# Referendum over de Wet op de inlichtingen- en veiligheidsdiensten 2017

Op 21 maart 2018 is er in Nederland een raadgevend referendum. U kunt dan stemmen over de vraag: bent u voor of tegen de Wet op de inlichtingen- en veiligheidsdiensten 2017? Waar gaat deze wet precies over? Wat zijn de verschillen met de huidige wet? En waarom wordt er een referendum over gehouden? Dat en meer leest u op de website **www.referendumwiv2017.nl**. In dit document vindt u alle teksten die op deze website staan.

## De Referendumcommissie

De informatie in deze pdf en op de website **www.referendumwiv2017.nl** komt van de Referendumcommissie. Deze onafhankelijke commissie heeft als wettelijke taak om de kiezers te informeren over de inhoud van de wet waar het referendum over gaat. Daarnaast bepaalt de commissie de aanduiding van de wet op het stembiljet, stelt ze de datum van het referendum vast en verleent ze subsidies voor activiteiten die het debat over de Wiv 2017 stimuleren.

## Inhoudsopgave

REFERENDUM commissie

# De Wiv 2017 in het kort

Op 21 maart 2018 is er in Nederland een raadgevend referendum over de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017). Op deze pagina leest u in het kort waar deze wet over gaat, wat de aanleiding ervoor is en wat de grootste verschillen zijn met de huidige wet: de Wiv 2002.

## Over het werk van de Nederlandse inlichtingen- en veiligheidsdiensten

De Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) gaat over het werk van de Nederlandse inlichtingen- en veiligheidsdiensten: wat zijn hun taken, welke middelen mogen ze daarvoor inzetten en hoe is het toezicht geregeld? De wet geldt zowel voor de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) als voor de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Hun opdracht is om de veiligheid en de democratische rechtsorde te helpen beschermen door het verzamelen en analyseren van informatie. Denk daarbij aan dreigingen en risico's voor de samenleving en voor vredesoperaties, en aan (internationaal) terrorisme. Dat geldt voor de AIVD, maar ook voor de MIVD voor zover de krijgsmacht daarbij betrokken is of kan raken.

## Vervanger van de Wet op de inlichtingen- en veiligheidsdiensten 2002

De nieuwe wet vervangt de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). Deze wet is volgens de regering op een aantal punten verouderd. Zo zijn meer mensen internet gaan gebruiken en heeft vrijwel iedereen een smartphone. In 2002 verliep de internationale telecommunicatie voor het merendeel door de lucht, via de ether. Inmiddels communiceren we wereldwijd grotendeels via glasvezel- of koperkabels. Mobiele telefoons, laptops en andere apparaten maken contact met modems of zendmasten, die vervolgens informatie doorgeven over de kabel. Onder de huidige wet mogen de AIVD en de MIVD deze kabelgebonden communicatie slechts beperkt onderscheppen. Een belangrijke wijziging in de Wiv 2017 is de verruiming van hun bevoegdheden op dit gebied.

## Meer mogelijkheden om communicatie te onderscheppen

Door de verruiming van hun bevoegdheden kunnen de AIVD en de MIVD onder de nieuwe wet kabelgebonden communicatie breder onderscheppen dan nu. Dat kan ertoe leiden dat er bij de diensten ook gegevens terechtkomen over personen die niet kwaadwillend zijn. In dit verband wordt in het publieke debat soms van een 'sleepnet' gesproken en wordt de wet zelf ook wel 'Sleepwet' genoemd. De diensten mogen deze communicatie echter niet volledig ongericht onderscheppen. Ze mogen alleen gegevens verzamelen met een bepaald doel en moeten niet-relevante gegevens zo snel mogelijk vernietigen. Om ervoor te zorgen dat dit zorgvuldig en rechtmatig gebeurt, wordt het onafhankelijk toezicht op het werk van de diensten uitgebreid.

## Veiligheid en privacy

De nieuwe wet vergroot het bereik van de diensten en daarmee de mogelijkheid dat er inbreuk wordt gemaakt op de privacy van burgers. Door een pakket aan extra waarborgen, zoals een uitgebreider onafhankelijk toezicht op de diensten, probeert de wet een balans aan te brengen tussen het belang van de nationale veiligheid en de privacy van individuele personen. Het publieke debat richt zich op de vraag of die balans goed is gekozen.

## Meer weten?

Op de pagina's hierna leest u meer over de aanleiding voor de Wiv 2017 en over de verschillen met de huidige wet. Ook vindt u in dit document een samenvatting van alle hoofdstukken van de wet. Het document sluit af met de antwoorden op een aantal veelgestelde vragen over de Wiv 2017 en het referendum op 21 maart 2018.

## Breed onderscheppen van telecommunicatie

***Een van de grootste verschillen tussen de Wet op de inlichtingen- en veiligheidsdiensten 2017 en de huidige wet is dat de AIVD en de MIVD (de diensten) de bevoegdheid krijgen om breed telecommunicatie af te tappen die via de ether én via de kabel verloopt. Dit gaat gepaard met meer toezicht.***

De diensten hebben ***vooraf toestemming*** nodig van de minister en de onafhankelijke Toetsingscommissie Inzet Bevoegdheden (TIB). De TIB toetst of de toestemming volgens de wettelijke regels kan worden verleend.

De diensten ***tappen een brede stroom van telecommunicatie af***, bijvoorbeeld tussen een Syrische stad en Nederland. Dit doen ze altijd ***gericht op een specifiek doel***. Niet-relevante gegevens moeten zo snel mogelijk worden vernietigd.

De onafhankelijke Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) ***controleert tijdens het aftappen van de communicatie en achteraf*** of de diensten zich aan de wettelijke regels houden/hebben gehouden.

REFERENDUM commissie

# Aanleiding voor de Wet op de inlichtingen- en veiligheidsdiensten 2017

De Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) vervangt de wet die nu nog van kracht is: de Wiv 2002. Volgens de regering zijn er verschillende redenen waarom het noodzakelijk is om deze wet te vervangen. De belangrijkste redenen zijn de toegenomen cyberdreiging en de veranderingen in het digitale communicatieverkeer.

## Verhoogde terreur- en cyberdreiging

Sinds 2002 is het aantal terroristische aanslagen en dreigingen in de wereld sterk toegenomen. Internationale troepenmachten voeren operaties uit om de organisaties daarachter te bestrijden. Daarnaast worden bedrijven en overheidsorganisaties steeds vaker geconfronteerd met cyberaanvallen. Daarbij gaat het bijvoorbeeld om sabotage van digitale systemen of diefstal van vertrouwelijke gegevens. Deze aanvallen en dreigingen kunnen een gevaar zijn voor de nationale veiligheid en de democratische rechtsorde.

Het is de taak van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) om die veiligheid en rechtsorde te helpen beschermen. Dat doen ze door informatie te verzamelen, waardoor ze een grotere kans hebben om dreigingen en risico's tijdig te herkennen. Daarvoor kunnen ze verschillende middelen (bevoegdheden) inzetten. Een van de belangrijkste middelen is het onderscheppen van telecommunicatie, zoals telefoongesprekken, e-mail- en appverkeer.

## Veranderingen in het digitale communicatieverkeer

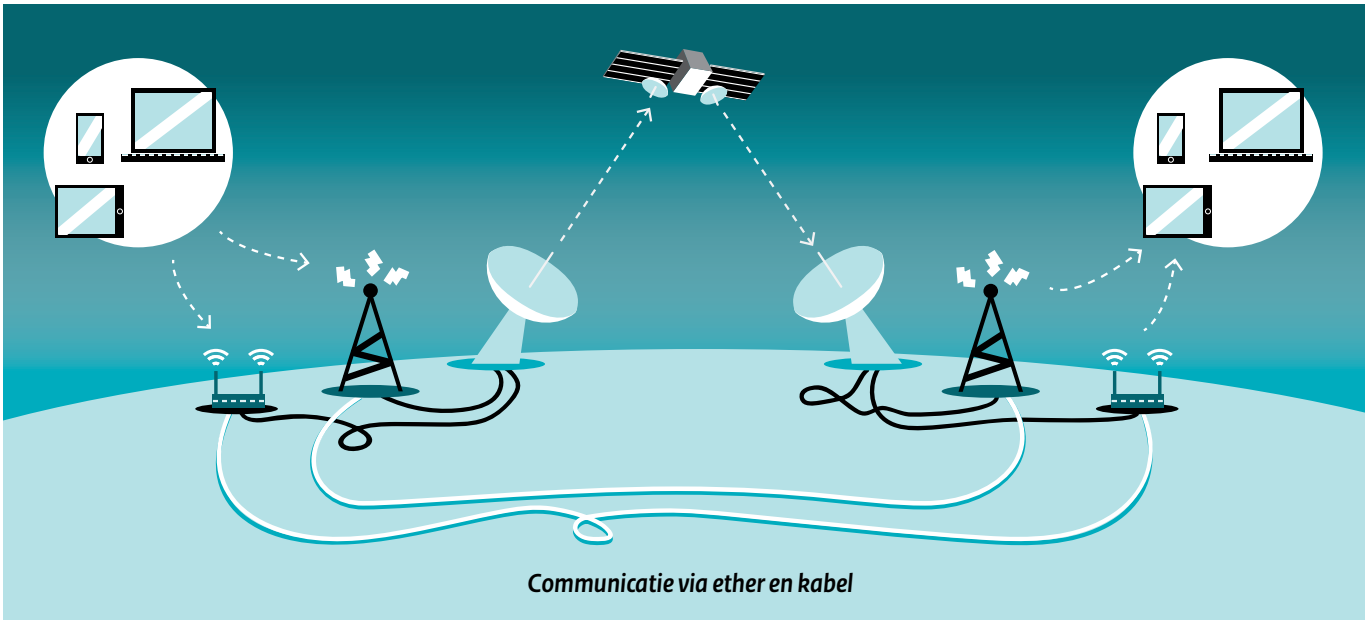
In de telecommunicatie is de laatste 15 jaar veel veranderd. In 2002 verliep deze communicatie internationaal gezien voor het merendeel door de lucht, via de ether. Inmiddels verloopt de telecommunicatie wereldwijd grotendeels via glasvezel- of koperkabels. Mobiele telefoons, laptops en andere apparaten maken contact met modems of zendmasten, die vervolgens informatie doorgeven over de kabel.

Als het gaat om deze kabelgebonden telecommunicatie biedt de Wiv 2002 beperkte mogelijkheden. De diensten mogen deze communicatie nu alleen 'gericht' onderscheppen. Dat wil zeggen dat de communicatie gekoppeld moet zijn aan een bepaalde persoon of organisatie. Denk aan het aftappen van telefoon- of e-mailverkeer van en naar een bepaald nummer of IP-adres. Het breed onderscheppen van kabelgebonden communicatie (dus niet gekoppeld aan een bepaalde persoon of organisatie) is onder de Wiv 2002 niet toegestaan.

Het gevolg van de huidige regels is dat het merendeel van de telecommunicatie buiten het zicht van de diensten blijft. Het is namelijk lang niet altijd mogelijk om deze communicatie gericht te onderscheppen. Zo weten de diensten niet altijd op voorhand welke personen zij in de gaten moeten houden. Bovendien communiceren die personen vaak niet via een vast telefoonnummer of IP-adres, maar maken zij anoniem gebruik van het internet, bijvoorbeeld via het wifinetwerk van een restaurant of de chatfunctie van een computergame.

## De nieuwe wet

Om die reden is het volgens de regering noodzakelijk dat de diensten de bevoegdheid krijgen om kabelgebonden telecommunicatie ruimer te kunnen onderscheppen. Met deze bevoegdheid verwacht de regering dat de diensten beter in staat zijn om terreurdreigingen tijdig te herkennen. De ruimere bevoegdheid is volgens de regering ook nodig om cyberaanvallen tegen te gaan en om op gelijke voet samen te werken met buitenlandse veiligheidsdiensten.



*Communicatie via ether en kabel*

# Aanleiding voor de Wet op de inlichtingen- en veiligheidsdiensten 2017

De Wiv 2017 maakt deze extra bevoegdheid mogelijk. De nieuwe wet vergroot zo het bereik van de diensten, maar ook de mogelijkheid dat er inbreuk wordt gemaakt op de privacy van burgers. Door een pakket aan waarborgen, zoals een uitgebreider onafhankelijk toezicht op het werk van de diensten, probeert de wet een balans aan te brengen tussen het belang van de nationale veiligheid en de privacy van individuele personen. Het publieke debat richt zich op de vraag of die balans goed is gekozen.

### Meer weten?

- Op de volgende pagina's leest u meer over de veranderingen in de nieuwe wet. Hoe deze wet tot stand is gekomen leest u op pagina 28.
- De aanleiding voor de wet is ook beschreven in de Memorie van Toelichting bij de Wiv 2017 (paragraaf 1.3 en 1.4). Deze is te vinden op Overheid.nl: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html**.

REFERENDUM commissie

# Verschillen tussen de Wiv 2002 en de Wiv 2017

De Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) verschilt op een groot aantal punten van de huidige wet, de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). Op de volgende pagina's worden enkele belangrijke verschillen beschreven. Deze verschillen zijn:

## 8 verschillen komen aan de orde:

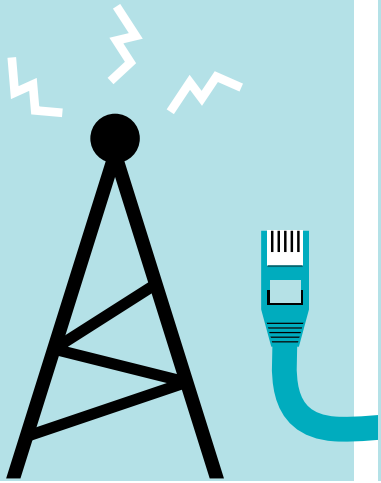


# De Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017)

## Enkele belangrijke verschillen met de Wiv 2002

### Meer bevoegdheden

**1.** De AIVD en MIVD kunnen ***breed telecommunicatie aftappen die via de ether én via de kabel verloopt*** (aan de hand van een vooraf geaccordeerde onderzoeksopdracht). Ze moeten gegevens die niet relevant zijn, direct vernietigen. Gegevens die zij na ***3 jaar*** nog niet op hun relevantie hebben onderzocht, moeten zij op dat moment vernietigen.



### Meer toezicht

**2.** Om een bevoegdheid in te zetten die de privacy sterk aantast, is ***vooraf toestemming nodig van de minister én van een nieuwe onafhankelijke commissie***: de Toetsingscommissie Inzet Bevoegdheden (TIB). De commissie beoordeelt of de toestemming door de minister rechtmatig is verleend. Zo niet, dan vervalt de toestemming.

**3.** De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) krijgt een ***onafhankelijke afdeling Klachtbehandeling***. Deze behandelt klachten van burgers over het handelen van de AIVD en de MIVD. De afdeling doet hierover een ***bindende uitspraak***, die de minister moet opvolgen. De afdeling Klachtbehandeling gaat daarnaast functioneren als ***meldpunt voor misstanden*** binnen de AIVD of de MIVD.

**4.** De AIVD en de MIVD mogen ***ongeëvalueerde gegevens alleen aan buitenlandse collega-diensten verstrekken met toestemming van de minister***. Daarbij gaat het om gegevens waarvan de diensten nog niet hebben onderzocht of ze relevant zijn voor hun onderzoeken. De CTIVD wordt direct op de hoogte gesteld en controleert of de verstrekking rechtmatig is.

### Duidelijkere regels

**5.** De regels voor het hacken van computers zijn in de Wiv 2017 explicieter geformuleerd. Volgens deze regels mogen de diensten ook een computer hacken ***via een computer of netwerk van een derde.***

**6.** Activiteiten verbonden aan ***DNA-onderzoek*** krijgen in de Wiv 2017 een expliciete ***wettelijke grondslag***. Deze regels bepalen onder meer dat de diensten DNA-profielen mogen maken op basis van gevonden celmateriaal. Ze mogen deze profielen ***5 jaar bewaren***.

**7.** De bestaande ***criteria voor samenwerking met buitenlandse collega-diensten*** staan nu expliciet ***in de wet***. In principe mogen de AIVD en de MIVD alleen gegevens delen met diensten die aan de gestelde criteria voldoen.

**8.** De diensten mogen alleen met ***toestemming van de Rechtbank Den Haag communicatie aftappen tussen journalisten en hun bronnen en tussen advocaten en hun cliënten***. Ook is toestemming van de rechtbank nodig als een dienst informatie aan het OM wil doorgeven die is verkregen door het aftappen van communicatie tussen een advocaat en zijn cliënt.

REFERENDUM commissie

# Verschillen tussen de Wiv 2002 en de Wiv 2017

## Betekenis van enkele veelgebruikte termen

Op deze pagina's wordt regelmatig het woord 'diensten' gebruikt. Daarmee wordt bedoeld: de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Leest u 'de betrokken minister' of 'de verantwoordelijke minister', dan wordt de minister bedoeld die voor de betreffende dienst verantwoordelijk is. Voor de AIVD is dat de minister van Binnenlandse Zaken en Koninkrijksrelaties, voor de MIVD de minister van Defensie en voor de coördinatie van het werk van beide diensten de minister-president.

## 1. Breed onderscheppen van telecommunicatie via de kabel

Voor de Nederlandse inlichtingen- en veiligheidsdiensten, AIVD en MIVD, is het onderscheppen van telecommunicatie een belangrijk middel om informatie te verzamelen. Denk aan het aftappen van telefoongesprekken, e-mail- en appverkeer. In de Wiv 2017 worden hun bevoegdheden op dit gebied verruimd.

### Wat verandert er in de nieuwe wet?

In 2002 verliep de internationale telecommunicatie voor het merendeel door de lucht, via de ether. Inmiddels communiceren we wereldwijd grotendeels via glasvezel- of koperkabels. Mobiele telefoons, laptops en andere apparaten maken contact met modems of zendmasten, die vervolgens informatie doorgeven over de kabel. Onder de huidige wet mogen de AIVD en de MIVD deze kabelgebonden telecommunicatie alleen onderscheppen als die gericht is op een bepaalde persoon of organisatie. Onder de Wiv 2017 mogen de diensten ook breder communicatie onderscheppen die via de kabel verloopt. Dit mogen ze alleen doen in het kader van een vooraf geformuleerde en geaccordeerde onderzoeksopdracht. Daarom spreekt de wet van 'onderzoeksopdrachtgerichte interceptie' (OOG-interceptie).

### Waarom deze nieuwe bevoegdheid?

Op pagina 3 van dit document wordt de aanleiding voor de Wiv 2017 beschreven. Daarbij worden verschillende redenen genoemd waarom het volgens de regering nodig is om kabelgebonden telecommunicatie breder te kunnen onderscheppen. De belangrijkste reden is dat de AIVD en de MIVD bij het onderzoeken van een bepaalde dreiging soms nog geen zicht hebben op specifieke personen. Daar is een verkennend onderzoek voor nodig van een grotere hoeveelheid communicatiegegevens.

Vanwege die grote hoeveelheid wordt in het publieke debat soms van een 'sleepnet' gesproken als het gaat om het breed onderscheppen van communicatie. De wet bepaalt echter dat de diensten die communicatie niet geheel ongericht mogen onderscheppen. Ze mogen alleen gegevens verzamelen met een specifiek doel (een bepaalde dreiging) en alleen als dat noodzakelijk is om hun werk goed te kunnen doen. Ook moeten ze gegevens die niet relevant zijn zo snel mogelijk verwijderen.

### Wanneer mogen de diensten deze bevoegdheid inzetten?

De diensten mogen alleen breed communicatie onderscheppen als dat nodig is voor een bepaald doel. Dat doel is gekoppeld aan een onderzoeksopdracht. Een voorbeeld van zo'n opdracht is het onderzoeken van alle internetcommunicatie tussen de Syrische stad Raqqa en Nederland. Een reden daarvoor kan zijn om mogelijke jihadisten te achterhalen.

De ministers die voor de veiligheidsdiensten verantwoordelijk zijn, bepalen of de diensten de genoemde bevoegdheid mogen inzetten. Deze beslissing moeten de ministers vervolgens voorleggen aan een speciale commissie (de Toetsingscommissie Inzet Bevoegdheden, TIB). Alleen als die commissie toestemming geeft, mogen de diensten beginnen met het aftappen van de communicatie. Telecomaanbieders zijn verplicht hieraan mee te werken.

REFERENDUM commissie

# Verschillen tussen de Wiv 2002 en de Wiv 2017

## Hoe verloopt het proces?

Breed onderscheppen van dataverkeer (OOG-interceptie) gaat in stappen. Voor elke stap is vooraf toestemming nodig van de verantwoordelijke minister en de TIB. Ten eerste schatten de diensten in waar de gezochte communicatie op de kabel vermoedelijk te vinden is. Vervolgens tappen ze dat deel van de kabel af. Daarna worden de gegevens die niet relevant zijn eruit gefilterd. Denk aan gegevens over het gebruik van Netflix of Spotify.

De gegevens die overblijven, worden in 2 stromen verdeeld: metadata en inhoudelijke gegevens. Metadata zijn gegevens over telecommunicatie die niet de inhoud van die communicatie weergeven, maar alleen informatie geven over bijvoorbeeld de gebruikte nummers of IP-adressen, de start- en eindtijd van de communicatie of de gebruikte communicatiemiddelen. Op deze gegevens voeren de diensten een geautomatiseerde metadata-analyse uit.

Uit de inhoudelijke gegevens selecteren de diensten de gegevens die zij verder gaan onderzoeken. Die selectie is altijd gekoppeld aan specifieke personen, organisaties of onderwerpen. Blijken de gegevens daadwerkelijk relevant te zijn, dan kunnen ze gebruikt worden voor alle lopende onderzoeken.

### Hoelang mogen de diensten de verzamelde gegevens bewaren?

De diensten mogen de gegevens die zij hebben onderschept, maximaal 3 jaar bewaren nadat ze verzameld of ontsleuteld zijn. In de Wiv 2002 bedraagt die termijn 1 jaar. Gegevens waarvan zij constateren dat ze niet relevant zijn voor het betreffende onderzoek of voor een ander lopend onderzoek, moeten zij direct vernietigen. Gegevens die zij na 3 jaar nog niet op hun relevantie hebben onderzocht, moeten zij op dat moment vernietigen.

### Meer informatie over OOG-interceptie

- De wettelijke regels voor OOG-interceptie staan beschreven in artikel 48 t/m 50 van de Wiv 2017. De wettekst is te vinden op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html**.
- De artikelen worden toegelicht in de Memorie van Toelichting bij de Wiv 2017 (paragraaf 3.3.4.4.7). Deze staat op Overheid.nl: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html.**
- Artikel 48 t/m 50 staan in hoofdstuk 3 van de Wiv 2017. Een samenvatting van dit hoofdstuk vindt u op pagina 17 van dit document.

REFERENDUM commissie

# Verschillen tussen de Wiv 2002 en de Wiv 2017

## 2. Toetsing op de inzet van bijzondere bevoegdheden

Om hun taken uit te voeren kunnen de AIVD en MIVD verschillende bijzondere bevoegdheden inzetten, zoals het doorzoeken van woningen, het onderscheppen van telecommunicatie en het hacken van computers. Voor een aantal van deze bevoegdheden geldt dat de diensten ze alleen mogen inzetten als ze daarvoor toestemming hebben van de minister die voor de dienst verantwoordelijk is. Daarbij gaat het om de bevoegdheden die de meeste inbreuk maken op de privacy van individuele personen.

### Wat verandert er in de nieuwe wet?

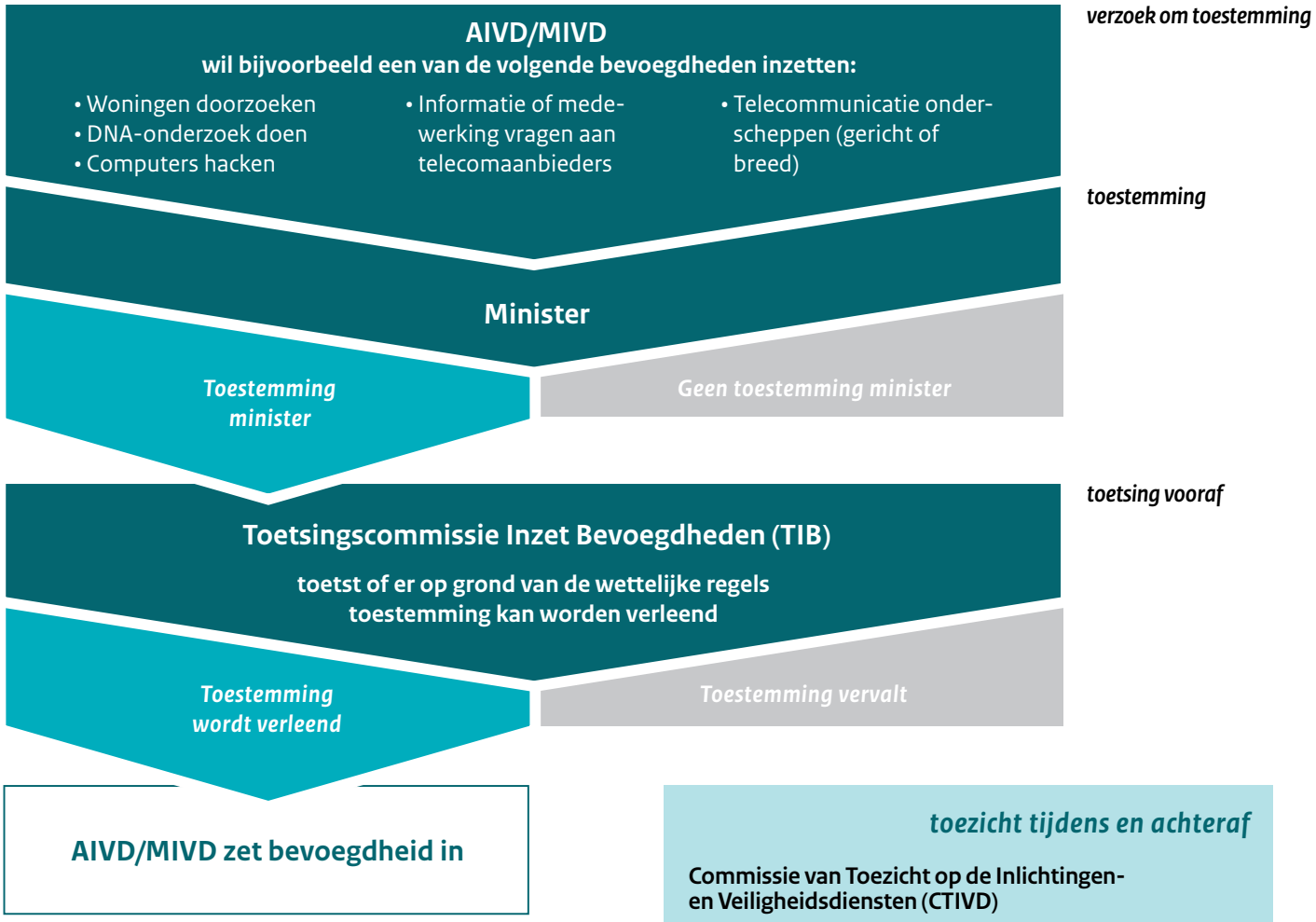
Onder de nu geldende Wiv 2002 is de toestemming van de minister voldoende om een van de genoemde bevoegdheden te kunnen inzetten. Onder de Wiv 2017 moet de minister deze toestemming eerst voorleggen aan de Toetsingscommissie Inzet Bevoegdheden (TIB). Deze commissie beoordeelt of de toestemming rechtmatig is verleend. Alleen als dit oordeel positief is, mag de dienst de bevoegdheid inzetten.

De TIB is een nieuwe commissie die in oprichting is. Deze commissie bestaat uit 3 leden, van wie er minimaal 2 ervaren oud-rechters zijn. Zij worden voor 6 jaar benoemd en kunnen niet tegelijkertijd lid zijn van de commissie van toezicht (zie punt 3).

### Waarom deze verandering?

De oprichting van deze toetsingscommissie komt voort uit uitspraken van het Europees Hof voor de Rechten van de Mens. Deze hadden te maken met het gebruik van bijzondere bevoegdheden door de diensten. Daarover zijn extra bepalingen opgenomen in de nieuwe wet.

## Toetsing vooraf door de TIB




*toezicht tijdens en achteraf*

**Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)**

controleert tijdens de inzet van de bevoegdheden en achteraf of de dienst zich aan de wettelijke regels houdt/heeft gehouden

# Verschillen tussen de Wiv 2002 en de Wiv 2017

Zo maakt de Wiv 2017 het mogelijk om breed telecommunicatie te onderscheppen die via de kabel verloopt (zie punt 1). Voor communicatie door de lucht (via de ether) was dit onder de Wiv 2002 al toegestaan. De sterk gegroeide telecommunicatie verloopt inmiddels grotendeels via glasvezel- of koperkabels. Mobiele telefoons, laptops en andere apparaten maken contact met modems of zendmasten, die vervolgens informatie doorgeven over de kabel. Om ook deze communicatie te kunnen onderscheppen, zijn de bevoegdheden van de diensten uitgebreid.

Deze uitbreiding brengt met zich mee dat de diensten ook communicatie kunnen onderscheppen van burgers die niet kwaadwillend zijn. Weliswaar mogen de diensten deze gegevens niet gebruiken, maar toch maakt dit een inbreuk op de privacy van deze mensen. Daarom moet de TIB waarborgen dat er een goede afweging wordt gemaakt voordat deze bevoegdheid wordt ingezet.

### Meer informatie over de toetsingscommissie

- De taken, samenstelling en werkwijze van de toetsingscommissie staan beschreven in artikel 32 t/m 37 van de Wiv 2017. De wettekst is te vinden op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html.**
- De artikelen worden toegelicht in de Memorie van Toelichting bij de Wiv 2017 (paragraaf 3.3.1). Deze staat op Overheid.nl: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html.**
- Artikel 32 t/m 37 staan in hoofdstuk 3 van de Wiv 2017. Een samenvatting van dit hoofdstuk vindt u op pagina 17 van dit document.

## 3. Bindende klachtenregeling en meldpunt voor misstanden

Bij de uitvoering van hun taken moeten de AIVD en de MIVD zich vanzelfsprekend houden aan de wet. Om dit te waarborgen wordt er toezicht gehouden op de manier waarop de diensten hun taken uitvoeren. Dat gebeurt door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Deze onafhankelijke commissie bestaat al sinds de Wiv 2002, maar ondergaat met de Wiv 2017 een aantal veranderingen.

### Wat verandert er in de nieuwe wet?

Ten eerste bepaalt de nieuwe wet dat binnen de CTIVD een strikt onderscheid wordt gemaakt tussen een afdeling Toezicht en een afdeling Klachtbehandeling. Deze afdelingen opereren afzonderlijk van elkaar (artikel 97).

Ten tweede krijgt de afdeling Klachtbehandeling een sterkere positie. Bij deze afdeling kunnen burgers klachten indienen over het handelen van de AIVD of de MIVD. De afdeling beoordeelt vervolgens of er onrechtmatig gehandeld is. Is dat het geval, dan meldt de afdeling dat aan de betrokken minister. Daarbij kan de afdeling bepalen dat de AIVD of de MIVD moet stoppen met een onderzoek of met de uitoefening van een bepaalde bevoegdheid, of dat zij de verwerkte gegevens moet vernietigen. De minister moet zich vervolgens aan het oordeel van de afdeling Klachtbehandeling houden (artikel 124). Onder de huidige wet, de Wiv 2002, hoeft dat niet.

### Waarom deze veranderingen?

Dat burgers klachten kunnen indienen bij de CTIVD is niet nieuw. Maar op dit moment heeft de afdeling Klachtbehandeling geen zelfstandige positie. Daardoor kan het voorkomen dat een klacht wordt behandeld door dezelfde persoon als die het toezicht op de betreffende kwestie heeft gehouden. Dit kan de onafhankelijkheid van de klachtbehandeling aantasten.

Bovendien heeft de CTIVD nu alleen een adviserende taak als het om klachten gaat. De minister is momenteel niet verplicht om de uitspraak van de CTIVD te volgen. Omdat in de Wiv 2017 de bevoegdheden van de diensten worden verruimd, vindt de regering het belangrijk dat daar een stevige klachtenregeling tegenover staat. Daarom is voor deze bindende regeling gekozen.

### Wat verandert er nog meer in de nieuwe wet?

Een derde verandering in de nieuwe wet is dat er een regeling komt voor de melding van misstanden. Dit betekent dat medewerkers van de AIVD en de MIVD het bij de afdeling Klachtbehandeling kunnen melden als ze een vermoeden hebben van een misstand binnen hun dienst. Onder de huidige wet hebben ze die mogelijkheid niet.

De afdeling Klachtbehandeling onderzoekt de meldingen over mogelijke misstanden en rapporteert hierover aan de betrokken minister. Deze moet binnen 2 weken laten weten wat hij met het oordeel van de afdeling doet. De minister stuurt dit oordeel en zijn reactie daarop naar het parlement (artikel 131). In de praktijk zal het meestal gaan naar de Commissie Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer (CIVD), ook wel de 'commissie-Stiekem' genoemd.

### Waarom deze verandering?

Er bestaat al een klokkenluidersregeling voor ambtenaren, maar ambtenaren van de AIVD en de MIVD zijn hiervan uitgesloten. Dat heeft te maken met het heimelijke karakter van hun werkzaamheden. Vanwege het belang van de betrouwbaarheid en integriteit van die diensten is nu een speciale regeling opgesteld om interne misstanden te kunnen melden.

### Meer informatie over de CTIVD

- De taken, samenstelling en werkwijze van de CTIVD staan beschreven in artikel 97 t/m 134 van de Wiv 2017. De wettekst is te vinden op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html.**

# Verschillen tussen de Wiv 2002 en de Wiv 2017

- De artikelen worden toegelicht in de Memorie van Toelichting bij de Wiv 2017 (paragraaf 7.1 t/m 7.3). Deze staat op Overheid.nl: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html.**
- Artikel 97 t/m 134 staan in hoofdstuk 7 van de Wiv 2017. Een samenvatting van dit hoofdstuk vindt u op pagina 24 van dit document.

## 4. Toestemming vereist voor het delen van ruwe gegevens met buitenlandse diensten

De AIVD en de MIVD mogen onder voorwaarden gegevens die zij hebben verzameld, delen met inlichtingen- en veiligheidsdiensten van andere landen. Dat is al zo onder de Wiv 2002 en dat blijft zo onder de Wiv 2017. In de Wiv 2017 is echter een nieuwe regeling opgenomen voor het delen van 'ongeëvalueerde' gegevens met andere diensten. Dit zijn gegevens waarvan de AIVD en de MIVD nog niet hebben onderzocht of ze relevant zijn voor hun onderzoeken. Daarbij gaat het bijvoorbeeld om gegevens die met het oog op een bepaalde dreiging zijn verzameld door het breed onderscheppen van telecommunicatie (zie punt 1). Hier kunnen ook gegevens bij zitten over personen die niet kwaadwillend zijn.

### Wat verandert er in de nieuwe wet?

De Wiv 2017 bepaalt dat de diensten ongeëvalueerde gegevens alleen aan buitenlandse collega-diensten mogen doorgeven als ze daarvoor toestemming hebben van de verantwoordelijke minister. Gaat het om gegevens die zijn verzameld door het breed onderscheppen van telecommunicatie, dan moeten ze daarnaast meteen de commissie van toezicht (CTIVD) op de hoogte brengen. Deze controleert of de verstrekking van de gegevens rechtmatig plaatsvindt.

Verder geldt dat de AIVD en de MIVD de gegevens in principe alleen mogen doorgeven aan buitenlandse diensten waarmee ze een samenwerkingsrelatie hebben (artikel 62 en 89) (zie punt 7). Deze diensten moeten aan een aantal criteria voldoen op het gebied van bijvoorbeeld mensenrechten en professionaliteit.

Wil de AIVD of de MIVD de gegevens ook aan andere diensten doorgeven? Dan mag dat alleen als dat noodzakelijk is om hun taken goed uit te voeren en als daar een dringende en gewichtige reden voor is. Ook hiervoor is de toestemming van de minister nodig (artikel 64). In een brief aan de Tweede Kamer van 15 december 2017[1] schrijft de minister van BZK, mede namens de minister van Defensie, dat die uitzondering alleen mogelijk is als er - door deze informatie niet te geven- mensenlevens in gevaar kunnen komen.

