca. 2%) worden beoordeeld op relevantie voor de taakuitvoering. Door onder meer de geautomatiseerde analyse van de verworven metadata en door het gebruik van selectoren in het selectieproces (zoals telefoonnummers en e-mailadressen, maar ook trefwoorden) vindt een verdere schifting plaats van gegevens die wel en niet zijn te relateren aan de personen, organisaties en onderwerpen waarnaar de AIVD en de MIVD onderzoek verrichten. Dit leidt er uiteindelijk toe dat de uitkomsten van metadata-analyse en de met behulp van selectoren geselecteerde gegevens voor gebruik beschikbaar komen voor het operationeel team dat het onderzoek verricht. Dit betekent echter niet dat die gegevens ook daadwerkelijk van waarde zijn voor het onderzoek. Geautomatiseerde data-analyse en het toepassen van technische kenmerken of trefwoorden kan immers ook gegevens beschikbaar maken, die niet waren beoogd en geen bijdrage leveren aan het onderzoek. Om te bepalen of de gegevens relevant zijn, d.w.z. daadwerkelijk van betekenis voor het onderzoek, dient in de operationele context een nadere inhoudelijke beoordeling plaats te vinden van de geselecteerde gegevens. Dit is essentieel voor de rechtsbescherming van de burger. Pas dan wordt immers gewaarborgd dat gegevens die weliswaar aan de onderzoeksopdrachten zijn gerelateerd, maar uiteindelijk toch niet relevant blijken te zijn, worden verwijderd dan wel vernietigd. De nieuwe wet(sgeschiedenis) geeft een gedegen en toetsbaar kader voor deze relevantie beoordeling.[4]

[4] De behandeling van het wetsvoorstel in de Eerste Kamer heeft meer duidelijkheid gegeven over het begrip relevantie en de beoordeling daarvan bij onderzoeksopdrachtgerichte interceptie. Ook de in het regeerakkoord vastgelegde toezegging dat van het willekeurig verzamelen van gegevens van burgers in Nederland of het buitenland geen sprake kan, mag en zal zijn, biedt hiervoor steun.

Toezicht

Zijn er voldoende mogelijkheden voor effectief toezicht?
Ja, de CTIVD kan en zal toezicht houden op elk van de genoemde onderdelen van het proces van het in bulk tappen van de kabel. Zij zal zich daarbij op zowel de werking van het systeem als op de toepassing en uitwerking daarvan in concrete gevallen richten.

- Bij het tappen van de kabel ligt het zwaartepunt voor de CTIVD bij het toetsen van de filters die worden toegepast. Deze filters bepalen welke gegevens worden opgeslagen (die 2%) en welke gegevens direct worden vernietigd (die 98%). De CTIVD zal in dat verband ook toetsen of de opgeslagen gegevens in voldoende mate te relateren zijn aan de onderzoeksopdrachten en vallen binnen de door de minister verleende en door de TIB geautoriseerde toestemming.
- Ook waar het gaat om het verkennen van communicatie (search), het geautomatiseerd analyseren van de verworven metadata en het selecteren van inhoud zal de CTIVD beoordelen of de AIVD en de MIVD blijven binnen de verleende voorafgaande toestemming (hierboven punt 1). Een belangrijk onderdeel van deze beoordeling is of de selectoren die door de diensten worden toegepast (bijvoorbeeld telefoonnummers en e-mailadressen, maar ook trefwoorden), voldoende aansluiten bij de personen, organisaties en onderwerpen ten aanzien waarvan toestemming is verleend.
- Vervolgens zal de CTIVD beoordelen of de AIVD en de MIVD in de praktijk in het kader van verantwoorde databeperking voldoende invulling geven aan de vereiste relevantiebeoordeling (hierboven punt 2). Het gaat daarbij om de vraag of de gegevens die uiteindelijk gebruikt en langdurig bewaard worden daadwerkelijk relevant zijn voor de taakuitvoering van de diensten.
- Tot slot zal de CTIVD beoordelen of alle niet relevante gegevens vernietigd zijn en of alle niet beoordeelde gegevens binnen de wettelijke termijn van drie jaar na verwerving vernietigd zijn.

