

Geheime diensten krijgen misschien meer bevoegdheden. Wat is het risico? ‘Ik vrees dat je de rode loper uitrolt voor autocraten’

Famke Seine

Nederland moet zich beter kunnen weren tegen onder meer de Russische en Chinese dreiging, vindt het kabinet. Met een wetsvoorstel wil het daarom de bevoegdheden van de inlichtingendiensten flink verruimen. Door de regering aangewezen ‘opponenten’, naast Rusland en China bijvoorbeeld ook Iran, zouden zo sneller en makkelijker onderzocht kunnen worden door de geheime diensten.

Nu verplicht de wetgeving dat ieder af luisterverzoek of hack vooraf wordt getoetst door de toezichthouder, de Toetsingscommissie Inzet Bevoegdheden (TIB). Het wetsvoorstel beoogt die verplichting grotendeels te schrappen. De diensten zouden dan maximaal – zonder toetsing vooraf – een jaar lang zo’n aangewezen tegenstander mogen tappen, volgen en hacken.

Het is een grote verbouwing van de wet

Minister Dilan Yesilgöz (Defensie, VVD) noemt de wet „keihard nodig om Nederland en onze bondgenoten te kunnen blijven beschermen”. Zo stelde ze in de verklaring bij het wetsvoorstel, dat vorige week vrijdag door de ministerraad ging. Russen die gevoelige politiegegevens proberen te verkrijgen en Chinese hackers die „op listige wijze” technologieën willen stelen, worden als voorbeelden genoemd waartegen Nederland zich beter moet wapenen. „Met deze wet wordt ons mes scherper”, aldus Yesilgöz.

Van wie de inlichtingendiensten data mogen verzamelen, is deels geregeld in de Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Al gauw nadat die wet was ingegaan in 2017, kwamen de beperkingen bovendien. Onder meer de Algemene Rekenkamer stelde dat de Wiv voor moeilijkheden zorgde. Zo bleek die verouderd, terwijl de internationale situatie in rap tempo veranderde – met de Russische inval van Oekraïne in 2022 en een China dat steeds meer technologische kennis uit Nederland wil verkrijgen.

Rusland onderneemt ook cyberaanvallen op Europese infrastructuur – soms met [succes](#). En de diensten waren té beperkt door de Wiv om daartegen snel op te treden. Aldus wensten die een nieuwe wet, die nu ter internetconsultatie ligt, zodat organisaties en burgers hun mening over het voorstel kunnen geven. Pas later in het wetsproces, nadat de internetconsultatie is gesloten en de Raad van State – het adviesorgaan van de regering – zich hierover heeft gebogen, volgt een uitgebreid Kamerdebat over de wet.

[Lees ook](#)

[AIVD en MIVD verzamelden in 2024 meer geheime informatie dan de jaren daarvoor](#)



‘Vergroot risico op politisering’

„Het is een grote verbouwing van de wet”, stelt Bart Jacobs, hoogleraar computer security aan de Radboud Universiteit over het voorstel. Hij maakte deel uit van de evaluatiecommissie van de Wiv en van

de kenniskring van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Op een aantal punten beschouwt Jacobs het als een verbetering. Dat in het geval van een aangewezen ‘opponent’ niet iedere keer opnieuw om toestemming hoeft te worden gevraagd bij de toezichthouder, scheelt „veel bureaucratische rompslomp”.

Toch kan het grijs gebied worden wie als ‘opponent’ wordt aangemerkt. „Je denkt al gauw aan buitenlandse inlichtingendiensten, zoals die van Iran en Rusland, maar instellingen voor culturele uitwisseling? Daar wordt het al ingewikkelder.” Daarom is het volgens Jacobs belangrijk dat de toezichthouder stevig toetst op die bepaling.

Hoe meer toetsing je aan de voorkant hebt, hoe minder snel je kunt handelen, dat is de redenering vanuit de diensten

Eén onderdeel deed Jacobs vooral zijn wenkbrauwen fronsen: de toevoeging van het staatsnoodrecht. „Waar ik bang voor ben, is dat je met dit soort bepalingen de rode loper uitlegt voor autocraten.”

Wanneer het kabinet bepaalt dat het staatsnoodrecht moet gelden voor de diensten, hoeft het hacken, tappen en onderzoeken van personen en organisaties niet meer getoetst te worden bij de toezichthouder. „De toezichthouder wordt buitenspel gezet”, aldus Jacobs. „Hiermee vergroot men het risico dat diensten gepolitiseerd worden en zich bijvoorbeeld op politieke tegenstanders van de eigen minister moeten richten.”

Jacobs verwijst naar landen als Polen en Hongarije waar al meerdere schandalen naar boven zijn gekomen waarbij mogelijk telefoons zijn gehackt van oppositieleiden uit het parlement. „Dit zal niet van de een op andere dag gebeuren, maar het is wel een kwetsbaarheid die je toelaat”.

‘Zorgvuldig worden ingebed’

In een debat over de geheime diensten afgelopen donderdag vroeg onder meer Kamerlid Joost Sneller (D66) zich af welke risico’s kleven aan de nieuwe wet. Evenals Jacobs verwees hij naar Polen en Hongarije. „Volgens mij moeten we hierin voorzichtig zijn”, zei Sneller. Ook Pro-Kamerlid Barbara Kathmann had haar vraagtekens bij onder meer het toevoegen van het staatsnoodrecht. „Het moet niet snel ingezet kunnen worden en daarom zorgvuldig worden ingebed. Het lijkt erop dat dat nu nog niet het geval is.”

Jan-Jaap Oerlemans, onderzoeker aan de Universiteit Leiden en tot 2024 onderzoeker bij de CTIVD, noemt het wetsvoorstel duidelijk een „product van zijn tijd”. „In de toelichting worden meermaals termen als ‘grijze zone’ en ‘hybride dreigingen’ gebruikt.” Daar heeft de onderzoeker begrip voor, want „het dreigingslandschap is immers veranderd”.

Evenals Jacobs ziet Oerlemans dat de effectiviteit van de diensten flink kan worden verbeterd door het wetsvoorstel: „Hoe meer toetsing je aan de voorkant hebt, hoe minder snel je kunt handelen, en soms heb je die tijd niet, dat is de redenering vanuit de diensten.” Daar heeft de onderzoeker ook begrip voor, maar: „Het gaat wel om de bescherming van fundamentele rechten. *The devil is in the details* met dit soort wetgeving, dus een uitgebreid debat hierover is op zijn plaats.”

[Lees ook](#)

[NCTV zeer bezorgd over nihilistisch extremisme en gewelddadige extremisten die menen dat ‘een kwaadaardige elite burgers onderdrukt’](#)