Tot slot bepaalt de Wiv 2017 dat de AIVD en de MIVD bij het verstrekken van gegevens aan buitenlandse collega-diensten de voorwaarde kunnen stellen dat deze diensten de gegevens niet aan anderen doorgeven. De betrokken minister, of namens deze het hoofd van de dienst, kan hier later incidenteel en onder bepaalde voorwaarden van afwijken en besluiten dat de gegevens toch mogen worden doorgegeven (artikel 65).

### Waarom deze nieuwe regeling?

Onder de Wiv 2017 wordt het voor de diensten mogelijk om breed telecommunicatie te onderscheppen die via de kabel verloopt. Onder de Wiv 2002 mocht dit alleen bij telecommunicatie die via de ether verliep. Hierdoor – en doordat het gebruik van internet enorm is toegenomen – krijgen de diensten veel meer gegevens tot hun beschikking dan voorheen. Omdat ze 3 jaar de tijd hebben om die op hun relevantie te onderzoeken, zitten daar veel ongeëvalueerde gegevens bij, waaronder mogelijk ook gegevens van onschuldige burgers.

Gegevens die door brede onderschepping verkregen zijn, kunnen nuttig zijn voor onderzoeken van collega-diensten, bijvoorbeeld voor de bestrijding van grensoverschrijdend terrorisme. Tegelijkertijd kunnen ze de privacy aantasten van burgers die niet kwaadwillend zijn. De nieuwe regeling moet waarborgen dat er zorgvuldig beoordeeld wordt of het noodzakelijk is om deze gegevens met buitenlandse diensten te delen.

### Meer informatie over het verstrekken van gegevens aan buitenlandse diensten

- De regels voor het verstrekken van gegevens aan buitenlandse diensten staan beschreven in artikel 62, 64 en 89 van de Wiv 2017. De wettekst is te vinden op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html.**
- De artikelen worden toegelicht in de Memorie van Toelichting bij de Wiv 2017 (paragraaf 3.6.3 en 6.3.3). Deze staat op Overheid.nl: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html.**
- Artikel 62 en 64 staan in hoofdstuk 3 van de Wiv 2017 en artikel 89 staat in hoofdstuk 6. Een samenvatting van deze hoofdstukken vindt u op pagina 17 en 23 van dit document.

## 5. Duidelijkere regels voor het hacken van computers

De laatste jaren is het hacken, ofwel binnendringen van computers een steeds belangrijker middel geworden voor de veiligheidsdiensten om onder meer terreur- en cyberdreigingen tijdig op het spoor te komen. In de Wiv 2002 is hier al een regeling voor getroffen. Deze is in de Wiv 2017 overgenomen, maar op een paar punten aangescherpt. Overigens gaat het hier niet alleen om computers, maar ook om smartphones, servers en andere apparaten en netwerken die automatisch gegevens verwerken. In de Wiv worden dat 'geautomatiseerde werken' genoemd.

[1] Deze brief is te vinden op Rijksoverheid.nl: **http://bit.ly/2EReg83.**

REFERENDUM commissie

# Verschillen tussen de Wiv 2002 en de Wiv 2017

### Wat verandert er in de nieuwe wet?

In de Wiv 2002 zijn impliciet een aantal normen verwerkt voor het hacken, ofwel binnendringen van computers. In de Wiv 2017 zijn die normen expliciet onder woorden gebracht. Daardoor komen sommige bevoegdheden nu duidelijker naar voren.

Ten eerste stelt de Wiv 2017 nu expliciet dat het mogelijk is om toegang tot de gewenste computer te verwerven via een computer of systeem van een andere persoon of organisatie (een 'derde'). Vaak zal dit een computer of netwerk zijn van een provider of leverancier. Maar het kan ook een apparaat zijn van een individuele persoon, bijvoorbeeld een gebruiker van dezelfde server. De diensten zullen deze mogelijkheid alleen gebruiken als ze op geen enkele andere manier kunnen binnendringen in de gewenste computer. Ze moeten hiervoor apart toestemming vragen aan de verantwoordelijke minister.

Ten tweede is in de Wiv 2017 expliciet de bevoegdheid opgenomen om in een computer technische voorzieningen te installeren, bijvoorbeeld software die het mogelijk maakt om een camera of microfoon in de computer te activeren. Hierdoor kan een ruimte worden geobserveerd of een gesprek worden opgenomen. Daarnaast bepaalt de Wiv 2017 dat de diensten eerst een technische verkenning kunnen doen, voordat ze daadwerkelijk in een computer binnendringen. Zo kunnen zij gerichter te werk gaan. Voor de inzet van deze bevoegdheden is toestemming van de minister en de TIB vereist.

### Waarom deze veranderingen?

De regels voor het hacken blijven voor een groot deel gelijk aan de regels in de Wiv 2002. De veranderingen in de Wiv 2017 zijn vooral ingegeven door de snelle technologische ontwikkelingen en de wens om een duidelijke wettelijke basis te geven aan het optreden van de inlichtingen- en veiligheidsdiensten.

Van de bepalingen die nu expliciet in de wet zijn opgenomen, valt vooral de mogelijkheid op om via een andere computer binnen te dringen in de gewenste computer. Daarmee wordt niet alleen inbreuk gemaakt op de privacy van de gebruiker van de gewenste computer, maar ook op die van de andere computer. De reden dat dit toch in de wet is opgenomen, is dat het steeds moeilijker is om rechtstreeks binnen te dringen in de computers van de personen die de diensten onderzoeken. Deze personen weten steeds beter hoe zij hun computers het best kunnen beveiligen. De tussenstap via een andere computer biedt daarvoor vaak uitkomst.

Doordat deze bevoegdheden nu duidelijk in de wet zijn opgenomen, gelden hier ook alle voorwaarden voor die voor de andere bijzondere bevoegdheden gelden. Zo moet de inzet ervan noodzakelijk zijn en in verhouding staan tot het doel dat ermee wordt beoogd. Ook moet de toestemming die de minister heeft gegeven, worden getoetst door de Toetsingscommissie Inzet Bevoegdheden (TIB) (zie punt 2).

### Meer informatie over het hacken van computers

- De regels voor het hacken van computers staan beschreven in artikel 45 van de Wiv 2017. De wettekst is te vinden op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html.**
- Dit artikel wordt toegelicht in de Memorie van Toelichting bij de Wiv 2017 (paragraaf 3.3.4.4.6). Deze staat op Overheid.nl: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html.**
- Artikel 45 staat in hoofdstuk 3 van de Wiv 2017. Een samenvatting van dit hoofdstuk vindt u op pagina 17 van dit document.

## 6. Duidelijkere regels voor DNA-onderzoek

Om de identiteit van een persoon vast te stellen of te controleren, kunnen de AIVD en de MIVD DNA-onderzoek doen. Dit houdt in dat ze het celmateriaal onderzoeken dat ze hebben gevonden op een voorwerp dat deze persoon heeft aangeraakt. Denk aan een sigarettenpeuk of een glas. De Wiv 2002 biedt de diensten al de mogelijkheid om dit DNA-onderzoek te doen. In de Wiv 2017 zijn de regels daarvoor aangevuld.

### Wat verandert er in de nieuwe wet?

Bij het doen van DNA-onderzoek volgen de diensten een aantal regels. Deze regels zijn slechts gedeeltelijk vermeld in de Wiv 2002. In deze wet zijn geen bepalingen opgenomen over onder meer het bewaren van celmateriaal en het beheren van een DNA-gegevensbestand. Het Europees Hof voor de Rechten van de Mens heeft bepaald dat ook daarvoor een expliciete wettelijke grondslag nodig is. In de Wiv 2017 is dat gebeurd (artikel 43).

### Welke regels stelt de wet voor DNA-onderzoek?

De Wiv 2017 bepaalt dat de inlichtingen- en veiligheidsdiensten een DNA-profiel mogen maken op basis van celmateriaal dat zij op een voorwerp hebben gevonden. Dit DNA-profiel (een soort cijfercode) kunnen zij vergelijken met andere DNA-profielen in hun eigen DNA-gegevensbestand. Ook kunnen de diensten hun profielen aanbieden aan andere databanken, zoals de DNA-databank voor strafzaken, met het verzoek om na te gaan of er een match is. Op basis van die vergelijking kunnen de diensten de identiteit van een persoon vaststellen of controleren.

De diensten moeten het DNA-profiel maken binnen 3 maanden nadat zij het celmateriaal hebben verkregen. Daarna moeten zij het celmateriaal binnen 3 maanden vernietigen. Het DNA-profiel zelf mogen zij maximaal 5 jaar bewaren. Alleen met toestemming van de minister mag deze termijn steeds met 5 jaar worden verlengd, met een maximum van 30 jaar. De bewaarde DNA-profielen kunnen de diensten gebruiken als vergelijkingsmateriaal voor nieuwe profielen. Ook kunnen ze deze delen met andere instanties, zoals buitenlandse veiligheidsdiensten. Daarvoor moeten ze wel apart toestemming vragen aan de minister.

# Verschillen tussen de Wiv 2002 en de Wiv 2017

### Waarom is gekozen voor een bewaartermijn van 5 tot maximaal 30 jaar?

Personen van wie de inlichtingen- en veiligheidsdiensten een DNA-profiel hebben, verdwijnen soms lang uit beeld. Denk aan Syriëgangers of internationaal werkende terroristen. Als er dan na een paar jaar weer een spoor van hen opduikt, bijvoorbeeld bij een aanslag, is het belangrijk om snel te kunnen controleren om welke persoon het gaat. De vergelijking van het gevonden spoor met een bestaand DNA-profiel is daarvoor het geëigende middel. Maar dat kan alleen als dat DNA-profiel lang genoeg wordt bewaard.

### Waarom deze verandering?

Met het DNA-onderzoek maken de diensten inbreuk op de privacy van de personen om wie het gaat. Daarom is het belangrijk dat er duidelijkheid bestaat over de regels voor dit type onderzoek. Dat gebeurt met de Wiv 2017. De regels gaan gepaard met de eis om toestemming te vragen aan de verantwoordelijke minister, voordat deze bevoegdheid wordt ingezet. Bovendien moet de minister deze toestemming voorleggen aan de Toetsingscommissie Inzet Bevoegdheden (TIB) (zie punt 2).

### Meer informatie over de regels voor DNA-onderzoek

- De regels voor het doen van DNA-onderzoek staan beschreven in artikel 43 van de Wiv 2017. De wettekst is te vinden op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html.**
- Dit artikel wordt toegelicht in de Memorie van Toelichting bij de Wiv 2017 (paragraaf 3.3.4.4.4). Deze staat op Overheid.nl: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html.**
- Artikel 43 staat in hoofdstuk 3 van de Wiv 2017. Een samenvatting van dit hoofdstuk vindt u op pagina 17 van dit document.

## 7. Duidelijkere regels voor samenwerking met buitenlandse diensten

De AIVD en de MIVD werken al jaren samen met buitenlandse inlichtingen- en veiligheidsdiensten. Daarvoor gaan ze samenwerkingsrelaties aan met de diensten die hiervoor in aanmerking komen. Welke diensten dat zijn, wordt bepaald door de hoofden van de AIVD en de MIVD, in samenspraak met de betrokken ministers. Daarbij hanteren ze een aantal criteria.

### Wat verandert er in de nieuwe wet?

De meeste criteria voor het aangaan van een samenwerkingsrelatie staan alleen in de toelichting op de huidige wet, maar niet in de wet zelf. In de Wiv 2017 zijn alle criteria expliciet opgenomen. Ook is in de nieuwe wet vastgelegd dat de diensten alleen een nieuwe samenwerkingsrelatie mogen aangaan, als ze daarvoor toestemming hebben van de verantwoordelijke minister.

### Welke criteria gelden er voor de samenwerking met buitenlandse diensten?

Om te bepalen of de AIVD en de MIVD een samenwerkingsrelatie aangaan met een collega-dienst in een ander land, maken zij (in een 'wegingsnotitie') een afweging aan de hand van de volgende criteria:

- de democratische inbedding van die dienst in dat land;
- de naleving van de mensenrechten door dat land;
- de professionaliteit en betrouwbaarheid van die dienst;
- de wettelijke bevoegdheden en mogelijkheden van die dienst, inclusief het toezicht daarop;
- de mate waarin die dienst gegevens beschermt.

Dit betekent niet dat samenwerking met een buitenlandse dienst wordt uitgesloten als deze niet aan alle criteria voldoet. Daarbij spelen ook andere overwegingen een rol, zoals de dreigingssituatie. Verder worden de criteria ook gebruikt om te bepalen hoe ver deze samenwerking reikt (artikel 88).

### Wat houdt een samenwerkingsrelatie in?

Als er een samenwerkingsrelatie met een collega-dienst is, betekent dit dat de AIVD en de MIVD gegevens met die dienst kunnen uitwisselen (artikel 89). Als het gaat om gegevens die de diensten nog niet onderzocht hebben op relevantie (ongeëvalueerde gegevens), gelden speciale voorwaarden (zie punt 4). Daarnaast kunnen de diensten elkaar op verzoek technische assistentie en andere ondersteuning bieden (artikel 90). Dit kan alleen met toestemming van de verantwoordelijke minister.

De CTIVD houdt toezicht op deze praktijk. De minister van BZK heeft in een brief aan de Tweede Kamer van 15 december 2017[2], mede namens de minister van Defensie, toegezegd dat de CTIVD op het moment dat de wet in werking treedt, beschikt over de belangrijkste wegingsnotities.

### Waarom deze veranderingen?

Het meeste wat hierboven staat, doen de diensten nu ook al. Het verschil is dat de criteria voor een samenwerkingsrelatie nu in de wet staan en dat er nu altijd toestemming nodig is om zo'n relatie aan te gaan. Dit is bedoeld om transparantie en zorgvuldigheid te bevorderen.

### Meer informatie over de samenwerking met buitenlandse diensten

- De regels voor de samenwerking met buitenlandse diensten staan beschreven in artikel 88 t/m 90 van de Wiv 2017. De wettekst is te vinden op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html.**
- De artikelen worden toegelicht in de Memorie van Toelichting bij de Wiv 2017 (paragraaf 6.3). Deze staat op Overheid.nl: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html.**

[2] Deze brief is te vinden op Rijksoverheid.nl: **http://bit.ly/2EReg83.**

# Verschillen tussen de Wiv 2002 en de Wiv 2017

- Artikel 88 t/m 99 staan in hoofdstuk 6 van de Wiv 2017. Een samenvatting van dit hoofdstuk vindt u op pagina 23 van dit document.

## 8. Waarborgen voor journalisten en advocaten

Bij het inzetten van hun bijzondere bevoegdheden kunnen de AIVD en de MIVD inbreuk maken op het recht van journalisten om hun bronnen geheim te houden. Bronnen zijn personen die aan journalisten informatie verstrekken. In de Wiv 2002 is er niets geregeld om de anonimiteit van deze bronnen te beschermen. Dat geldt ook voor de vertrouwelijke communicatie tussen advocaten en cliënten. Wel werd in 2016 na verschillende rechterlijke uitspraken een 'Tijdelijke regeling'[3] van kracht voor de inzet van bijzondere bevoegdheden tegenover advocaten en journalisten. Deze regeling is in de Wiv 2017 verwerkt en aangescherpt.

### Wat verandert er in de nieuwe wet?

De Wiv 2017 bevat een aangescherpte regeling voor zowel journalisten als advocaten. De eerste regeling richt zich op de gevallen waarin een dienst de communicatie van een journalist wil aftappen, zijn post wil openen of een andere bevoegdheid tegenover die journalist wil inzetten. Het kan zijn dat er daardoor informatie vrijkomt over een bron van die journalist. Als dat risico er is, bepaalt de Wiv 2017 dat de verantwoordelijke minister toestemming moet vragen aan de Rechtbank Den Haag. Alleen als de rechtbank die toestemming geeft, mag de dienst de bevoegdheid inzetten (artikel 30, lid 2).

Eenzelfde soort regeling is in de Wiv 2017 opgenomen voor de bescherming van de vertrouwelijke communicatie tussen advocaten en hun cliënten. Onder de Wiv 2002 hadden de AIVD en de MIVD – voordat de Tijdelijke regeling van kracht werd – alleen toestemming van de minister nodig om deze communicatie te kunnen aftappen. Onder de Wiv 2017 moet de minister hiervoor eerst toestemming vragen aan de Rechtbank Den Haag (artikel 30, lid 3). Voor beide regelingen geldt dat de toestemming wordt verleend voor maximaal 4 weken in plaats van de gebruikelijke 3 maanden (artikel 30, lid 2 en 3).

Daarnaast moet de minister de rechtbank om toestemming vragen als een dienst informatie aan het Openbaar Ministerie (OM) wil doorgeven die ze heeft verkregen door het onderscheppen van de vertrouwelijke communicatie tussen een advocaat en zijn cliënt. Als de rechtbank die toestemming niet verleent, mag de dienst de informatie niet aan het OM verstrekken (artikel 66, lid 3).

### Waarom deze veranderingen?

In de afgelopen jaren zijn er verschillende rechterlijke uitspraken geweest over de bronbescherming van journalisten en over de vertrouwelijke communicatie tussen advocaten en cliënten. Uit deze uitspraken bleek dat de veiligheidsdiensten door het aftappen van communicatie van journalisten en advocaten in strijd hebben gehandeld met artikel 8 en 10 van het Europees Verdrag tot bescherming van de rechten van de mens (EVRM). Dat concludeerde onder meer het Europese Hof voor de Rechten van de Mens.

Om dit te voorkomen is het nodig dat een onafhankelijke instantie toetst of de diensten de genoemde communicatie mogen onderscheppen of een andere bevoegdheid tegenover een advocaat of journalist mogen inzetten. Die onafhankelijke instantie is de Rechtbank Den Haag. De rechtbank mag alleen toestemming verlenen nadat ze het bijzondere belang van journalisten en advocaten goed heeft afgewogen. Ook moeten er concrete aanwijzingen zijn dat er een direct gevaar is voor de nationale veiligheid.

### Meer informatie over de regelingen voor journalisten en advocaten

- De regelingen voor journalisten en advocaten staan beschreven in artikel 30 en 66 van de Wiv 2017. De wettekst is te vinden op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html.**
- De artikelen worden toegelicht in de Memorie van Toelichting bij de Wiv 2017 (paragraaf 3.3.2.5.3). Deze staat op Overheid.nl: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html.**
- Artikel 30 en 66 staan in hoofdstuk 3 van de Wiv 2017. Een samenvatting van dit hoofdstuk vindt u op pagina 17 van dit document.

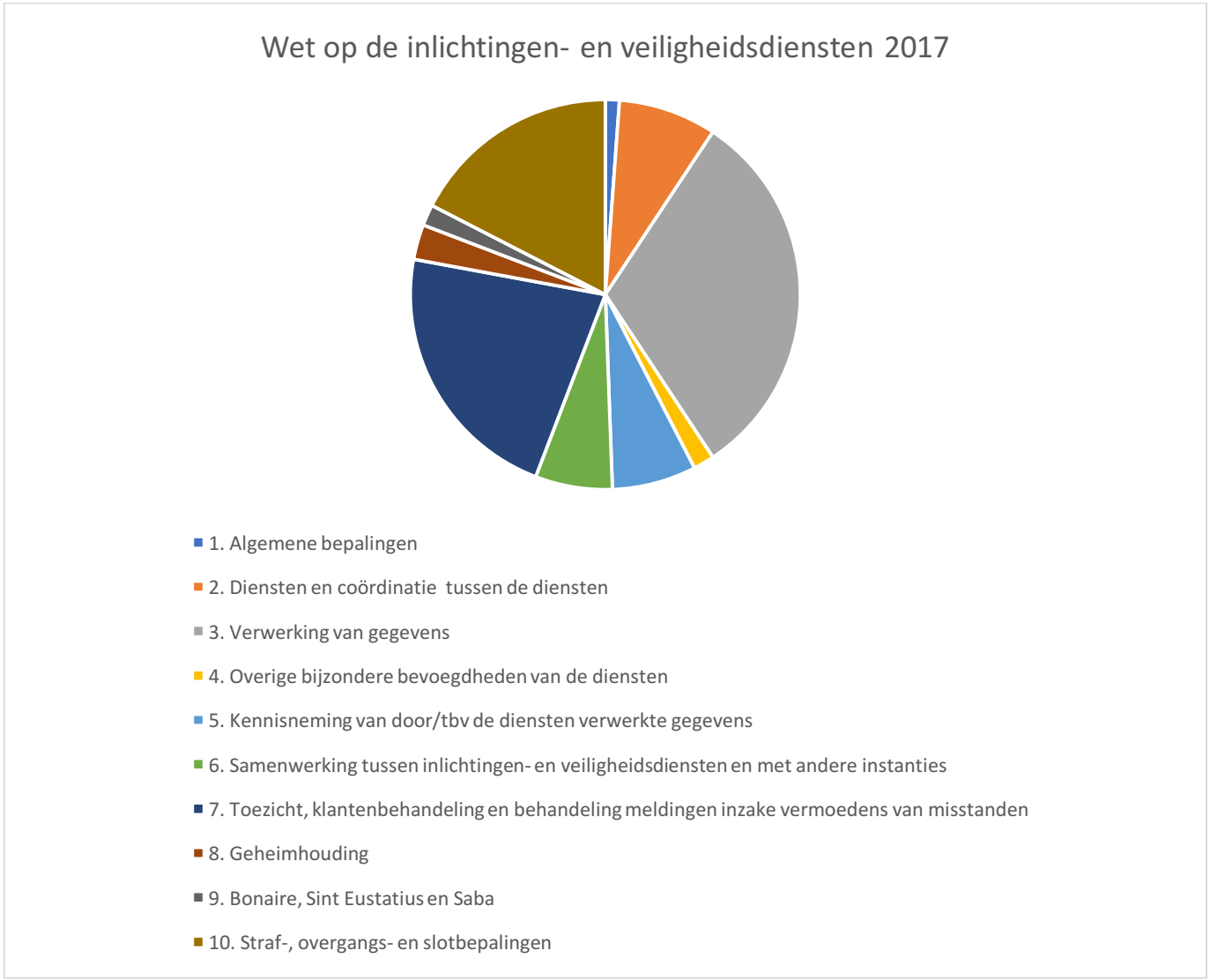
3 Deze regeling is te vinden op Overheid.nl: **http://bit.ly/2CiSc4d.**

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

De Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) bepaalt de taken en bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten. Ook staat erin welke voorwaarden er gelden voor de inzet van deze bevoegdheden, en hoe het toezicht daarop geregeld is. De wet geldt zowel voor de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) als voor de Militaire Inlichtingen- en Veiligheidsdienst.

## Wet op de inlichtingen- en veiligheidsdiensten 2017

De Wiv 2017 bestaat uit 10 hoofdstukken met in totaal 172 artikelen. Het langste hoofdstuk is hoofdstuk 3, over de verwerking van gegevens. Daarnaast worden het toezicht en de klachtenbehandeling uitgebreid beschreven in hoofdstuk 7.



REFERENDUM commissie

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

## Samenvatting per hoofdstuk

Op de volgende pagina's vindt u een samenvatting van alle hoofdstukken van de Wiv 2017:



### Wilt u liever de complete wettekst lezen?

Ga dan naar Overheid.nl:
**https://zoek.officielebekendmakingen.nl/stb-2017-317.html.**

### Over deze informatie

De Referendumcommissie informeert u in deze samenvatting over de inhoud van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017). Daarvoor baseert de commissie zich op de wet zelf. De teksten op deze pagina's zijn daar korte, vereenvoudigde weergaven van. De verwijzingen naar artikelen uit de wet zijn bedoeld om de breedte van de wet te illustreren; de teksten geven geen volledige weergave van deze artikelen.

Waar 'diensten' staat, worden bedoeld: de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Waar 'de betrokken minister' staat wordt de minister bedoeld die voor de betreffende dienst verantwoordelijk is. Voor de AIVD is dat de minister van Binnenlandse Zaken en Koninkrijksrelaties, voor de MIVD de minister van Defensie en voor de coördinatie van het werk van beide diensten de minister-president.

## Hoofdstuk 1: Algemene bepalingen

In hoofdstuk 1 van de Wiv 2017 wordt gedefinieerd wat er in deze wet onder bepaalde termen wordt verstaan. Een veelgebruikte term is 'gegevensverwerking' of 'verwerking van gegevens'. Hieronder verstaat de Wiv:

- het verzamelen, vastleggen, ordenen, bewaren, bijwerken en wijzigen van gegevens;
- het opvragen, raadplegen, gebruiken en ter beschikking stellen van gegevens;
- het verspreiden, samenbrengen en met elkaar in verband brengen van gegevens;
- het afschermen, uitwissen of vernietigen van gegevens;
- alle andere handelingen waarbij er iets met gegevens gebeurt.

Het gaat hier zowel om gegevens over personen als om andere gegevens (artikel 1).

### Meer informatie

Lees de officiële wettekst van artikel 1 t/m 2 van de Wiv 2017 op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e72.**

REFERENDUM commissie

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

## Hoofdstuk 2: De diensten en de coördinatie tussen de diensten

Hoofdstuk 2 van de Wiv 2017 gaat over de taken van de AIVD en de MIVD, en de coördinatie tussen deze diensten. Ook beschrijft dit hoofdstuk hoe bepaald wordt welke onderzoeken de diensten uitvoeren. Daarnaast bevat dit hoofdstuk enkele bepalingen over de verslaglegging van het werk van de diensten en over de beveiliging van de medewerkers.

### De taken van de Algemene Inlichtingen- en Veiligheidsdienst (artikel 8 en 9)

De taken van de AIVD zijn:

a. Het onderzoeken van organisaties en personen die door hun doelen of activiteiten aanleiding geven voor een ernstig vermoeden dat zij een gevaar vormen voor de democratische rechtsorde, voor de veiligheid of voor andere belangen van de staat.

b. Het doen van veiligheidsonderzoeken naar kandidaten voor vertrouwensfuncties.

c. Het bevorderen van maatregelen die zich onder meer richten op de beveiliging van onderdelen van de overheid en het bedrijfsleven die van vitaal belang zijn voor het maatschappelijk leven.

d. Het doen van onderzoek naar andere landen.

e. Het opstellen van dreigings- en risicoanalyses voor de beveiliging van specifieke personen, objecten en diensten.

f. Het onder voorwaarden verstrekken van gegevens die bij de dienst bekend zijn over een bepaalde persoon of instantie.

### De taken van de Militaire Inlichtingen- en Veiligheidsdienst (artikel 10 en 11)

De taken van de MIVD zijn:

a. Het doen van onderzoek naar:

- de strijdkrachten van andere landen met als doel om de eigen krijgsmacht beter te kunnen inrichten en benutten;
- factoren die van invloed (kunnen) zijn op de handhaving en bevordering van de internationale rechtsorde, voor zover de krijgsmacht daarbij betrokken is of kan worden.

b. Het doen van veiligheidsonderzoeken naar kandidaten voor vertrouwensfuncties bij Defensie.

c. Het onderzoeken van mogelijke maatregelen:

- om activiteiten te voorkomen die bedoeld zijn om de veiligheid of de paraatheid van de krijgsmacht te schaden;
- om een juist verloop te bevorderen van de mobilisatie van strijdkrachten;
- om een ongestoorde voorbereiding en inzet van de krijgsmacht te realiseren voor de handhaving of bevordering van de internationale rechtsorde.

d. Het bevorderen van maatregelen om de veiligheid en de paraatheid van de krijgsmacht te beschermen.

e. Het doen van onderzoek naar andere landen, gericht op onderwerpen met militaire relevantie.

f. Het opstellen van dreigingsanalyses voor de beveiliging van specifieke personen, objecten en diensten die van militair belang zijn.

g. Het onder voorwaarden verstrekken van gegevens die bij de dienst bekend zijn over een bepaalde persoon of instantie van militair belang.

### De coördinatie van het werk van de inlichtingen- en veiligheidsdiensten (artikel 3 t/m 7)

De inlichtingen- en veiligheidsdiensten vallen onder de verantwoordelijkheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties (voor de AIVD), de minister van Defensie (voor de MIVD) en de minister-president (voor de coördinatie van het werk van beide diensten). Deze ministers bepalen welke onderzoeken de diensten uitvoeren. Daarbij werken ze samen met een coördinator en met de Commissie Veiligheids- en Inlichtingendiensten Nederland (CVIN). Hierover bepaalt de wet onder meer het volgende:

- De coördinator heeft tot taak om het overleg tussen de betrokken ministers voor te bereiden en het werk van de diensten te coördineren. Ook is hij voorzitter van de CVIN en houdt hij de ministers op de hoogte van belangrijke zaken (artikel 4). De taak van de coördinator wordt in de praktijk vervuld door de secretaris-generaal van het ministerie van Algemene Zaken.
- De CVIN bestaat uit vertegenwoordigers van de ministeries van Algemene Zaken, Binnenlandse Zaken, Defensie, Buitenlandse Zaken, en Justitie en Veiligheid. De commissie heeft tot taak om de inlichtingenbehoefte van de ministers in kaart te brengen, gerelateerd aan de taken van de diensten. De commissie weegt en prioriteert deze behoefte en stelt op basis daarvan een voorstel op voor de zogenoemde 'geïntegreerde aanwijzing'. De geïntegreerde aanwijzing is een plan voor 4 jaar, waarin staat welke onderzoeken de diensten gaan doen en welke prioriteiten ze daarbij stellen (artikel 5).
- De minister-president en de ministers van Binnenlandse Zaken en Defensie stellen de geïntegreerde aanwijzing vast. Dit doen ze voor beide diensten gezamenlijk. Jaarlijks checken ze of de aanwijzing moet worden aangepast. Ze mogen de geïntegreerde aanwijzing alleen vaststellen of aanpassen als er overleg is geweest met de ministers van Buitenlandse Zaken en van Justitie en Veiligheid (artikel 6).

REFERENDUM commissie

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

### Verslaglegging over het werk van de diensten (artikel 12)

De betrokken ministers moeten jaarlijks aan de Eerste en Tweede Kamer verslag uitbrengen over het werk dat de inlichtingendiensten hebben verricht. Voor dit verslag geldt onder meer het volgende:

- Het verslag moet een volledig overzicht bevatten van de aandachtsgebieden in het afgelopen en het lopende jaar.
- Het verslag mag geen gegevens vermelden die zicht geven op ingezette middelen in concrete zaken, op geheime bronnen of op het actuele kennisniveau van de diensten. De minister kan deze gegevens eventueel wel vertrouwelijk aan de Eerste en/of Tweede Kamer doorgeven. In de praktijk betekent dit dat de minister de Commissie Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer op de hoogte stelt. In het publieke debat wordt deze commissie ook wel de 'commissie-Stiekem' genoemd.

### Bijzondere bepalingen over medewerkers van de AIVD of de MIVD (artikel 13 t/m 15)

Functionarissen die bij of voor de AIVD of de MIVD werken, doen soms risicovol werk. Hierover bepaalt de wet onder meer het volgende:

- De functionarissen zijn niet bevoegd om strafbare feiten op te sporen (artikel 13).
- De functionarissen mogen niet reizen naar of verblijven in risicolanden, behalve als dit voor hun functie nodig is (artikel 14).
- De hoofden van de diensten dragen zorg voor de beveiliging van hun ambtenaren. In dat kader kunnen zij toestaan dat een ambtenaar een andere identiteit of hoedanigheid gebruikt bij de uitoefening van zijn taken (artikel 15).

### Meer informatie

Lees de officiële wettekst van artikel 3 t/m 16 van de Wiv 2017 op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e178.**

## Hoofdstuk 3: De verwerking van gegevens

Hoofdstuk 3 van de Wiv 2017 gaat over de kernactiviteit van de AIVD en de MIVD, namelijk de verwerking van gegevens (zie ook hoofdstuk 1). De diensten verwerken onder meer gegevens over personen die een mogelijke dreiging vormen voor de staatsveiligheid. Ook verwerken ze gegevens over bijvoorbeeld cyberaanvallen of de situatie in een militair missiegebied. In dit hoofdstuk ligt de nadruk op het verzamelen van deze gegevens en de middelen die de diensten daarvoor mogen inzetten. Daarnaast gaat dit hoofdstuk in op het verstrekken van deze gegevens aan andere organisaties en buitenlandse veiligheidsdiensten.

### Algemene eisen waaraan de diensten moeten voldoen (artikel 17 t/m 24)

Als de inlichtingen- en veiligheidsdiensten (AIVD en MIVD) gegevens verzamelen en verwerken, moeten ze aan een aantal algemene eisen voldoen. Enkele eisen zijn:

- De diensten mogen alleen gegevens verzamelen en verwerken voor een bepaald doel. Ze moeten dit op een behoorlijke en zorgvuldige manier doen, in overeenstemming met de wet. En ze moeten bij de verzamelde gegevens aangeven hoe betrouwbaar die zijn en uit welke bron ze komen (artikel 18).
- De diensten mogen alleen gegevens van een persoon verwerken als die persoon behoort tot een categorie die is genoemd in artikel 19.[1] Daarbij gaat het bijvoorbeeld om personen van wie een ernstig vermoeden bestaat dat ze een gevaar vormen voor de democratische rechtsorde of de staatsveiligheid. Behoort een persoon niet tot een van de categorieën in artikel 19, dan mogen de diensten alleen gegevens over hem verwerken als die onlosmakelijk deel uitmaken van een gegevensbestand dat de diensten met toestemming hebben verworven (artikel 19).
- De diensten verwerken geen gegevens van personen op basis van hun godsdienst, ras, vakbondslidmaatschap, gezondheid of seksuele leven, tenzij dat voor de verwerking van andere gegevens onvermijdelijk is (artikel 19).
- De diensten moeten gegevens vernietigen zodra die geen betekenis (meer) hebben voor het doel waarvoor ze zijn verwerkt. Blijken gegevens niet te kloppen, dan moeten de diensten ze corrigeren (artikel 20).

### Middelen (bevoegdheden) die de diensten mogen inzetten (artikel 25 en 39 t/m 58)

Om gegevens te verzamelen, kunnen de AIVD en de MIVD verschillende middelen inzetten. Deze middelen worden bevoegdheden genoemd. Er zijn algemene en bijzondere bevoegdheden. Hieronder volgt een beschrijving van die bevoegdheden en van de voorwaarden die gelden voor de inzet ervan.

#### Algemene bevoegdheden (artikel 25)

De diensten zijn bevoegd om informatie te verzamelen:

- uit informatiebronnen die voor iedereen toegankelijk zijn, bijvoorbeeld websites en sociale media;
- uit informatiebronnen waar de diensten toegang toe hebben gekregen, zoals gegevensbestanden van de politie;
- door informatie te delen met buitenlandse inlichtingen- en veiligheidsdiensten waarmee een samenwerkingsrelatie bestaat en met andere instanties;
- door informatie te vragen aan bestuursorganen, ambtenaren en ieder ander die mogelijk relevante gegevens heeft. De betreffende instanties of personen zijn niet verplicht om de

[1] Zie hiervoor de wettekst op Overheid.nl: http://bit.ly/2qoNGQg.

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

gevraagde informatie te delen. Doen ze dit wel, dan kunnen ze de diensten desgewenst rechtstreeks online toegang geven tot gegevensbestanden (artikel 25 en 39). Overigens zijn communicatieaanbieders als KPN, Skype of Facebook wel verplicht om de gevraagde informatie aan de diensten te verstrekken (artikel 51 t/m 56).

Voor de inzet van deze bevoegdheden hoeven de diensten geen aparte toestemming te vragen, behalve als het gaat om de medewerking van communicatieaanbieders.

**Bijzondere bevoegdheden (artikel 40 t/m 58)**
Om informatie te verzamelen, kunnen de diensten ook bijzondere bevoegdheden inzetten. Daarvoor moeten ze eerst toestemming vragen; hieronder wordt per bevoegdheid aangegeven bij wie ze daarvoor moeten zijn. De toestemming wordt voor maximaal 3 maanden verleend (artikel 29). Is toestemming van de minister nodig, dan moet die toestemming getoetst worden door de Toetsingscommissie Inzet Bevoegdheden (TIB). Daarover leest u later meer.

De bijzondere bevoegdheden zijn:

1. **Observeren en volgen van personen en zaken.** Als het nodig is, mag dit met gebruik van technische hulpmiddelen, zoals camera's, drones of gps-apparatuur (artikel 40).

   toestemming vereist van de minister of namens hem het hoofd van de dienst

2. **Inzet van agenten.** Daarbij gaat het om personen die onder verantwoordelijkheid en instructie van de AIVD of de MIVD – eventueel met een andere identiteit – gericht gegevens verzamelen over personen en organisaties (artikel 41).

   toestemming vereist van de minister of namens hem het hoofd van de dienst

3. **Doorzoeken van woningen, koffers en andere besloten plaatsen en voorwerpen.** Als het nodig is, mag dit met gebruik van technische hulpmiddelen, zoals röntgenapparatuur (artikel 42).

   toestemming vereist van de minister of namens hem het hoofd van de dienst; bij woningen is toestemming vereist van de minister en de TIB

4. **Doen van DNA-onderzoek.** Dit houdt in dat de diensten een DNA-profiel kunnen maken op basis van celmateriaal dat zij op een voorwerp hebben aangetroffen. Dit mogen zij alleen doen om de identiteit van een persoon vast te stellen of te controleren. Zij moeten dit profiel maken binnen 3 maanden nadat zij het celmateriaal hebben verkregen. Daarna moeten de diensten het celmateriaal binnen 3 maanden vernietigen. Het DNA-profiel zelf (een soort cijfercode) mogen zij maximaal 5 jaar bewaren. Alleen met toestemming van de minister mag deze termijn steeds met 5 jaar worden verlengd (artikel 43).

   toestemming vereist van de minister en de TIB

5. **Openen van brieven en andere geadresseerde zendingen,** zonder medeweten van de afzender of de geadresseerde (artikel 44).

   toestemming vereist van de Rechtbank Den Haag

6. **Hacken ofwel het gericht binnendringen in computers, smartphones, servers** en andere apparaten en netwerken ('geautomatiseerde werken'). De diensten mogen hiervoor elke beveiliging doorbreken, valse identiteiten gebruiken en malware installeren. Ook mogen ze in een computer technische voorzieningen installeren om bijvoorbeeld een ruimte te observeren, of om gesprekken op te nemen. Lukt het niet om toegang tot een apparaat te krijgen, dan kunnen de diensten dit proberen via een apparaat of systeem van een andere persoon of organisatie, bijvoorbeeld een provider (artikel 45).

   toestemming vereist van de minister en de TIB

7. **Gericht onderscheppen van telecommunicatie,** zoals telefoongesprekken, e-mail- en appverkeer. 'Gericht' betekent dat het moet gaan om communicatie van en naar specifieke personen, organisaties of nummers, zoals telefoonnummers en user-ID's. Het maakt niet uit of deze communicatie door de lucht of via kabels verloopt. Is de communicatie versleuteld, dan mogen de diensten deze ontsleutelen (artikel 47).

   toestemming vereist van de minister en de TIB

8. **Onderzoeksopdrachtgericht onderscheppen van telecommunicatie,** zoals telefoongesprekken, e-mail- en appverkeer. 'Onderzoeksopdrachtgericht' houdt in dat de inlichtingen- en veiligheidsdiensten gedurende 1 jaar een brede stroom van telecommunicatie mogen onderscheppen, waarvoor vooraf een duidelijke onderzoeksopdracht is geformuleerd. De te onderscheppen communicatie hoeft niet gekoppeld te zijn aan een bepaalde persoon of organisatie. Ook maakt het niet uit of deze communicatie door de lucht of via kabels verloopt. Is de communicatie versleuteld, dan mogen de diensten deze ontsleutelen (artikel 48 t/m 50).

   toestemming vereist van de minister en de TIB

REFERENDUM commissie

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

9. **Vragen van medewerking aan telecomaanbieders.** Het gaat hier om medewerking die nodig is om de juiste telecommunicatie te kunnen onderscheppen. De aanbieders zijn verplicht om deze medewerking te verlenen (artikel 51 t/m 53).

   toestemming vereist van de minister en de TIB

10. **Opvragen van opgeslagen telecommunicatie van een bepaalde persoon in een bepaalde periode.** Het gaat hier bijvoorbeeld om e-mails, WhatsApp- of voicemailberichten die door telecomaanbieders of dataopslagdiensten, bijvoorbeeld ergens in the cloud, zijn opgeslagen. De aanbieders en opslagdiensten zijn verplicht om de gevraagde communicatie te leveren (artikel 54).

    toestemming vereist van de minister en de TIB

11. **Opvragen van gegevens over het communicatieverkeer van een persoon** voor, op of na het tijdstip van het verzoek. Het gaat hier niet om gegevens over de inhoud van de communicatie, maar om metadata, bijvoorbeeld de tijdstippen waarop die persoon gebeld of geappt heeft en de locatie waar hij zich toen bevond. De aanbieders zijn verplicht om deze gegevens direct te verstrekken (artikel 55).

    toestemming vereist van de minister en de TIB

12. **Opvragen van de contactgegevens van een gebruiker van een communicatiedienst.** De inlichtingendiensten kunnen hierom vragen als ze bijvoorbeeld de communicatie van een persoon willen aftappen, maar niet weten wat de naam en het telefoonnummer van die persoon zijn. Als de aanbieders deze gegevens niet hebben, moeten zij deze achterhalen (artikel 56).

    toestemming vereist van het hoofd van de dienst of diens vervanger

13. **Vragen van medewerking om telecommunicatie te ontsleutelen.** Het gaat hier om de medewerking van experts bij het ontsleutelen van versleutelde telecommunicatie die de inlichtingendiensten (gericht of onderzoeksopdrachtgericht) hebben onderschept. De experts zijn verplicht om deze medewerking te verlenen (artikel 57).

    toestemming vereist van de minister en de TIB

14. **Plaatsen van apparatuur in ruimtes zoals woningen,** zonder toestemming van de bewoner, huurder of eigenaar van de ruimte. De inlichtingen- en veiligheidsdiensten mogen deze apparatuur heimelijk plaatsen om bijvoorbeeld af te kunnen luisteren, een computer te hacken of een persoon te observeren (artikel 58).

    toestemming vereist van de minister of namens hem het hoofd van de dienst

### Algemene voorwaarden voor het gebruik van deze bevoegdheden (artikel 26 t/m 31)

De AIVD en de MIVD mogen de bovengenoemde bevoegdheden alleen inzetten onder bepaalde voorwaarden. Voor zowel de algemene als de bijzondere bevoegdheden gelden de volgende voorwaarden (ook wel het 'afwegingskader' genoemd):

- De diensten moeten altijd kiezen voor de bevoegdheid die de betrokken personen zo min mogelijk nadeel oplevert. Daarbij moeten ze een afweging maken tussen de omstandigheden (bijvoorbeeld de ernst van een dreiging), de beschikbare middelen en de gevolgen daarvan. Dit wordt ook wel het **subsidiariteitsbeginsel** genoemd (artikel 26).
- De bevoegdheid die de dienst inzet moet in verhouding staan tot het doel dat ermee wordt beoogd. Is het nadeel van de inzet van die bevoegdheid voor een betrokken persoon onevenredig groot ten opzichte van het doel? Dan mag de dienst deze bevoegdheid niet inzetten. Dit wordt het **proportionaliteitsbeginsel** genoemd (artikel 26).
- De diensten moeten onmiddellijk stoppen met de inzet van de bevoegdheid zodra het beoogde doel is bereikt of zodra dit doel bereikt kan worden met een minder ingrijpend middel (artikel 26).

Voor de bijzondere bevoegdheden gelden daarnaast onder meer de volgende voorwaarden:

- De inlichtingen- en veiligheidsdiensten mogen hun bijzondere bevoegdheden alleen uitoefenen als dat nodig is voor de goede uitvoering van hun taken. Dit is het **noodzakelijkheidsvereiste**. Het gaat hierbij om de taken a en d uit artikel 8 en de taken a, c en e uit artikel 10 van de wet (artikel 28). Zie voor een beschrijving van deze taken de samenvatting van hoofdstuk 2 (pagina 16 van dit document).
- De diensten moeten de gegevens die zij verzameld hebben door de inzet van een bijzondere bevoegdheid zo spoedig mogelijk – maar uiterlijk binnen 1 jaar – op relevantie onderzoeken. Ze mogen deze gegevens daarna alleen bewaren als ze belangrijk zijn voor het onderzoek waarvoor ze verzameld zijn, of voor een ander lopend onderzoek. Zijn ze niet relevant, dan moeten ze onmiddellijk vernietigd worden (artikel 27). Zijn ze na 1 jaar nog niet onderzocht, dan moeten ze op dat moment vernietigd worden. Een uitzondering vormen gegevens die verkregen zijn door 'onderzoeksopdrachtgerichte interceptie'

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

(zie punt 8). Hiervoor geldt een termijn van 3 jaar in plaats van 1 jaar (artikel 48).

- Als de inlichtingen- en veiligheidsdiensten een bijzondere bevoegdheid willen inzetten jegens een journalist of advocaat, moeten ze daarvoor toestemming vragen aan de Rechtbank Den Haag (artikel 30).

### Extra controle door de Toetsingscommissie Inzet Bevoegdheden, TIB (artikel 32 t/m 37)

Als de minister toestemming heeft verleend voor de inzet van een bijzondere bevoegdheid, moet hij deze toestemming voorleggen aan de Toetsingscommissie Inzet Bevoegdheden (TIB). De TIB toetst dan of de toestemming rechtmatig is verleend. Zo niet, dan vervalt de toestemming. De TIB wordt alleen ingezet voor de bevoegdheden die de meeste inbreuk maken op de privacy van burgers. Voorbeelden zijn het doorzoeken van woningen, het verrichten van DNA-onderzoek en het onderscheppen van telecommunicatie (artikel 32).

### Betrokken personen informeren over de inzet van enkele bijzondere bevoegdheden (artikel 59)

De betrokken ministers hebben een 'notificatieplicht' als de inlichtingen- en veiligheidsdiensten zonder medeweten van de betreffende persoon:

- brieven of pakjes hebben geopend die aan hem waren gericht (zie punt 5);
- gericht telecommunicatie van deze persoon hebben afgetapt (zie punt 7);
- de woning van deze persoon zijn binnengegaan (zie punt 14).

Deze notificatieplicht geldt alleen voor personen en niet voor organisaties. De plicht houdt in dat de betrokken ministers na 5 jaar moeten onderzoeken of de betreffende persoon geïnformeerd kan worden over het feit dat de diensten deze middelen bij hem hebben ingezet. Deze 5 jaar gaan in op het moment dat de diensten gestopt zijn met de inzet van de middelen ten aanzien van die persoon.

Als uit dit onderzoek blijkt dat de persoon geïnformeerd kan worden, moet de minister dat zo spoedig mogelijk doen. Blijkt dat informeren niet mogelijk is, dan moet hij dit melden aan de commissie van toezicht (CTIVD). Daarna moet de minister dit onderzoek elk jaar herhalen. Informeren hoeft niet als daardoor zwaarwegende belangen worden geschaad van de inlichtingen- en veiligheidsdiensten, van collega-diensten of van andere landen.

### De verwerking van gegevens door geautomatiseerde data-analyses (artikel 60)

Voor het onderzoeken van grote gegevensbestanden (*big data*) kunnen de inlichtingen- en veiligheidsdiensten gebruikmaken van geautomatiseerde data-analyses. Ze mogen deze analyses toepassen op eigen en publieke gegevensbestanden en op gegevensbestanden die anderen aan hen hebben verstrekt. Daar is geen aparte toestemming van de minister voor nodig, behalve als deze analyses gericht zijn op de identiteit van een specifieke persoon.

De analyse kan verschillende vormen hebben, waaronder het doorzoeken van gegevens aan de hand van profielen. Dit houdt in dat bijvoorbeeld alle personen eruit worden gefilterd die voldoen aan een aantal kenmerken. De diensten mogen geen maatregelen tegen personen (laten) treffen enkel op basis van een geautomatiseerde data-analyse. Daarvoor is altijd een menselijke afweging nodig. De CTIVD ziet daarop toe.

### Het verstrekken van gegevens aan eigen medewerkers en aan andere instanties (artikel 61 t/m 63)

De AIVD en de MIVD kunnen gegevens die zij verzameld en verwerkt hebben, verstrekken aan eigen medewerkers, voor zover deze die gegevens nodig hebben om hun taak goed te kunnen uitoefenen. Dit wordt 'interne verstrekking' genoemd (artikel 61). Daarnaast kunnen ze onder voorwaarden mededelingen over verwerkte gegevens doen aan ministers, bestuursorganen en andere instanties waarvoor deze gegevens van belang zijn. Daaronder vallen ook het Openbaar Ministerie en internationale organisaties als de EU, de NAVO en de Verenigde Naties (artikel 62).

### Het verstrekken van gegevens aan buitenlandse collega-diensten (artikel 62 t/m 70 en 89)

Als de AIVD of de MIVD gegevens wil verstrekken aan buitenlandse inlichtingen- en veiligheidsdiensten, gelden de volgende regels:

- De diensten mogen gegevens verstrekken aan inlichtingen- en veiligheidsdiensten ('collega-diensten') van landen waarmee zij een samenwerkingsrelatie hebben (artikel 62 en 89). Zo'n samenwerkingsrelatie mogen zij alleen aangaan onder strikte criteria en met toestemming van de betrokken minister (artikel 88). U leest hier meer over in de samenvatting van hoofdstuk 6 (zie pagina 23).
- De diensten mogen alleen gegevens verstrekken aan de genoemde buitenlandse diensten, als dat nodig is om de eigen taken goed te kunnen uitvoeren of om de belangen van collega-diensten te behartigen (artikel 62 en 89). Bij dat laatste geldt dat de belangen van de collega-diensten niet onverenigbaar mogen zijn met de eigen belangen.
- Wil een dienst gegevens verstrekken aan een inlichtingen- en veiligheidsdienst van een land waarmee zij geen samenwerkingsrelatie heeft? Dan mag dat alleen als daar een dringende reden voor is en de betrokken minister er toestemming voor heeft verleend (artikel 64).
- Als de diensten gegevens aan buitenlandse diensten willen verstrekken die nog niet op relevantie zijn onderzocht ('ongeëvalueerde gegevens'), mag dit alleen met toestemming van

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

de minister. Gaat het om gegevens die zijn verzameld door het breed onderscheppen van telecommunicatie, dan moeten ze daarnaast meteen de commissie van toezicht (CTIVD) informeren (artikel 64 en 89).

- Bij het verstrekken van gegevens aan buitenlandse inlichtingen- en veiligheidsdiensten kan de voorwaarde worden gesteld dat deze diensten de gegevens niet aan anderen doorgeven. De betrokken minister of namens deze het hoofd van de dienst kan hier incidenteel een uitzondering op maken (artikel 65).

### Het melden van strafbare feiten (artikel 66)

Als de inlichtingen- en veiligheidsdiensten bij de verwerking van verzamelde gegevens stuiten op strafbare feiten, kunnen ze die melden aan het Openbaar Ministerie (OM). Ze hoeven die melding niet te doen als de gevolgen daarvan – opsporing en vervolging door het OM – een eigen onderzoek van de dienst belemmeren. Daarbij moeten ze rekening houden met de ernst van het delict: hoe ernstiger dit is, hoe kleiner de ruimte wordt om dit delict niet bij het OM te melden.

Zijn de diensten op een strafbaar feit gestuit door het onderscheppen van vertrouwelijke communicatie tussen een advocaat en zijn cliënt? Dan mogen ze deze informatie alleen aan het OM doorgeven als ze daarvoor toestemming hebben verkregen van de Rechtbank Den Haag.

### Bijzondere bepalingen over het verstrekken van persoonsgegevens (artikel 68 en 69)

Als de inlichtingen- en veiligheidsdiensten persoonsgegevens aan andere instanties doorgeven, moeten ze dat altijd schriftelijk doen. Zij mogen geen persoonsgegevens verstrekken waarvan niet zeker is dat ze correct zijn of die meer dan 10 jaar geleden zijn verwerkt. Bij uitzondering kunnen de diensten dergelijke gegevens wel verstrekken aan:

- buitenlandse inlichtingen- en veiligheidsdiensten waarmee de diensten een samenwerkingsrelatie hebben;
- internationale organisaties als de NAVO, de EU of de Verenigde Naties;
- instanties die belast zijn met de opsporing en vervolging van strafbare feiten;
- andere instanties die door de minister zijn aangewezen.

### Meer informatie

Lees de officiële wettekst van artikel 17 t/m 70 van de Wiv 2017 op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e706.**

## Hoofdstuk 4: Overige bijzondere bevoegdheden van de diensten

Hoofdstuk 4 van de Wiv 2017 is een kort hoofdstuk dat gaat over 2 bijzondere bevoegdheden van de AIVD en de MIVD:

- de mogelijkheid om een aparte organisatie (rechtspersoon) op te richten om bepaalde activiteiten voor te bereiden of te ondersteunen;
- de mogelijkheid om maatregelen te treffen of te bevorderen om de nationale veiligheid, de democratische rechtsorde en andere belangen van de staat te beschermen.

### De oprichting en inzet van een aparte organisatie (artikel 72)

Voor sommige activiteiten van de AIVD en de MIVD is het belangrijk dat de identiteit van de medewerkers die deze activiteiten uitvoeren, onherkenbaar is. Dat geldt ook voor de voertuigen en communicatiemiddelen die zij gebruiken. In die gevallen kan het nuttig zijn om een aparte organisatie op te richten, waarin die medewerkers en zaken worden ondergebracht. Artikel 72 van de wet biedt die mogelijkheid. De diensten kunnen deze organisatie zowel inzetten voor de voorbereiding als de ondersteuning van activiteiten. Voordat ze dat doen, moeten ze eerst toestemming vragen aan de verantwoordelijke minister of namens hem het hoofd van de dienst.

### Het treffen of bevorderen van maatregelen (artikel 73)

Het is de taak van de AIVD en de MIVD om de staatsveiligheid, de democratische rechtsorde, de veiligheid van de krijgsmacht en andere belangen van de staat te beschermen. Daartoe mogen de diensten bepaalde maatregelen treffen of bevorderen, zoals het verstoren van communicatie via internet. Zo nodig mogen zij daarvoor overtredingen begaan zonder dat zij daarvoor gestraft worden.

Voor de inzet van de maatregelen gelden enkele voorwaarden. Zo moeten de diensten altijd kiezen voor de maatregel die de betrokken personen zo min mogelijk nadeel oplevert. Ook moet de maatregel in verhouding staan tot het doel dat ermee wordt beoogd. Bovendien moeten de diensten onmiddellijk met de maatregel stoppen zodra het beoogde doel is bereikt of zodra dit doel bereikt kan worden met een minder ingrijpende maatregel. En tot slot is toestemming vereist van de verantwoordelijke minister of namens hem het hoofd van de dienst.

### Meer informatie

Lees de officiële wettekst van artikel 71 t/m 73 van de Wiv 2017 op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e2867.**

REFERENDUM commissie

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

## Hoofdstuk 5: Kennisneming van door of ten behoeve van de diensten verwerkte gegevens

Bij de onderzoeken die zij doen, verwerken de AIVD en de MIVD veel gegevens. Welke gegevens zij precies verwerken, is in principe geheim. Tot op zekere hoogte mogen burgers deze gegevens opvragen of inzien. Hoofdstuk 5 van de Wiv 2017 bepaalt wie dat mogen doen en welke voorwaarden daarvoor gelden.

### Recht om verwerkte persoonsgegevens in te zien (artikel 76 t/m 79 en 59)

Elke burger mag opvragen welke persoonsgegevens de AIVD of de MIVD over hem heeft verwerkt. Hij moet daarvoor een schriftelijke aanvraag indienen bij de verantwoordelijke minister. Enkele bepalingen hierover zijn:

- Als iemand een aanvraag heeft ingediend, moet de verantwoordelijke minister binnen 3 maanden aan de aanvrager laten weten of de dienst gegevens over hem heeft verwerkt en zo ja, welke gegevens. Als de aanvraag wordt ingewilligd, mag de aanvrager de gegevens binnen 4 weken inzien (artikel 76).
- Of de aanvraag wordt ingewilligd, hangt onder meer af van de bevoegdheid die de dienst tegenover de aanvrager heeft ingezet. Voor sommige bevoegdheden geldt dat de minister 5 jaar na beëindiging hiervan moet onderzoeken of de verzamelde gegevens aan de betreffende persoon kunnen worden doorgegeven. Is dit het geval, dan wordt de aanvraag ingewilligd, tenzij er sprake is van een van de uitzonderingen die aan het einde van deze pagina worden genoemd (artikel 59).
- In principe mogen burgers alleen persoonsgegevens over zichzelf inzien. Een uitzondering geldt voor nabestaanden: deze mogen ook een aanvraag indienen om de gegevens in te zien over een overleden echtgenoot, geregistreerd partner, ouder of kind (artikel 79).
- Als de aanvrager meent dat de gegevens onjuistheden bevatten, kan hij bij die gegevens een verklaring voegen waarin hij zijn zienswijze geeft (artikel 77).
- Een (oud-)medewerker van een inlichtingendienst mag gegevens over zichzelf uit de personeels- en salarisadministratie opvragen. Het hoofd van de dienst geeft de persoon binnen 4 weken de gelegenheid om die gegevens in te zien. De persoon mag geen gegevens inzien die zicht geven op bronnen die geheim moeten blijven (artikel 78).

### Recht om andere verwerkte gegevens in te zien (artikel 80)

Burgers mogen ook een aanvraag indienen om andere gegevens in te zien die de diensten hebben verwerkt. Het gaat dan om gegevens over onderwerpen die betrekking hebben op het beleid van de diensten ('bestuurlijke aangelegenheden'). De procedure en de termijnen voor deze aanvraag zijn gelijk aan die voor een aanvraag om persoonsgegevens in te zien.

### Wijze waarop de aanvrager de gegevens kan inzien (artikel 81)

Als de minister heeft bepaald dat een burger de gevraagde gegevens mag inzien, kan dat op verschillende manieren gebeuren. Zo kan de aanvrager een kopie of een samenvatting krijgen van het document waar de gegevens in staan, of hij kan dit document zelf inzien. De keuze van de procedure hangt af van de belangen van de dienst en de voorkeur van de aanvrager.

### Redenen om een aanvraag af te wijzen (artikel 82 t/m 85)

De minister kan een aanvraag om gegevens in te zien om verschillende redenen afwijzen. Enkele redenen zijn:

- De gegevens zijn minder dan 5 jaar geleden gebruikt in een onderzoek van een van de diensten (artikel 82).
- Door het verstrekken van de gegevens kan de nationale veiligheid in gevaar komen (artikel 84).
- Het belang van het verstrekken van de gegevens weegt niet op tegen andere belangen, zoals de internationale betrekkingen van Nederland, de opsporing van strafbare feiten en de bescherming van de privacy van medeburgers (artikel 84).

Wijst de minister een aanvraag af, dan moet hij de commissie van toezicht (CTIVD) daarvan op de hoogte brengen (artikel 84).

### Meer informatie

Lees de officiële wettekst van artikel 74 t/m 85 van de Wiv 2017 op Overheid.nl:
**https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e2943.**

REFERENDUM commissie

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

## Hoofdstuk 6: Samenwerking tussen inlichtingen- en veiligheidsdiensten en met andere instanties

Hoofdstuk 6 van de Wiv 2017 gaat over de samenwerking tussen de AIVD en de MIVD onderling, en over de samenwerking met collega-diensten in andere landen. Ook gaat het hoofdstuk over de samenwerking met andere instanties in Nederland, zoals de Koninklijke Marechaussee en de Nationale Politie.

### Samenwerking tussen de AIVD en de MIVD (artikel 86 en 87)

De AIVD en de MIVD werken zo veel mogelijk samen.
Deze samenwerking houdt onder meer het volgende in:

- De diensten mogen gegevens met elkaar uitwisselen en elkaar technische en andere ondersteuning bieden (artikel 86).
- De diensten kunnen elkaar ondersteuning bieden bij de inzet van een bijzondere bevoegdheid, zoals het onderscheppen van telecommunicatie. Dit mag alleen als de betrokken minister daarvoor toestemming heeft verleend (artikel 86).
- De diensten kunnen samenwerkingsverbanden aangaan, zoals de Joint Sigint Cyber Unit (JSCU). Deze eenheid is actief bij het verwerven en analyseren van gegevens uit telecommunicatie en ander dataverkeer (artikel 86).
- De diensten moeten elkaar tijdig informeren over voorgenomen operationele activiteiten die invloed kunnen hebben op het werk van de andere dienst. Daarbij gaat het zowel om activiteiten in Nederland als in andere landen (artikel 87).

### Samenwerking met veiligheidsdiensten van andere landen (artikel 88 t/m 90)

De AIVD en de MIVD mogen samenwerkingsrelaties aangaan met collega-diensten in andere landen. Hiervoor geldt onder meer het volgende:

- Om te bepalen of de Nederlandse inlichtingen- en veiligheidsdiensten een samenwerkingsrelatie mogen aangaan met een collega-dienst uit een ander land, moeten zij een afweging maken aan de hand van de volgende criteria:
  a. de democratische inbedding van die dienst in dat land;
  b. de naleving van de mensenrechten door het land;
  c. de professionaliteit en betrouwbaarheid van die dienst;
  d. de wettelijke bevoegdheden en mogelijkheden van die dienst, inclusief het toezicht daarop;
  e. de mate waarin die dienst gegevens beschermt (artikel 88).
- De aard en intensiteit van de samenwerkingsrelatie hangen af van de mate waarin aan de genoemde criteria wordt voldaan en van het belang dat met de samenwerking is gemoeid.
- De diensten mogen alleen een samenwerkingsrelatie met een collega-dienst aangaan als ze daarvoor toestemming hebben van de verantwoordelijke minister of namens hem het hoofd van de dienst (artikel 88). Is er sprake van een samenwerkingsrelatie, dan mogen de AIVD en MIVD gegevens verstrekken aan de collega-dienst in het andere land (artikel 89).
- Willen de diensten gegevens delen die nog niet onderzocht zijn op relevantie, dan is aparte toestemming van de minister vereist (artikel 89). Als deze gegevens verkregen zijn door het breed onderscheppen van telecommunicatie, dan moet meteen de commissie van toezicht (CTIVD) worden geïnformeerd.
- De inlichtingendiensten mogen op verzoek van een samenwerkende collega-dienst technische of andere ondersteuning bieden als ze daarvoor toestemming hebben van de minister. Ook mogen ze zelf aan een collega-dienst om ondersteuning vragen. Gaat het om activiteiten waarvoor de inzet van een bijzondere bevoegdheid nodig is, bijvoorbeeld het aftappen van een telefoon in het buitenland? Dan mogen ze dit verzoek alleen doen als ze daarvoor toestemming hebben gekregen van de minister (artikel 89 en 90).

### Samenwerking met andere instanties in Nederland (artikel 91 t/m 95 en 66)

De AIVD en de MIVD werken samen met verschillende Nederlandse overheidsinstanties. Die samenwerking betreft onder meer het volgende:

- De Nationale Politie, de Koninklijke Marechaussee, de Belastingdienst, de Immigratie- en Naturalisatiedienst (IND) en de Inspectie SZW verrichten werkzaamheden voor de AIVD en de MIVD. De ministers bepalen welke ambtenaren daarvoor worden ingezet (artikel 91).
- Leden van het Openbaar Ministerie (OM) geven het meteen aan de inlichtingendiensten door als zij op gegevens stuiten die voor de diensten van belang kunnen zijn (artikel 92). Datzelfde geldt voor ambtenaren van de Nationale Politie, de Koninklijke Marechaussee en de Belastingdienst (artikel 94). Andersom hoeven de inlichtingendiensten het niet altijd aan het OM door te geven als ze bij hun onderzoek stuiten op strafbare feiten. Als het gaat om gegevens uit contacten tussen een advocaat en zijn cliënt, mag dat alleen met toestemming van de Rechtbank Den Haag (artikel 66).
- De AIVD en de MIVD kunnen technische en andere ondersteuning verlenen aan de Nationale Politie, het OM en andere opsporingsinstanties. Ook kunnen ze zelf technische of andere ondersteuning vragen aan de Nationale Politie en de Koninklijke Marechaussee (artikel 95).
- De diensten kunnen ook een samenwerkingsverband aangaan met andere Nederlandse instanties (artikel 96). Een voorbeeld daarvan is de Contraterrorisme Infobox (CT Infobox). Hierin werken de diensten samen met onder meer de IND en de Inspectie SZW aan de bestrijding van terrorisme en radicalisme.

REFERENDUM commissie

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

### Meer informatie

Lees de officiële wettekst van artikel 86 t/m 96 van de Wiv 2017 op Overheid.nl:
**https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e3304.**

## Hoofdstuk 7: Toezicht, klachtbehandeling en de behandeling van meldingen inzake vermoedens van misstanden

Hoofdstuk 7 van de Wiv 2017 gaat over het externe toezicht op de rechtmatigheid van de uitvoering van deze wet. Dat is sinds 2002 belegd bij de onafhankelijke Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Zij houdt toezicht *tijdens* de uitvoering en *achteraf*. Voor een toets *vooraf* wordt met ingang van de Wiv 2017 de onafhankelijke Toetsingscommissie Inzet Bevoegdheden (TIB) ingesteld (zie pagina 7). De CTIVD mag ook de rechtmatigheid beoordelen van de besluiten van de TIB.

Dit hoofdstuk gaat in op de samenstelling, taken en bevoegdheden van de CTIVD en specifiek op de behandeling van klachten en meldingen van mogelijke misstanden.

### Samenstelling van de CTIVD (artikel 97 t/m 105)

Over de samenstelling van de CTIVD bepaalt de wet onder meer het volgende:

- De CTIVD bestaat uit 2 gescheiden afdelingen: een afdeling Toezicht en een afdeling Klachtbehandeling. De eerste afdeling houdt toezicht op de rechtmatige uitvoering van de wettelijke taken van de AIVD en de MIVD. De tweede afdeling onderzoekt en beoordeelt klachten van burgers en meldingen van mogelijke misstanden (artikel 97).
- De CTIVD bestaat uit 4 leden inclusief de voorzitter. 1 lid is voorzitter van de afdeling Klachtbehandeling. De andere 3 vormen de afdeling Toezicht. Bij de afdeling Klachtbehandeling werken daarnaast nog minimaal 2 andere leden. Alle leden worden voor 6 jaar benoemd en kunnen 1 keer worden herbenoemd (artikel 98).
- Als er vacatures zijn bij de CTIVD draagt de Tweede Kamer ten minste 3 kandidaten voor per vacature. De regering maakt daaruit vervolgens een keuze (artikel 99).
- De leden van de afdelingen mogen geen lid zijn van de TIB (artikel 99).

### Verplichting om informatie te geven aan de CTIVD (artikel 107 t/m 111)

Om hun werk goed te kunnen doen, hebben de afdelingen van de CTIVD de juiste informatie nodig. Daarom bepaalt de wet het volgende:

- De inlichtingendiensten en hun verantwoordelijke ministers moeten aan de CTIVD alle inlichtingen verstrekken die zij nodig hebben voor de uitoefening van hun taken. Ook moeten zij de CTIVD rechtstreeks toegang geven tot verwerkte gegevens (artikel 107).
- De CTIVD kan mensen oproepen om inlichtingen te verschaffen als getuige of deskundige. Daarbij gaat het bijvoorbeeld om de hoofden of medewerkers van de inlichtingendiensten. Deze getuigen en deskundigen zijn verplicht om hun medewerking te verlenen (artikel 108).

### Taken van de afdeling Toezicht (artikel 112 en 113)

De afdeling Toezicht verricht onderzoeken naar de manier waarop de AIVD en de MIVD hun wettelijke taken uitvoeren. Daarvoor geldt onder meer het volgende:

- De afdeling bepaalt zelf welke onderzoeken zij uitvoert. Zij kan deze onderzoeken op eigen initiatief uitvoeren of op verzoek van de Eerste en/of Tweede Kamer (artikel 112).
- Na afronding van een onderzoek maakt de afdeling een rapport van de bevindingen. De minister reageert hierop. Daarna stelt de afdeling het rapport vast en stuurt de minister het met zijn reactie naar de Kamers. Het rapport is openbaar, met uitzondering van de gegevens die zicht geven op geheime bronnen of onderzoeksmiddelen (artikel 113). Op de website van de CTIVD vindt u voorbeelden van dergelijke rapporten.[2]

### Behandeling van klachten (artikel 114 t/m 124)

Iedereen heeft het recht om een klacht in te dienen bij de afdeling Klachtbehandeling van de CTIVD. Deze klacht moet gaan over het optreden van de AIVD, de MIVD of de betrokken ministers jegens een persoon of organisatie. Hiervoor geldt de volgende procedure:

- Voordat iemand een klacht indient bij de CTIVD, moet hij eerst de minister op de hoogte brengen en deze de gelegenheid geven om op de klacht te reageren (artikel 114).
- De afdeling Klachtbehandeling moet elke klacht in behandeling nemen, behalve als zij niet bevoegd is om een onderzoek in te stellen. Dat is bijvoorbeeld het geval als er een procedure loopt bij de rechter. Ook is de afdeling niet verplicht om een klacht te onderzoeken als de klager niet zelf benadeeld is, als er al aan de klacht tegemoet is gekomen, of als er sprake is van een van de andere uitzonderingen in de wet (artikel 120 t/m 122).

[2] Zie: **https://www.ctivd.nl/onderzoeken.**

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

- Als de afdeling een klacht in behandeling neemt, beoordeelt zij of er behoorlijk is gehandeld in de situatie waarover de klacht gaat. Dit oordeel stuurt zij naar de klager en naar de minister. Oordeelt de afdeling dat er sprake is (geweest) van onrechtmatig of onbehoorlijk gedrag? Dan kan zij bepalen dat de dienst moet stoppen met het onderzoek en/of met de uitoefening van een bevoegdheid, en/of dat de dienst de verwerkte gegevens moet vernietigen. De minister moet zich aan deze uitspraak houden (artikel 124).

### Behandeling van meldingen van mogelijke misstanden (artikel 125 t/m 131)

De afdeling Klachtbehandeling behandelt ook meldingen van mogelijke misstanden bij de AIVD of de MIVD. Deze meldingen kunnen gedaan worden door medewerkers van de diensten of door andere betrokkenen bij de uitvoering van de wet. Hiervoor geldt de volgende procedure:

- Iemand kan een melding doen als hij vermoedt dat er sprake is van een misstand binnen een dienst, waardoor het maatschappelijk belang in het geding is of waardoor er risico's zijn voor de veiligheid van personen of voor het goed functioneren van de dienst. De melder moet hiervoor eerst aankloppen bij de leidinggevende of vertrouwenspersoon van de dienst. Is het niet redelijk om dat van de klager te vragen, dan kan hij de melding direct doen bij de afdeling Klachtbehandeling (artikel 125 en 126).
- Als de afdeling Klachtbehandeling de melding in behandeling neemt, geeft ze de inhoud ervan door aan de minister. Daarbij zorgt ze ervoor dat de identiteit van de melder niet bekend wordt, tenzij deze daar zelf mee instemt (artikel 127).
- De afdeling Klachtbehandeling hoeft geen onderzoek in te stellen of voort te zetten als de misstand al eerder is onderzocht, als de melder onvoldoende aan het onderzoek meewerkt of als er sprake is van een van de andere uitzonderingen in de wet (artikel 128).
- Als de afdeling Klachtbehandeling de melding wel in behandeling neemt, onderzoekt ze of het aannemelijk is dat er sprake is van een misstand. Van dat onderzoek brengt ze een rapport uit, waarop de melder en de minister mogen reageren. Daarna stelt de afdeling het rapport vast en meldt ze het definitieve oordeel aan de minister. De minister laat binnen 2 weken weten wat hij met het oordeel gaat doen en wanneer. Ook stuurt hij het oordeel en de reactie naar de Eerste en Tweede Kamer. In de praktijk zal het meestal gaan naar de Commissie Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer (CIVD), ook wel de 'commissie-Stiekem' genoemd (artikel 131).

### Verslaglegging door de CTIVD (artikel 106 en artikel 132 t/m 134)

De vergaderingen van de CTIVD en haar afdelingen zijn niet openbaar (artikel 106). Dat geldt ook voor de gegevens die de diensten en andere betrokkenen aan de commissie en haar afdelingen hebben verstrekt. Verzoeken om kennisneming of openbaarmaking van deze gegevens worden geweigerd (artikel 133). Wel openbaar is het jaarverslag dat de CTIVD uitbrengt (artikel 132).

### Meer informatie

Lees de officiële wettekst van artikel 97 t/m 134 van de Wiv 2017 op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e3671.**

## Hoofdstuk 8: Geheimhouding

Hoofdstuk 8 van de Wiv 2017 gaat over de geheimhoudingsplicht van iedereen die betrokken is bij de uitvoering van deze wet. Verder gaat het hoofdstuk over de verplichting om inlichtingen te verstrekken in bestuursrechtelijke en civiele procedures, en de mogelijkheden om dat te weigeren. In alle gevallen komt het erop neer dat de rechter beslist of geheimhouding van informatie gerechtvaardigd is. Dit sluit aan bij artikel 6 van het Europees Verdrag tot bescherming van de rechten van de mens (EVRM), dat gaat over het vereiste van een eerlijk proces.

### Geheimhoudingsplicht voor ambtenaren en andere betrokkenen bij de wet (artikel 135 en 136)

Ambtenaren van de AIVD en de MIVD zijn verplicht om alle vertrouwelijke gegevens geheim te houden die zij ter beschikking krijgen. Dat geldt ook voor andere mensen die betrokken zijn bij de uitvoering van de Wiv 2017, zoals ambtenaren van de IND of medewerkers van telecomaanbieders. Zij mogen deze gegevens alleen bekendmaken als een wettelijk voorschrift hen daartoe verplicht. De geheimhoudingsverplichting blijft bestaan als iemand niet meer betrokken is bij de uitvoering van de wet (artikel 135).

Moet een ambtenaar die betrokken is (geweest) bij de uitvoering van de wet optreden als getuige of deskundige? Dan mag hij alleen vertrouwelijke informatie verstrekken als de verantwoordelijke minister en de minister van Justitie en Veiligheid hem daarvoor toestemming hebben gegeven (artikel 136).

### Inlichtingen verstrekken in een bestuursrechtelijke procedure (artikel 137)

Een minister die verantwoordelijk is voor de inlichtingendiensten, kan in een bestuursrechtelijke procedure verplicht worden om inlichtingen te verstrekken, stukken te overleggen of

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

deze ter inzage te geven. Denk bijvoorbeeld aan een procedure over een besluit van een burgemeester dat (mede) gebaseerd is op informatie van de AIVD (ambtsberichten). Deze verplichting geldt ook voor de commissie van toezicht (CTIVD). De minister of commissie kan aan die verplichting voldoen met het voorbehoud dat alleen de bestuursrechter kennis mag nemen van de inlichtingen en stukken. Zij mogen dit voorbehoud alleen maken als ze daarvoor gewichtige redenen hebben.

De bestuursrechter beoordeelt vervolgens of het gerechtvaardigd is dat alleen hij de inlichtingen en stukken mag lezen en de andere partij in de procedure niet. Oordeelt hij dat dit niet gerechtvaardigd is, dan stelt hij de minister of de commissie in de gelegenheid om het voorbehoud in te trekken. Doen zij dit niet, dan ontvangen zij de stukken terug en worden deze niet in de procedure gebruikt.

### Inlichtingen verstrekken in een civielrechtelijke procedure (artikel 138)

Ook in een civielrechtelijke procedure kan er sprake zijn van geheime stukken. Artikel 138 legt vast wat hierover al in de jurisprudentie is ontwikkeld. De staat (de regering) kan in zo'n civielrechtelijke procedure verplicht worden om inlichtingen te verstrekken, stukken te overleggen of deze ter inzage te geven. De staat kan dit weigeren met een beroep op geheimhouding om gewichtige redenen, bijvoorbeeld wanneer door inzage in die geheime stukken de bronnen of de werkwijze van de AIVD of de MIVD bekend zouden worden. In dat geval geeft de staat de inlichtingen en stukken wel ter inzage aan de rechter, zodat deze kan beoordelen of de weigering gerechtvaardigd is.

Oordeelt de rechter dat de weigering gerechtvaardigd is, dan hoeft de staat de stukken niet te verstrekken. Wel kan de staat de rechter toestaan om de stukken te betrekken bij de beoordeling van de zaak, zonder dat de andere partij hiervan kennis kan nemen. De rechter doet dit alleen als de andere partij daar toestemming voor geeft.

Oordeelt de rechter dat de weigering niet gerechtvaardigd is, maar houdt de staat aan de weigering vast? Of geeft de andere partij geen toestemming om de stukken bij de beoordeling van de zaak te betrekken? Dan trekt de rechter zich terug uit de zaak en stuurt hij de stukken naar de staat terug.

### Meer informatie

Lees de officiële wettekst van artikel 135 t/m 139 van de Wiv 2017 op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e4700**

## Hoofdstuk 9: Bonaire, Sint Eustatius en Saba

Het korte hoofdstuk 9 van de Wiv 2017 gaat over Caribisch Nederland: Bonaire, Sint Eustatius en Saba (de BES-eilanden). Deze 3 'openbare lichamen' functioneren als een bijzondere gemeente van Nederland. In de bepalingen van dit hoofdstuk staat:

- De Wiv 2017 is ook van toepassing op Bonaire, Sint Eustatius en Saba (artikel 140).
- Telecomproviders die hun diensten aanbieden op de eilanden, zijn verplicht om mee te werken aan de uitvoering van de bijzondere bevoegdheden van de AIVD en de MIVD. Dat wil zeggen dat de telecomaanbieders moeten meewerken aan het aftappen of opnemen van communicatie en dat zij op verzoek gegevens moeten verstrekken over een gebruiker of over zijn telecommunicatieverkeer.
- In bijzondere gevallen kunnen providers ontheffing krijgen van deze plicht tot meewerken. Dit kan alleen als de ministers van Binnenlandse Zaken en Koninkrijksrelaties, Defensie en Economische Zaken en Klimaat gezamenlijk besluiten zo'n ontheffing af te geven (artikel 142).

### Meer informatie

Lees de officiële wettekst van artikel 140 t/m 142 van de Wiv 2017 op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e4807.**

## Hoofdstuk 10: Straf-, overgangs- en slotbepalingen

Als de Wiv 2017 in werking treedt, zijn er enkele aanpassingen nodig in andere wetten, zoals de Telecommunicatiewet, de Algemene wet bestuursrecht en de Wet politiegegevens. Hoofdstuk 10 legt vast welke aanpassingen er moeten worden gedaan. Ook bepaalt hoofdstuk 10 dat overtreding van bepaalde artikelen uit deze wet strafbaar is. Dit worden strafbepalingen genoemd. Tot slot gaat het hoofdstuk in op de evaluatie en de inwerkingtreding van de wet.

### Strafbepalingen (artikel 143)

De diensten hebben bij hun werk in een aantal gevallen medewerking nodig van post- en vervoerbedrijven en (tele) communicatiediensten. Daarbij gaat het onder andere om het onderscheppen van post, het aftappen van telecommunicatie, het ontsleutelen van (technische) gegevens en het verstrekken van gegevens over gebruikers van communicatiediensten. In hoofdstuk 3 (zie pagina 17) is bepaald wanneer deze medewerking verplicht is. Voldoen de genoemde bedrijven of personen niet aan deze verplichting, dan zijn ze strafbaar.

REFERENDUM commissie

# Samenvatting van de Wet op de inlichtingen- en veiligheidsdiensten 2017

### Evaluatie (artikel 167)

Artikel 167 bepaalt dat de regering binnen 5 jaar nadat de wet is ingegaan, een evaluatie naar het parlement moet sturen over de werking van de wet. De Tweede Kamer heeft echter de motie-Recourt[3] aangenomen die bepaalt dat de regering binnen 2 jaar een rapportage moet maken over de bewaartermijn van gegevens. Daarnaast heeft de minister van BZK namens de regering in de Eerste Kamer toegezegd[4] dat er binnen 2 jaar een evaluatie komt over de Toetsingscommissie Inzet Bevoegdheden (TIB). Deze toezegging is eind 2017 verbreed[5] naar een evaluatie van de Wiv 2017 na 2 jaar door een onafhankelijke commissie. Deze commissie moet in elk geval aandacht besteden aan het verzamelen van gegevens, de internationale uitwisseling van gegevens, de TIB en de bewaartermijnen.

### Inwerkingtreding (art 171)

Artikel 171 bepaalt dat de artikelen van de Wiv 2017 in werking treden op een tijdstip dat de regering bepaalt. Verschillende onderdelen van de wet kunnen op verschillende tijdstippen ingaan.

Inmiddels zijn op 1 september 2017 al enkele onderdelen van de wet van kracht geworden. Daarbij gaat het om de wetsartikelen over de samenstelling van de nieuwe, onafhankelijke toetsingscommissie (TIB) en de afdeling Klachtbehandeling van de commissie van toezicht (CTIVD). De leden daarvan moeten worden geworven voordat de wet volledig van kracht kan zijn.

De overige onderdelen van de wet zouden op 1 januari 2018 ingaan, maar dit is uitgesteld. De reden is dat er meer tijd nodig is om kandidaten voor de TIB te vinden. Inwerkingtreding van de wet op 1 mei 2018 lijkt haalbaar. Als de uitslag van het referendum een 'nee' is tegen de Wiv 2017, zal de regering de wet opnieuw moeten overwegen.

### Meer informatie

Lees de officiële wettekst van artikel 143 t/m 172 van de Wiv 2017 op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html#d17e4837.**

[3] De tekst van deze motie is te vinden op Tweedekamer.nl: **http://bit.ly/2CF9zRo.**
[4] Dit valt terug te lezen op Eerstekamer.nl**: https://www.eerstekamer.nl/toezegging/versnelde_evaluatie_tib_34_588.**
[5] Zie de Kamerbrief op Rijksoverheid.nl: **http://bit.ly/2EReg83.**

REFERENDUM commissie

# Ontstaan van de Wet op de inlichtingen- en veiligheidsdiensten 2017

In 2017 namen de Eerste en Tweede Kamer de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) aan. Deze wet vervangt de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). De nieuwe wet is in verschillende stappen tot stand gekomen. Op deze pagina leest u hoe dat proces is verlopen en wanneer de wet mogelijk in werking treedt.

## Advies van de commissie van toezicht

De eerste stap naar de Wiv 2017 dateert uit 2011. Die stap was een advies aan de regering van de CTIVD, de toezichthouder op de inlichtingen- en veiligheidsdiensten. De CTIVD adviseerde onder meer: onderzoek of de diensten de bevoegdheid moeten krijgen om breder telecommunicatie via de kabel te onderscheppen. De Wiv 2002 was op dat punt volgens de CTIVD 'wat gedateerd'.

## Evaluatie van de commissie-Dessens

Naar aanleiding van het advies van de CTIVD vroeg de Tweede Kamer om een evaluatie van de Wiv 2002. De commissie-Dessens voerde deze evaluatie uit in 2013. Dessens adviseerde onder meer om brede onderschepping van informatie via de kabel mogelijk te maken. De commissie pleitte ook voor een steviger toezicht op de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten.

## Consultatie

Vervolgens stelde de regering een conceptwetsvoorstel op. In 2015 konden burgers, organisaties en bedrijven hun mening over dit voorstel geven in een internetconsultatie. Dit leverde meer dan 1100 reacties op. De regering vroeg apart om een reactie van de Nationale ombudsman en de CTIVD. Dit omdat het wetsvoorstel gevolgen had voor de werkwijzen van deze organisaties.

## Privacy Impact Assessment

In 2016 volgde in opdracht van de regering een onafhankelijk Privacy Impact Assessment (PIA), uitgevoerd door wetenschappers van TNO en het Tilburg Institute for Law, Technology, and Society (TILT). Een PIA is een analyse van de effecten van een wetsvoorstel (of van een product of dienst) op de privacy van mensen. De PIA oordeelde kritisch over het wetsvoorstel. Zo concludeerden de onderzoekers onder meer dat privacyrisico's onvoldoende werden onderkend en dat de voorgestelde waarborgen vaak niet voldoende waren om die risico's af te dekken.

## Advies van de Raad van State

Vanzelfsprekend adviseerde ook de Raad van State over het wetsvoorstel. In dit advies oordeelde de Raad dat het wetsvoorstel voldeed aan de eisen die voortvloeien uit het Europees Verdrag tot bescherming van de rechten van de mens (EVRM). Wel uitte de Raad ernstige twijfels over de effectiviteit van het voorgestelde toezichtstelsel. Zo zou de nieuw te vormen Toetsingscommissie Inzet Bevoegdheden (TIB) onbedoeld slechts een 'alibifunctie' kunnen vervullen (door 'het zekere voor het onzekere' te nemen en standaard toestemming te verlenen). Ook had de Raad van State ernstige twijfels over de bewaartermijn van gegevens die diensten verzamelen door het breed onderscheppen van telecommunicatie.

## Aangepast wetsvoorstel

Al deze reacties en adviezen leidden tot een aangepast wetsvoorstel dat de regering in het najaar van 2016 naar de Tweede Kamer stuurde. In hoofdstuk 12 van de Memorie van Toelichting op de Wiv 2017 beschrijft de regering hoe de reacties en aanbevelingen in het nieuwe wetsvoorstel zijn verwerkt. Deze Memorie van Toelichting is te vinden op **https://zoek.officielebekendmakingen.nl/kst-34588-3.html.**

## Behandeling in de Tweede en Eerste Kamer

In februari 2017 stemde de Tweede Kamer in met de Wet op de inlichtingen- en veiligheidsdiensten 2017, die op een enkel punt nog geamendeerd (gewijzigd) was door Kamerleden. De PvdA, VVD, SGP, ChristenUnie, CDA, PVV, Groep Bontes/Van Klaveren, Van Vliet, 50PLUS, Houwers en Monasch stemden voor. GroenLinks, PvdD, SP, Groep Kuzu/Öztürk (DENK), Klein en D66 stemden tegen.

De Eerste Kamer ging akkoord in juli 2017. De VVD, PvdA, CDA, SGP, ChristenUnie, 50PLUS, OSF en PVV stemden voor. GroenLinks, PvdD, SP en D66 stemden tegen.

Alle stukken van de parlementaire behandeling vindt u in de verzamelde Kamerstukken: **http://bit.ly/2EMz5AL**

Daarnaast vindt u op **www.referendumwiv2017.nl** op de pagina 'Ontstaan van de Wet op de inlichtingen- en veiligheidsdiensten 2017' rechtstreekse links naar onder meer:

- het verslag van het debat in de Tweede Kamer op 8 februari 2017
- de stemverhoudingen en aangenomen amendementen in de Tweede Kamer
- het verslag van het debat in de Eerste Kamer op 11 juli 2017.

## Inwerkingtreding van de wet

Op 1 september 2017 zijn enkele onderdelen van de wet in werking getreden. Het gaat om de wetsartikelen over de samenstelling van de nieuwe, onafhankelijke toetsingscommissie (TIB) en de afdeling Klachtbehandeling van de commissie van toezicht (CTIVD). De leden daarvan moeten worden geworven voordat de wet volledig van kracht kan zijn.

De overige onderdelen van de wet zouden op 1 januari 2018 ingaan, maar dit is uitgesteld. De reden is dat er meer tijd nodig is om kandidaten voor de TIB te vinden. Inwerkingtreding van de hele wet op 1 mei 2018 lijkt haalbaar. Als de uitslag van het

referendum een 'nee' is tegen de Wiv 2017, dan zal de regering de wet opnieuw moeten overwegen.

### Meer weten?

Op **www.referendumwiv2017.nl** vindt u op de pagina 'Ontstaan van de Wet op de inlichtingen- en veiligheidsdiensten 2017' links naar onder meer:

- het evaluatierapport van de commissie-Dessens
- de reacties op de internetconsultatie
- de rapportage van het Privacy Impact Assessment
- het advies van de Raad van State.

Daarnaast vindt u op deze website het antwoord op een aantal veelgestelde vragen over de Wiv 2017 en het referendum.

De wettekst zelf vindt u op Overheid.nl:
**https://zoek.officielebekendmakingen.nl/stb-2017-317.html**

REFERENDUM commissie

# Veelgestelde vragen over de Wiv 2017 en het referendum van 21 maart 2018

Waarom wordt er een referendum gehouden de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017)? Worden er mensenrechten geschonden door deze wet? En wat gebeurt er met de uitkomst van het referendum? Hieronder vindt u het antwoord op deze en andere veelgestelde vragen.

## Vragen over het referendum op 21 maart 2018

### Waarom wordt er een referendum gehouden over de Wiv 2017?

Er wordt een raadgevend referendum gehouden over de Wiv 2017 omdat hiervoor voldoende geldige verzoeken zijn ingediend. Dit gebeurde na een oproep van 5 Amsterdamse studenten die het 'Sleepwet-burgerinitiatief' startten. Zij kregen steun van een aantal organisaties, zoals Amnesty International en Bits of Freedom. Op 1 november 2017 stelde de Kiesraad het aantal geldige verzoeken vast: 384.126. Er waren er 300.000 vereist voor een referendum.

De mogelijkheid van een raadgevend referendum over wetten en verdragen bestaat sinds 1 juli 2015. Daarvan is 1 keer eerder gebruikgemaakt: in april 2016 is een referendum gehouden over de Associatieovereenkomst tussen de Europese Unie en Oekraïne. Op de website van de Kiesraad leest u meer over de procedure voor het houden van een referendum.[1] Deze procedure is gebaseerd op de Wet raadgevend referendum.

### Wat houdt 'raadgevend' precies in?

Het referendum is raadgevend, niet bindend. Dat wil zeggen dat regering en parlement niet verplicht zijn de uitslag te volgen. De uitslag is een advies.

### Ik heb gehoord dat het referendum wordt afgeschaft. Gaat het referendum over de Wiv 2017 wel door?

In het regeerakkoord is inderdaad afgesproken dat het raadgevend referendum wordt afgeschaft. Er is een intrekkingswet opgesteld, die op 20 december 2017 bij de Tweede Kamer is ingediend. De Raad van State heeft daarvoor in zijn advies gesteld dat het juridisch mogelijk is om in de intrekkingswet expliciet te regelen dat de Wet raadgevend referendum daarop niet van toepassing is. In 2018 moeten de Eerste en Tweede Kamer over de intrekkingswet beslissen. Het besluit over het referendum over de Wiv 2017 is genomen vóórdat deze intrekkingswet eventueel in werking treedt. Daarom gaat dit referendum gewoon door.

### Hoe kan ik bepalen of ik voor of tegen de Wiv 2017 ben?

De Referendumcommissie informeert over de wet waarover het referendum gaat. In dit geval is dat de Wet op de inlichtingen- en veiligheidsdiensten 2017. Bij de informatie over de inhoud van de wet beperkt de commissie zich tot de wettekst. De commissie heeft er geen oordeel over. Wilt u weten wat de standpunten zijn van de voor- en tegenstanders van de wet? Volg dan in de periode voorafgaand aan het referendum het publieke debat. Dat kan via diverse media.

### Wat gebeurt er met de uitkomst van dit referendum?

Als minder dan 30% van de kiesgerechtigden heeft gestemd, is de uitslag ongeldig. Dan kan de regering de wet in werking laten treden. Als 30% of meer heeft gestemd, is de uitslag van het referendum geldig.

Als de uitslag geldig is, zijn er volgens de Wet raadgevend referendum 2 mogelijkheden:

- Een meerderheid van de kiezers is vóór. Dan kan de regering de wet in werking laten treden.
- Een meerderheid van de kiezers is tégen. Dan heeft de regering 2 mogelijkheden: het parlement voorstellen om de wet in te trekken. Of het parlement voorstellen om de uitslag van het referendum niet te volgen en de wet toch in te voeren. Het parlement kan het kabinetsvoorstel vervolgens goedkeuren of verwerpen.

Het referendum is raadgevend, niet bindend. Dat wil zeggen dat regering en parlement niet verplicht zijn de uitslag te volgen. Op de website van de Kiesraad leest u meer over het proces rond de uitslag van het referendum.[2]

### Wat gebeurt er als de Wiv 2017 wordt ingetrokken?

Als de regering en het parlement besluiten om de Wiv 2017 in te trekken, blijft de Wiv 2002 van kracht. De inlichtingen- en veiligheidsdiensten houden dan de bevoegdheden die ze nu hebben. Waarschijnlijk komt de regering dan later met een nieuw voorstel ter vervanging van de Wiv 2002.

## Vragen over de inhoud van de Wiv 2017

### Wat zijn inlichtingen- en veiligheidsdiensten?

Dat zijn in Nederland de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Beide overheidsdiensten worden in de volksmond soms 'geheime diensten' genoemd. De AIVD valt onder de verantwoordelijkheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), de MIVD onder die van het ministerie van Defensie.

De opdracht van de AIVD en de MIVD is om de veiligheid en democratische rechtsorde te helpen beschermen. Dat doen ze door informatie te verzamelen, waardoor ze een grotere kans hebben om dreigingen en risico's tijdig te herkennen. Daarbij gaat het onder meer om dreigingen voor de Nederlandse samenleving en voor vredesoperaties, en om (internationaal)

[1] Kijk hiervoor op **https://www.kiesraad.nl/verkiezingen/raadgevend-referendum**
[2] Kijk hiervoor op **https://www.kiesraad.nl/verkiezingen/raadgevend-referendum/uitslagen**

# Veelgestelde vragen over de Wiv 2017 en het referendum van 21 maart 2018

terrorisme. Dat geldt voor de AIVD, maar ook voor de MIVD voor zover de krijgsmacht daarbij betrokken is of kan raken.

### Waarom is een nieuwe wet op de inlichtingen- en veiligheidsdiensten nodig?

Volgens de regering is vervanging van de Wiv 2002 om verschillende redenen noodzakelijk. Een belangrijke reden is volgens haar de toegenomen dreiging van terreur- en cyberaanvallen. Een andere is de snel veranderende communicatietechnologie: het merendeel van de internationale telecommunicatie verloopt niet langer door de lucht (via de ether), maar via glasvezel- en koperkabels.

De Wiv 2017 maakt het voor de AIVD en de MIVD mogelijk om onder voorwaarden uitgebreider communicatie te onderscheppen die via kabelnetwerken verloopt. Dat vergroot hun bereik, maar ook de kans dat ze inbreuk maken op de privacy van burgers. Mede daarom is in de Wiv 2017 het onafhankelijk toezicht op het werk van de diensten uitgebreid. U leest hierover meer op pagina 3 van dit document.

### In de media gaat het veel over de 'sleepwet', de 'sleepnetwet' of de 'aftapwet'. Hoe zit dat?

Het gebruik van de termen 'sleepwet', 'sleepnetwet' en 'aftapwet' heeft te maken met enkele onderdelen van de Wiv 2017. Gebruikers van deze termen doelen op de mogelijkheid die de AIVD en de MIVD krijgen om kabelgebonden telecommunicatie 'breed' te onderscheppen. Dat wil zeggen dat de onderschepte gegevens niet gericht hoeven te zijn op een specifieke persoon of organisatie. Zo'n breed verkennend onderzoek van gegevens kan nodig zijn als er bij een bepaalde dreiging geen zicht is op specifieke personen.

Bij een dergelijk onderzoek is het mogelijk dat de diensten ook communicatie onderscheppen van onschuldige burgers. In het publieke debat wordt dit wel 'slepen' of 'bulkinterceptie' genoemd. Breed onderscheppen betekent echter niet dat dit volledig ongericht gebeurt. De diensten mogen alleen gegevens verzamelen met een specifiek doel (een bepaalde dreiging) en alleen als dat noodzakelijk is. Ook moeten ze niet-relevante gegevens zo snel mogelijk vernietigen. In de wet heet dit 'onderzoeksopdrachtgerichte interceptie' (OOG-interceptie). De diensten mogen deze bevoegdheid alleen inzetten als ze daarvoor toestemming hebben van de minister. Deze toestemming is een jaar geldig, maar kan met (nieuwe) toestemming van de minister telkens met een jaar worden verlengd.

Deze nieuwe bevoegdheid wordt in de Wiv 2017 gecombineerd met de instelling van een nieuwe, onafhankelijke toetsingscommissie (TIB). Deze toetst vooraf of de brede onderschepping van gegevens rechtmatig is. Ook toetst de commissie of de bevoegdheid niet te breed wordt ingezet. De TIB kan een besluit van de minister om dataverkeer te onderscheppen, tegenhouden. Een andere onafhankelijke (al bestaande) commissie, de CTIVD, controleert achteraf of de diensten zich aan de wet hebben gehouden.

### Kunnen de AIVD en de MIVD ook gegevens van onschuldige burgers verzamelen?

Ja, bij de brede onderschepping van dataverkeer (de zogeheten OOG-interceptie) verzamelen de diensten ook gegevens van mensen die niets kwaads in de zin hebben. Zodra blijkt dat deze gegevens niet van belang zijn, worden ze vernietigd. Wel kan het enige tijd duren voordat de diensten de verzamelde gegevens op relevantie hebben onderzocht. Als ze dit niet binnen 3 jaar gedaan hebben, moeten ze de gegevens hoe dan ook vernietigen. Overigens mogen de diensten alleen breed communicatie onderscheppen als ze daarvoor toestemming hebben van de minister én van de Toetsingscommissie Inzet Bevoegdheden (TIB).

### Worden er mensenrechten geschonden door deze wet?

Met hun werkzaamheden kunnen de inlichtingen- en veiligheidsdiensten inbreuk plegen op de persoonlijke levenssfeer (privacy) van mensen. Door de verruiming van de bevoegdheden in de Wiv 2017 is de mogelijkheid van zo'n inbreuk groter dan onder de huidige wet. Tegelijkertijd biedt de Wiv 2017 extra waarborgen voor de privacy van burgers. Zo mogen de diensten sommige bevoegdheden alleen inzetten als ze daarvoor toestemming hebben van de minister en van de onafhankelijke Toetsingscommissie Inzet Bevoegdheden (TIB). Bovendien houdt een andere onafhankelijke commissie, de CTIVD, toezicht op de uitoefening van die bevoegdheden.

De nieuwe wet vergroot het bereik van de diensten en daarmee de mogelijkheid dat er inbreuk wordt gemaakt op de privacy van burgers. Door een pakket aan extra waarborgen probeert de wet een balans aan te brengen tussen het belang van de nationale veiligheid en de privacy van individuele personen. Het publieke debat richt zich op de vraag of die balans goed is gekozen.

### Kunnen gegevens worden doorgegeven aan buitenlandse veiligheidsdiensten?

Ja, dat kan soms, onder bepaalde voorwaarden. De AIVD en de MIVD kunnen gegevens uitwisselen met buitenlandse veiligheidsdiensten waarmee ze een samenwerkingsrelatie hebben. Het gaat hier om alle gegevens, ook als die nog niet zijn onderzocht op relevantie. Dat betekent dat er nog gegevens bij kunnen zitten over niet-kwaadwillende burgers. Daarom is hiervoor toestemming nodig van de minister. Gaat het om gegevens die zijn verzameld door het breed onderscheppen van telecommunicatie? Dan moeten de diensten meteen de commissie van toezicht (CTIVD) informeren. Deze kan controleren of de verstrekking van de gegevens rechtmatig plaatsvindt.

REFERENDUM commissie

# Veelgestelde vragen over de Wiv 2017 en het referendum van 21 maart 2018

Onder voorwaarden mogen de AIVD of de MIVD gegevens – ook als deze verzameld zijn door brede onderschepping van telecom municatie uitwisselen met een collega-dienst waarmee geen samenwerkingsrelatie bestaat. Dit mag alleen als er door het niet geven van deze gegevens mensenlevens in gevaar kunnen komen.

### Kunnen advocaten en journalisten hun werk nog doen?

De Wiv 2017 bevat een extra waarborg voor de privacy van advocaten en journalisten. Deze waarborg richt zich op de gevallen waarin de AIVD of de MIVD de communicatie van een journalist met zijn bron of van een advocaat met zijn cliënt wil aftappen of op een andere manier wil onderscheppen. In die gevallen moet de dienst daarvoor eerst toestemming vragen aan de Rechtbank Den Haag. De rechtbank verleent alleen toestemming nadat ze het bijzondere belang van journalisten en advocaten goed heeft afgewogen. Ook moeten er concrete aanwijzingen dat er een direct gevaar is voor de nationale veiligheid.

### Helpt deze wet ook bij de bestrijding van cyberaanvallen?

Met de Wiv 2017 krijgen de AIVD en de MIVD meer en duidelijker omschreven bevoegdheden als het gaat om het onderscheppen van telecommunicatie en het hacken van computers. Daardoor neemt het bereik van de diensten toe en is er een grotere kans dat zij tijdig inlichtingen verkrijgen die kunnen helpen om dreigingen op en via het internet tegen te gaan. Een voorbeeld van zo'n dreiging is diefstal van digitale gegevens (staatsgeheimen, vitale economische informatie of persoonsgegevens). Andere voorbeelden zijn de beïnvloeding van het politieke debat, sabotage van digitale systemen en de ondermijning van militaire missies.

### Zijn providers verplicht om mee te werken aan aftappen?

Ja. De AIVD of de MIVD kan aanbieders van communicatiediensten de opdracht geven om mee te werken aan het onderscheppen van telecommunicatie. Dit is volgens de regering nodig omdat de diensten niet zelfstandig communicatieverkeer via de kabel kunnen aftappen. Ook zijn de aanbieders verplicht om op verzoek van de diensten gegevens te verstrekken over het communicatieverkeer van een bepaalde persoon, of om de opgeslagen communicatie van die persoon te leveren.
De diensten mogen de aanbieders hier alleen om vragen na toestemming van de minister. De regels hiervoor staan in hoofdstuk 3 van de Wiv 2017 (op pagina 17 vindt u een samenvatting van dit hoofdstuk).

### Kan ik inzage krijgen in de gegevens die de diensten van mij hebben?

Wilt u weten of de AIVD of de MIVD gegevens over u hebben verwerkt, dan kunt u bij de verantwoordelijke minister navragen of dat zo is. Op de website van de AIVD[3] leest u hoe u dat onder de huidige wet kunt doen. In de nieuwe wet, de Wiv 2017, blijven de regels hetzelfde.

De minister moet uw vraag binnen 3 maanden beantwoorden. Als er inderdaad gegevens over u zijn verzameld, kunt u deze binnen 4 weken inzien. Dit kan echter alleen als de diensten de gegevens langer dan 5 jaar geleden hebben verwerkt en als het verstrekken ervan geen risico's oplevert voor de nationale veiligheid of voor andere belangen. U leest hierover meer in hoofdstuk 5 van de Wiv 2017 (op pagina 22 vindt u een samenvatting van dit hoofdstuk).

Overigens kunt u alleen inzage krijgen in gegevens die de diensten al hebben onderzocht op relevantie. Hebben de diensten gegevens verzameld door het breed onderscheppen van telecommunicatie? En zijn deze gegevens nog niet onderzocht op relevantie? Dan kunt u ze niet inzien, omdat in dat geval onbekend is of er informatie over u tussen zit.

### Verzamelen de inlichtingen- en veiligheidsdiensten gegevens over iedereen in Nederland?

Nee. De diensten verzamelen geen gegevens over iedereen die zich in Nederland bevindt. De diensten zoeken zo gericht mogelijk naar informatie over personen die een dreiging vormen voor de nationale veiligheid. Wel kan het zijn dat bij de brede onderschepping van dataverkeer gegevens worden verzameld van mensen die niets met die dreiging te maken hebben. Leest u ook het antwoord op de vraag 'Kunnen de AIVD en de MIVD ook gegevens van onschuldige burgers verzamelen?'.

### Waar kan ik met mijn klachten over de inlichtingen- en veiligheidsdiensten terecht?

Als u een klacht heeft over het handelen van de AIVD of de MIVD, kunt u daarvoor terecht bij de afdeling Klachtbehandeling van de toezichtcommissie CTIVD. In de Wiv 2017 is vastgelegd dat dit een aparte afdeling wordt, die onafhankelijk opereert van de diensten én van de afdeling Toezicht van de CTIVD. Na onderzoek van uw klacht kan de afdeling Klachtbehandeling een bindende uitspraak doen en bijvoorbeeld bepalen dat de dienst een onderzoek moet stoppen of gegevens moet vernietigen. De minister moet deze uitspraak overnemen.

### Houdt de AIVD of de MIVD precies bij wat ik zeg op WhatsApp of Facebook?

Nee. De diensten houden niet bij welke berichten alle Nederlanders op internet of via andere communicatiekanalen uitwisselen. De diensten zoeken zo gericht mogelijk naar informatie over personen die een dreiging vormen voor de nationale veiligheid. Wel kan het zijn dat bij de brede onderschepping van dataverkeer gegevens worden verzameld van mensen die niets met die dreiging te maken hebben. Leest u ook het antwoord op de vraag 'Kunnen de AIVD en de MIVD ook gegevens van onschuldige burgers verzamelen?'.

[3] Zie hiervoor **http://bit.ly/2DkEMIR**

REFERENDUM commissie

# Veelgestelde vragen over de Wiv 2017 en het referendum van 21 maart 2018

### Wat doen de diensten als ze bij hun onderzoeken stuiten op strafbare feiten?

Als de AIVD en de MIVD bij hun onderzoeken stuiten op strafbare feiten kunnen ze die melden aan het Openbaar Ministerie (OM). Het OM kan vervolgens overgaan tot opsporing en vervolging. Zijn de diensten op strafbare feiten gestuit bij het onderscheppen van vertrouwelijk communicatieverkeer tussen een advocaat en een cliënt? Dan mogen ze die alleen bij het OM melden als ze daarvoor toestemming hebben van de Rechtbank Den Haag.

In bepaalde gevallen kunnen de diensten besluiten om strafbare feiten níet te melden. Dit kunnen ze doen als opsporing en vervolging door het OM hun onderzoek kunnen belemmeren. Daarbij moeten ze rekening houden met de ernst van het delict: hoe ernstiger dit is, hoe kleiner de ruimte wordt om dit delict niet bij het OM te melden. Dat is bepaald in hoofdstuk 3 van de Wiv 2017 (op pagina 17 vindt u een samenvatting van dit hoofdstuk).

### Wie zitten er in de CTIVD en de TIB, de toezichthouders op de diensten?

Als de diensten een bijzondere bevoegdheid willen inzetten die de privacy van burgers aantast, moeten ze daarvoor toestemming vragen van de verantwoordelijke minister. De minister legt die toestemming vervolgens voor aan de Toetsingscommissie Inzet Bevoegdheden (TIB). Dit is een nieuwe commissie die van start gaat als de Wiv 2017 in werking treedt. De TIB gaat bestaan uit 3 leden, van wie er minimaal 2 ervaren oud-rechters zijn.

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) houdt toezicht op het werk van de AIVD en de MIVD. Deze commissie bestaat al onder de huidige wet, maar wordt onder de Wiv 2017 gescheiden in een afdeling Toezicht en een afdeling Klachtbehandeling. De CTIVD bestaat uit 4 leden inclusief de voorzitter. 1 lid is voorzitter van de afdeling Klachtbehandeling. De andere 3 vormen de afdeling Toezicht. Bij de afdeling Klachtbehandeling komen daarnaast nog minimaal 2 andere leden te werken. De meeste leden zijn jurist.

### Wat staat er in het regeerakkoord over de Wiv 2017?

In het regeerakkoord 'Vertrouwen in de toekomst' staat (op pagina 4) dat er geen sprake 'kan, mag en zal zijn' van 'het willekeurig en massaal verzamelen van gegevens van burgers in Nederland of het buitenland ('sleepnet')'. Het kabinet zal bij de uitvoering van de wet 'strikt de hand houden aan de extra waarborgen'. Ook komt er binnen 2 jaar na de inwerkingtreding een evaluatie van de Wiv 2017, uitgevoerd door een onafhankelijke commissie. Naar aanleiding van de evaluatie kan het kabinet voorstellen doen om de wet aan te passen. Een toelichting op deze punten uit het regeerakkoord staat in de brief van de minister van BZK (mede namens de minister van Defensie) aan de Tweede Kamer van 15 december 2017.[4]

### Waar vind ik meer informatie over de Wiv 2017?

- Wilt u de complete tekst lezen van de Wiv 2007? Dan vindt u die op Overheid.nl: **https://zoek.officielebekendmakingen.nl/stb-2017-317.html**.
- Daar vindt u ook de Memorie van Toelichting: **https://zoek.officielebekendmakingen.nl/kst-34588-3.html**.

[4] U vindt deze brief op Rijksoverheid.nl: **http://bit.ly/2EReg83**