Mede in het kader van de door de Eerste en Tweede Kamer gevraagde en door de regering toegezegde evaluatie van de wet na twee jaar, zal de CTIVD vanaf de inwerkingtreding van de Wiv 2017 de werking van het proces van het in bulk tappen van de kabel en de verwijdering en vernietiging van gegevens daarbij, intensief monitoren. Zij zal van de uitkomsten daarvan d.m.v. openbare toezichtsrapporten berichten aan de betrokken ministers, het parlement en de samenleving.

(2) Internationale samenwerking

De CTIVD heeft zich in de loop van de parlementaire behandeling van het wetsvoorstel kritisch uitgelaten over de **overgangsbepaling** (artikel 166 Wiv 2017) die de wettelijke criteria voor **samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten** voor een periode van twee jaar buiten werking stelt voor bestaande samenwerkingsrelaties. Voor nieuwe samenwerkingsrelaties geldt deze overgangsbepaling niet en geldt de wet dus vanaf de datum van inwerkingtreding.

De toenmalige minister van BZK heeft in de Eerste Kamer in juni 2017 aangegeven dat de CTIVD toezicht kan houden zodra een wegingsnotitie binnen de genoemde periode van twee jaar gereed is. Een wegingsnotitie is een op schrift gestelde weging van risico's die, op basis van de wettelijke criteria voor samenwerking, aan de orde kunnen zijn in de samenwerking met een buitenlandse dienst. Het geeft aan of en zo ja in welke mate en onder welke voorwaarden, met een buitenlandse dienst kan worden samengewerkt, bijvoorbeeld op het terrein van de uitwisseling van persoonsgegevens.

De kabinetsbrief aan de Tweede Kamer van 15 december 2017 gaat een paar stappen verder. Het kabinet zegt toe dat bij de inwerkingtreding van de Wiv 2017 de wegingsnotities m.b.t. de meest hechte samenwerkingsrelaties van de AIVD en de MIVD reeds vastgesteld zullen zijn. Hieronder worden begrepen de buitenlandse diensten die deelnemen aan de Counter Terrorism Group (CTG) en diensten waarmee op het terrein van SIGINT intensief wordt samengewerkt. Ook zal na de inwerkingtreding van de wet voortvarend gewerkt worden aan wegingsnotities m.b.t. de andere bestaande samenwerkingsrelaties van de diensten. Deze wegingsnotities zullen na hun vaststelling direct werking krijgen en onder het toezicht van de CTIVD vallen. Deze toezegging biedt aanknopingspunten voor het toezicht. De CTIVD zal, zoals de Tweede Kamer haar reeds eerder heeft verzocht,[5] de betrokken ministers en het parlement d.m.v. een openbaar toezichtsrapport berichten over deze voortgang en de uitkomsten hiervan.

Verder is in de wet opgenomen dat de CTIVD terstond op de hoogte wordt gesteld wanneer de betrokken minister aan de AIVD of de MIVD toestemming heeft verleend voor de verstrekking aan een buitenlandse dienst van ongeëvalueerde gegevens die zijn verworven met toepassing van de bevoegdheid van het in bulk tappen van de kabel. Deze wettelijke verplichting draagt eveneens bij aan de mogelijkheden voor effectief toezicht.

(3) Zorgplicht

Nu de Wiv 2017 de diensten in de gelegenheid stelt grootschalig (persoons)gegevens te verwerken, is het van groot belang dat deze diensten kunnen instaan voor de kwaliteit van deze gegevensverwerking. Mede naar aanleiding van opmerkingen van de CTIVD is een zorgplicht voor deze kwaliteit in de nieuwe wet opgenomen. Het gaat hierbij bijvoorbeeld om de zorg voor de authenticiteit (juistheid) en betrouwbaarheid (volledigheid) van de te verwerken of al verwerkte gegevensbestanden. Het is bovendien noodzakelijk dat de diensten kunnen garanderen dat gegevensverwerkingstechnieken (zoals geautomatiseerde data-analyse of -vernietiging) doen wat daarvan wordt verwacht en dat de toezichthouder dit kan toetsen. De genoemde zorgplicht vormt hiervoor een belangrijke waarborg.

Hoe kan deze zorgplicht van de diensten worden geeffectueerd?
Om deze zorgplicht invulling te kunnen geven, adviseerde de CTIVD een aantal instrumenten in de Wiv 2017 op te nemen. Dit **instrumentarium voor de zorgplicht** houdt (onder meer) in het inrichten van specifiek beleid daartoe, het verrichten van privacy impactanalyses bij grote (ICT-) projecten en op audits om interne controle (compliance) uit te oefenen. De CTIVD heeft altijd benadrukt dat zonder het benoemen van concrete instrumenten het risico bestaat dat het toezicht op de naleving van deze belangrijke wettelijke verplichting van de AIVD en de MIVD onvoldoende effectief kan worden uitgeoefend.

