

Veiligheid en grondrechten in balans

Aanbevelingen voor de herziening van de Wiv 2017

Bericht aan het parlement

Op 3 september 2026 debatteert de commissie Binnenlandse Zaken over IVD-aangelegenheden. Het Rathenau Instituut signaleert dat het herzieningstraject van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) in dit debat niet expliciet geagendeerd staat. Dit terwijl de laatste kabinetsupdate over de herziening van de Wiv 2017 dateert van meer dan een jaar geleden.¹ Om die reden geven wij u enkele aanbevelingen mee ter overweging bij uw inbreng.²

Achtergrond: nieuwe dreigingen, snelle technologische ontwikkelingen

De actualiteit kenmerkt zich door nieuwe dreigingen en rappe technologische ontwikkelingen. Nieuwe dreigingen komen voort uit geopolitieke spanningen en conflicten. Daarnaast kunnen technologische ontwikkelingen bijdragen aan een veranderend dreigingsbeeld. Zo speelt digitalisering een rol bij het ontstaan van nieuwe vormen van extremisme, bijvoorbeeld uit de anti-institutionele hoek³ of vanuit internetniches⁴. Ook maakt toenemende digitalisering ons land steeds kwetsbaarder voor gerichte ontwijking door kwaadwillenden.⁵ Daarnaast dwingt de adoptie van nieuwe (communicatie)technologieën in de samenleving de inlichtingen- en veiligheidsdiensten tot aanpassingen in hun werkwijze; communicatiesporen moeten immers kunnen worden opgepikt.

Bevoegdheden diensten en grondrechten burgers

De bevoegdheden van inlichtingen- en veiligheidsdiensten, zoals vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017), moeten op deze veranderingen toegesneden zijn. Of de huidige Wiv 2017 daarvoor toereikend is, is al langer een punt van

1 De laatste update aan de Kamer over de herziening van de Wiv 2017 dateert uit juni 2025. Zie: Kamerstukken II 2024/25, 34 588, nr. 94.

2 Deze aanbevelingen zijn gebaseerd op het rapport *Signalen voor de toekomst* | Rathenau Instituut, 2025. *Signalen voor de toekomst. Hoe digitale ontwikkelingen menselijke interactie veranderen en wat dit betekent voor I&V-diensten*. Den Haag.

3 Nanninga, P. & F. Valk (2025). *Anti-institutionele tendensen in Nederland: een verkennende literatuurstudie vanuit religiewetenschappelijk perspectief*. Rijksuniversiteit Groningen: pp. 28, 38.

4 The Hague Centre for Strategic Studies. *Van meme tot moord. Hoe online extremistische broedkamers een nieuwe generatie van geweld kweken*. Den Haag: HCSS.

5 <https://www.cybersecurityraad.nl/actueel/nieuws/2026/01/15/csr-waarschuwt-kans-op-digitale-ontwijking-is-reeel>; <https://www.universiteitleiden.nl/nieuws/2025/10/daan-weggemans-digitale-veiligheid-is-niet-iets-voor-specialisten-alleen>; Wetenschappelijke Raad voor het Regeringsbeleid (2019) Voorbereiden op digitale ontwijking, WRR-Rapport 101, Den Haag: WRR.

discussie. De diensten pleiten doorgaans voor meer ‘operationele slagkracht en wendbaarheid’⁶, gezien de ‘ongekend grote en complexe veiligheidsopgave’⁷ waar Nederland voor staat. Dat is ook de inzet van het huidige kabinet en vorige kabinetten bij de aanstaande Wiv 2017-herziening.⁸ Toezichthouders en actiegroepen wijzen juist op het belang van de bescherming van grondrechten van burgers, die volgens hen in het geding kunnen komen als de diensten meer speelruimte krijgen.⁹

Balans tussen veiligheid en grondrechten

De Wiv zou een goede balans tussen (nationale) veiligheid en (individuele) grondrechten moeten reflecteren. Strenge regels rondom de inzet van bevoegdheden en het stelsel van toetsing en toezicht waarborgen deze balans. Het zijn deze *checks and balances* die onze diensten onderscheiden van die van totalitaire regimes.

Met de huidige nadruk op de ‘stapeling van dreigingen’¹⁰ voor de nationale veiligheid kunnen deze onder druk komen te staan. Daarom is het van groot belang om in de herziene Wiv aandacht te hebben voor deze *checks and balances*. Hieronder doet het Rathenau Instituut aanbevelingen ten behoeve daarvan, waarbij we de huidige nadruk op het dreigingsbeeld als uitgangspunt nemen.

Twee daarvan zien specifiek op de herziening van de Wiv 2017. De derde aanbeveling spoort aan tot een reflectie op de taakstelling van de diensten. We sluiten af met een bredere oproep ten behoeve van onze nationale veiligheid.

1. Bepaal grenzen voor gebruik van nieuwe databronnen en technologie

Dreigingen fungeren als wegingsfactor in het bepalen van de proportionaliteit van een voorgenomen inzet van bevoegdheden door de diensten. Hoe groter de dreiging, hoe eerder de inzet van een bevoegdheid proportioneel wordt geacht. Een belangrijke kanttekening daarbij is dat in de afgelopen jaren niet alleen de *dreigingen* zijn toegenomen, maar ook de potentiële *inbreuken* op grondrechten door de diensten. Dit hangt sterk samen met de technologische ontwikkelingen die de slagkracht van de diensten vergroten:

- Ten eerste kunnen de diensten over steeds meer en steeds intiemere gegevens beschikken. Via AI-chatbots en nieuwe consumententechnologieën (zoals *augmented reality*-brillen en neurotechnologie-*wearables*¹¹) laten mensen steeds meer en intiemere digitale sporen achter, die door de diensten opgepikt kunnen worden.
- Ten tweede kunnen de diensten met steeds geavanceerdere AI-systemen op geautomatiseerde wijze grote datasets analyseren, om zo dreigingen op het spoor te komen. Daarmee komen ook meer onschuldige mensen in het vizier van de diensten, waarmee hun privacy in het geding komt.

Het rapport *Signalen voor de toekomst* laat zien dat er vanuit wetgever, toezichthouders en diensten nog weinig reflectie is op deze nieuwe technologische mogelijkheden en de betekenis

6 Brief over de hoofdlijnen van het geheime jaarplan van de AIVD 2026 (Kamerstukken II, 2025/26, 30 977, nr. 176), p. 5.

7 Idem, p. 2.

8 Zie: Hoofdlijnennotitie wijziging Wiv 2017 (Kamerstukken II, 2022/23, 34 588, nr. 92; Stand van zaken Herziening Wet op de inlichtingen- en veiligheidsdiensten 2017 (Kamerstukken II, 2024/25, 34 588, nr. 94) en Regeerakkoord 2026-2030: pp. 15-16.

9 Zie onder meer: Toetsingscommissie Inzet Bevoegdheden. *Jaarverslag TIB 2025*. Den Haag: pp. 3, 21; Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten. *Jaarverslag 2025*. Den Haag: pp. 32-33; Bits of Freedom. *Geheime diensten* (dossier): <https://www.bitsoffreedom.nl/dossiers/geheime-diensten/>.

10 Regeerakkoord 2026-2030, p. 15.

11 Neurotechnologie, Rathenau Instituut, 2025.

daarvan voor de balans tussen veiligheid en grondrechten.¹² De huidige Wiv 2017 kent geen verzwaarde waarborgen voor intieme datatypen en krachtiger analysetechnieken. Sterker nog, in de Tijdelijke wet¹³ (die als blauwdruk geldt voor de nieuwe Wiv¹⁴) vervalt de toets door de Toetsingscommissie Inzet Bevoegdheden (TIB) op het toepassen van geautomatiseerde analyse van een bepaald type bulkdata¹⁵. Daarnaast zijn verschillende limieten op de bewaartermijnen van bulkdata in de Tijdelijke wet versoepeld. Het is daarom belangrijk om in de nieuwe Wiv oog te houden voor de toegenomen capaciteiten van de diensten die de potentiële inbreuk op de privésfeer vergroten. De toelaatbaarheid van nieuwe databronnen en geavanceerde analysetechnieken vraagt om betere juridische waarborgen.

2. Zorg voor *checks & balances* bij vereenvoudiging en toetsing

In één adem met de roep om meer slagkracht noemen de diensten het verminderen van ‘administratieve lasten’¹⁶ en het ‘vereenvoudigen’ van procedures¹⁷. Dat kan in praktijk neerkomen op aanpassingen in het stelsel van toetsing en toezicht. De Tijdelijke wet lijkt hierop voor te sorteren. Daarin is de rol van de TIB op onderdelen afgeschaald en deels overgeheveld naar de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).¹⁸ Het idee is dat de TIB voorwaarden en aandachtspunten kan meegeven aan de CTIVD en zo meer onderzoeken doorgang kunnen vinden.¹⁹ Twee kanttekeningen zijn hierbij op z’n plaats.

- Ten eerste is de verschuiving van toetsing *vooraf* (door de TIB) naar toezicht *tijdens* of *achteraf* (door de CTIVD) geen wondermiddel. Bij signalering van onrechtmatigheden in het handelen van de diensten is het kwaad immers al geschied: de inbreuk op grondrechten van de betrokken burgers is dan al een feit. Toezicht *tijdens* en *achteraf* kan ook meer werk zijn dan toetsing *vooraf*. In plaats van een goed omschreven verzoek *vooraf* te moeten beoordelen, moet de toezichthouder zelf op zoek naar onrechtmatigheden. Deze facetten dienen bij een eventuele wijziging van het toezichtstelsel te worden meegewogen.
- Ten tweede kan toetsing en toezicht in een democratische rechtsstaat niet worden afgedaan als louter administratieve last.²⁰ Deze *checks and balances* onderscheiden onze diensten van totalitaire regimes. Bovendien hoeft het realiseren van meer wendbaarheid voor de diensten niet te botsen met het afleggen van verantwoording. Er zijn mogelijkheden om toestemmings- en toetsingsprocedures te versnellen. Zo was volgens de TIB bij tot nu toe geweigerde verzoeken vaak sprake van vermijdbare

12 Signalen voor de Toekomst, Rathenau Instituut, 2025.

13 Voluit: Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen.

14 Kamerstukken II 2022-2023, 34 588, nr. 92 (Hoofdlinjennotitie herziening Wiv 2017), 2023.

15 Het gaat om metadata uit onderzoekso opdrachtgerichte interceptie ten aanzien van het identificeren van personen of organisaties. Zie Tijdelijke wet, art. 8.

16 Zie: Brief over de hoofdlijnen van het geheime jaarplan van de AIVD 2026 (Kamerstukken II, 2025/26, 30 977, nr. 176), p. 8; Algemene Rekenkamer (2021), *Slagkracht AIVD en MIVD*, p. 10.

17 <https://www.volkskrant.nl/binnenland/nederlandse-diensten-delen-minder-informatie-met-de-vs-soms-vertellen-wedingen-niet-meer~b4882f19/>

18 Dit geldt voor verkennende hackoperaties en de toepassing van geautomatiseerde data-analyse op metadata uit OOG-interceptie gericht op het identificeren van personen of organisaties.

19 Toetsingscommissie Inzet Bevoegdheden. *Jaarverslag TIB 2025*. Den Haag: p. 17. Ook het Regeerakkoord 2026-2030 (p. 15) oppert het samenvoegen van de toezichthouders.

20 Oerlemans, J., & Harleman, S. (2024). *Factsheet. Voorgenomen wijzigingen in de wet op de inlichtingen- en veiligheidsdiensten 2017*. Parlement en Wetenschap: p. 4.

‘slordigheden’²¹. Ook bieden de al bestaande ‘snelle toets’ en de ‘spoedprocedure’ van de TIB aanknopingspunten.²²

3. Reflecteer op de reikwijdte van de taakstelling van de diensten

De nieuwe dreigingen waarmee Nederland zich geconfronteerd ziet zijn diffuus van aard.²³ Dat roept vragen op over wat überhaupt geldt als ‘dreiging voor de nationale veiligheid en de democratische rechtsorde’ – een kwalificatie die aandacht van de AIVD legitimeert.²⁴ Voor dreigingen vanuit vijandelijke staten en terroristische netwerken is de legitimiteit van AIVD-bemoeienis evident. Voor nieuwe vormen van extremisme, bijvoorbeeld uit de anti-institutionele hoek of voortkomend uit internet-niches, is dat minder duidelijk. De AIVD beschouwt extremisme als ‘het uit ideologische motieven bereid zijn om [...] activiteiten te verrichten die de democratische rechtsorde ondermijnen’.²⁵ Maar bij nieuwe vormen van extremisme is ideologie vaak niet leidend.²⁶ Bovendien kan het geweld dat uit dit type extremisme voortkomt een zonderling karakter hebben.²⁷ Dat maakt het twijfelachtig of het een dreiging voor de nationale veiligheid en democratische rechtsorde betreft.

Aandacht van de diensten voor dit type extremisme zou een oprekking van de taakstelling van de diensten vergen, waarbij ideologie in mindere mate als onderscheidend element zou gelden en/of geweld eerder als dreiging voor de nationale veiligheid en rechtsorde geldt. Een dergelijke oprekking is niet zonder risico’s.

- Een eerste risico is dat ook vormen van legitiem maatschappelijk activisme binnen het aandachtsgebied van de diensten zouden komen te liggen – met een feitelijke inperking van burgerlijke vrijheden en democratische rechten tot gevolg.
- Een tweede risico is dat bij een dergelijke oprekking ook vormen van crimineel geweld binnen het aandachtsgebied van de diensten kunnen komen, waar dit voorheen een zaak van de politie was. Daardoor kan sfeervermenging tussen de terreinen van nationale veiligheid en van opsporing ontstaan.²⁸ Het is dus de vraag of een dergelijke oprekking wenselijk is. Het is zaak om politiek en maatschappelijk debat te voeren over reikwijdte van de taakstelling van de diensten. Uiteindelijk komt dit neer op de vraag welke mate van onveiligheid we als samenleving accepteren om adequate waarborging van grondrechten in een open en democratische samenleving te kunnen garanderen.

21 Toetsingscommissie Inzet Bevoegdheden. *Jaarverslag TIB 2025*. Den Haag: p. 7.

22 Zie: Toetsingscommissie Inzet Bevoegdheden (14 april 2022). ‘Reactie op het concept wetsvoorstel Tijdelijke wet onderzoek AIVD en MIVD naar landen met een offensief cyberprogramma’: p. 4. Ook tijdens het rondetafelgesprek over de Tijdelijke wet van 5 april 2023 werden deze bestaande versnellingsopties aangehaald. Zie: https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2023A01504.

23 In het jaarplan van de AIVD voor 2026 staan onder meer dreigingen genoemd voortkomend uit ‘aanhoudende conflicten en geopolitieke spanningen’ evenals terrorisme, extremisme, cyberdreiging, spionage en beïnvloeding. Zie: Brief over de hoofdlijnen van het geheime jaarplan van de AIVD 2026 (Kamerstukken II, 2025/26, 30 977, nr. 176), pp. 1-2.

24 Art. 8 Wet op de inlichtingen- en veiligheidsdiensten 2017.

25 Zie: <https://www.aivd.nl/onderwerpen/aandachtsgebieden/extremisme>.

26 Onderzoek laat zien dat de voedingsbodem van nieuwe soorten extremisme uit de rechts-extremistische en anti-institutionele hoek een mengelmoes is van eclectische denkbbeelden en persoonlijke problematiek. Zie: Van Buuren, J. (2022). Complotdenken en extremisme. Complotnarratieven in de context van coronaprotesten. *Tijdschrift over Cultuur & Criminaliteit*, 12(2), 53-71.

27 Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Martenson, C., & Svenson, P. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Security Informatics*, 2(11).

28 Toezichthouders TIB en CTIVD uitten eind 2024 in een brief aan de minister van Binnenlandse Zaken en Koninkrijksrelaties hun zorgen over een dergelijke sfeervermenging tussen de terreinen van nationale veiligheid en van opsporing. Zie: <https://www.tib-ivd.nl/documenten/2025/03/14/gezamenlijke-brief-ctivd-tib-mbt-criminele-ondermijning>.

4. Een veilige samenleving vergt een veelomvattende aanpak

Het veilig houden van onze samenleving vergt meer dan de inzet van de inlichtingen- en veiligheidsdiensten. Als een extremist in beeld komt bij de AIVD, is radicalisering immers al een voldongen feit. Het is zaak om eerder in de ‘radicaliseringsketen’ in te grijpen. Dat begint bij preventieve actie die ingrijpt op de oorzaken van radicalisering. Denk aan psychische problematiek²⁹, gebrek aan (economisch) perspectief, een verzwakt sociaal weefsel³⁰ en de toegang tot extremistische content en dito online communities³¹.

Voor een veilige online samenleving biedt het regeerakkoord aanknopingspunten, waaronder het bestrijden van desinformatie, het tegengaan van online beïnvloeding, het verbieden van verslavende en polariserende algoritmes en het optuigen van een ‘gecoördineerde’ preventieve aanpak van radicaliserende jongeren.³²

Deze plannen zijn nog weinig concreet. Het is belangrijk om deze uit te werken én te verbinden aan bredere maatschappelijke tendensen – zoals de knelpunten in de ggz, het ontbreken van bestaanszekerheid voor bepaalde groepen, en toenemende individualisering en eenzaamheid. Kortom, het is zaak om ook te investeren in de samenleving.³³ Een veilige samenleving waarin het prettig leven is, vergt de gezamenlijke inzet van de diensten, politie, ggz, welzijnsorganisaties, verschillende departementen en Kamercommissies en – uiteindelijk – van ons allemaal.

Gerelateerde publicaties

- Rathenau Instituut (2025). *Signalen voor de toekomst. Hoe digitale ontwikkelingen menselijke interactie veranderen en wat dit betekent voor I&V-diensten*. Den Haag. <https://www.rathenau.nl/nl/digitalisering/naar-een-menswaardige-digitale-technologie/signalen-voor-de-toekomst>

29 Raad Volksgezondheid & Samenleving (2025). *Op de rem! Voorbij de hypernerveuze samenleving*. Den Haag: RVS.

30 Sociaal en Cultureel Planbureau (2025). *Digitaal vervlochten, maar ook verbonden? De toekomst van sociale cohesie in het licht van digitalisering, ongelijkheden en individualisering*. Den Haag: SCP.

31 The Hague Centre for Strategic Studies. *Van meme tot moord. Hoe online extremistische broedkamers een nieuwe generatie van geweld kweken*. Den Haag: HCSS.

32 Regeerakkoord 2026-2030, pp. 16, 59.

33 Rathenau Instituut (2026) Hoeveel pixels is een knuffel. Dialogen over de toekomst van digitalisering en sociale relaties. Den Haag.