In de brief aan de Tweede Kamer van 15 december 2017 zegt het kabinet thans toe dat de AIVD en de MIVD voorafgaande aan de inwerkingtreding van de Wiv 2017 een adequaat instrumentarium voor de invulling van de zorgplicht zullen implementeren, waarmee gegevensbescherming geborgd wordt en

[5] Bij het verschijnen van haar toezichtsrapport nr. 48 in juni 2016.

waarop effectief toezicht kan worden uitgeoefend. Nadat de Wiv 2017 in werking is getreden zal de CTIVD dan ook in het kader van de toetsing van de kwaliteit van de gegevensverwerking, waaronder de gegevensbescherming, op het bestaan en de werking van dit instrumentarium toezien en daarover aan de betrokken ministers en het parlement rapporteren.

(4) Is de Wiv 2017 in balans?

Ja. De Wiv 2017 is niet volmaakt, maar wel in balans. In balans omdat het een werkbare basis biedt voor zowel de bescherming van de nationale veiligheid als de rechtsbescherming van de burger daarbij en voor effectief toezicht. Niet volmaakt omdat die basis weliswaar is verankerd in de wet, maar in niet onbelangrijke mate invulling krijgt in moties, toelichtingen en in de door de regering gedane toezeggingen omtrent de uitvoering van de nieuwe wet. Het zou de rechtszekerheid op de langere termijn gediend hebben als deze in de wet zelf waren opgenomen.

Het geboden niveau van rechtsbescherming in de Wiv 2017 is, na alle wijzigingen en toezeggingen op dit vlak, naar ons oordeel thans toereikend. Toereikend in de zin dat het voldoet aan de minimum eisen die onder meer door onze grondwet, het Europees Verdrag voor de Rechten van de Mens (EVRM) en de daarop gebaseerde rechtspraak daaromtrent stelt. In de kern gaat het erom dat ons nationale systeem dat ziet op onze geheime diensten als geheel, in evenwicht is. Dat wil zeggen dat zowel interne (binnen de organisatie van de diensten zelf) als externe waarborgen (onafhankelijke externe autorisatie-, toezichts- en klachteninstanties) voldoende rechtsbescherming bieden tegen niet-noodzakelijke en onevenredige privacy inbreuken. Naar het oordeel van de CTIVD is dat met de voorliggende wet thans het geval. Het uiteindelijke oordeel daarover is natuurlijk aan de eventueel in te roepen (Europese) rechter.

Ook van mogelijkheden voor effectief toezicht is naar ons oordeel nu voldoende sprake. Dit laatste is wel afhankelijk van en loopt vooruit op de wijze waarop de AIVD en de MIVD de komende tijd in de praktijk invulling zullen geven aan onder meer de zorgplicht voor de kwaliteit van gegevensverwerking en de vaststelling van de wegingsnotities m.b.t. samenwerkingsrelaties. De CTIVD zal de betrokken ministers en het parlement van de stand van zaken van een en ander d.m.v. openbare toezichtsrapporten op de hoogte stellen.

De inwerkingtreding van de nieuwe wet brengt veel met zich mee, niet alleen voor de beide diensten maar ook voor het toezicht. De CTIVD is goed voorbereid op de nieuwe wet, zodat zij direct na inwerkingtreding voortdurend en intensief toezicht kan houden. Zij heeft extra capaciteit en deskundigheid ingeruimd om de werking van de nieuwe wet op verschillende onderdelen vanaf het begin te toetsen.

Het is zaak dat met deze wet in handen, gewerkt wordt aan de bescherming van onze nationale veiligheid. Tegelijkertijd en daarmee in balans dienen belangrijke rechtsstatelijke thema's, gericht op een toereikende rechtsbescherming voor de burger, hun volledige erkenning en toepassing te krijgen. De CTIVD zal zich blijvend inzetten inzicht te geven in de juiste balans daarbij.

Tijdelijk adres:
Frederikkazerne, gebouw 35
Van Alkemadelaan 786 | 2597 Den Haag
Postbus 90701 | 2509 LS Den Haag

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl