



De nieuwe AIVD/MIVD wet: een eerste overzicht

📅 Sep 03 2026

In mijn vorige artikel schreef ik hoeveel de AIVD en MIVD nu al mogen. Inmiddels is het nieuwe wetsvoorstel gepubliceerd, en wat blijkt, men wil nog veel meer bevoegdheden, met veel minder toezicht.

Ik heb veel vragen gekregen wat nou het ergste is aan de nieuwe wet, maar het is in z'n geheel een totale uitholling van de rechtsstaat door een dienst die losgezongen is van de maatschappij en zelden of nooit naar zichzelf kijkt als de resultaten tegenvallen. En het is wel belangrijk allemaal. Een veilige democratie heeft een bepaalde hoeveelheid geheime dienst nodig. Te weinig en je loopt risico's dingen te missen. Maar bij teveel datavergaring loopt je (toekomstige) democratie op andere manieren gevaar. En dit blijft zo zelfs als men het beste toezicht belooft.

We willen de beste geheime diensten. En niet alleen de diensten met de ruimste bevoegdheden en het soepelste toezicht, ook al is de wereld eng en bedreigend.

Maar, over de wet. Ik zit al jaren in hoe het Europees mensenrechtenhof kijkt naar inlichtingen- en veiligheidsdiensten, en deze wet komt niet eens in de buurt van wat ze daar OK vinden in termen van toezicht en toetsing. En het is een schande dat men het zelfs maar probeert.

Het heeft geen zin om de wet artikel voor artikel te bestrijden. Want het is niet zo dat als je een paar artikelen aanpast dat het dan ineens wel door de beugel kan.

Desondanks is het belangrijk om te snappen hoe bezopen het allemaal is, dus hier een bloemlezing. Ik houd een kleine slag om de arm, want de wet plus toelichtingen zijn meer dan 400 pagina's, wat op zich al een probleem is. Als je zo'n lang verhaal moet houden om het uit te leggen is dat een slecht teken. Maar, dit is de eerste analyse. Als er iets niet klopt, mail me direct op bert@hubertnet.nl en dan kijk ik wat aanpassing behoeft. Want goeie kans dat de wet nog niet goed begrepen is.

Check vooral deze pagina over een paar dagen nog een keer, dan zijn er vermoedelijk uitbreidingen en correcties.

Inhoudsopgave:

- Hacken zonder te hacken
- Er komt helemaal geen “extra toezicht”
- Toestemming zonder toestemming te vragen
- Alles met AI
- Bulkinterceptie
- Bulkdatasets
- Doorkomen met die data!
- Staatsnoodrecht
- Het “net geen moord” artikel 97
- Samenwerking en samen hacken met het bedrijfsleven
- Afluisteren, hacken, ter taakondersteuning

Hacken zonder te hacken

Dit gaat een beetje een thema worden, maar de diensten spelen met woorden. Als de AIVD jouw telefoon of computer hackt, dan voel je je toch wel gehacked. Een spion in je apparaat. Maar, de AIVD heeft met een taaltrucje gezegd dat ze in je telefoon of server of kabelmodem mogen inbreken (artikel 76), en ze mogen er zelfs software op installeren (artikel 77), en **dan ben je volgens hun nog niet gehacked**, en hoeft er ook niet veel toestemming gevraagd te worden.

De toestemming is pas nodig als ze de data uit je apparaten ook daadwerkelijk gaan gebruiken in het inlichtingenproces (artikel 78). Nou heeft het Europees mensenrechtenhof weleens over vergelijkbare zaken geoordeeld dat zelfs al alleen het hebben van data leidt tot een inbreuk op de persoonlijke levenssfeer, en dus schadelijk is. Ook al doe je er nog niks mee.

Het zonder veel toestemming binnendringen in allemaal computers en daar hacktools neerpoten maakt een gatenkaas van onze netwerken, en kan leiden tot vervolgschade. Want als je een toegangsdeur op jouw telefoon monteert (artikel 77), dan is er altijd het risico dat ook iemand anders door die door gaat.

In het verleden moest men bij hacken expliciet rekening houden met technische risico's, wat zou er mis kunnen gaan. Kunnen er gegevens uitlekken, kunnen er dingen kapot gaan waar de maatschappij op draait. Maar, dit hoeft allemaal niet meer in de nieuwe wet, “want men neemt die afweging natuurlijk vanzelf mee”.

Dit is spannend in combinatie met de behoefte van de diensten om te kunnen “positioneren” (pagina 56 van de MvT). Het idee daarbij is om “alvast” dingen te hacken, in de hoop dat de infrastructuur waar men dan in zit, later gebruikt gaat worden door foute organisaties of mensen. “Dat betekent dat de diensten kijken naar mogelijkheden om posities in te nemen met als oogmerk dat daar in de toekomst waardevolle inlichtingen kunnen worden verzameld”.

Waar mag men dan allemaal positioneren? Nou, overal: “Dergelijke inzetten kunnen ook gericht zijn op non-targets”. Dus men mag mensen en servers hacken van mensen die zelf helemaal niet in aandacht staan. Men wil dan dus infrastructuur, gebruikt door de hele wereld, alvast hacken om later dingen mogelijk te maken.

Het is bezopen dat men op deze manier ‘hacken’ opsplitst in drie handelingen waarvoor alleen serieus toestemming gevraagd hoeft te worden voor de derde manier. Dit getuigt van hoe de diensten losgezongen zijn van de samenleving - wij bepalen wel of je “gehacked” bent. En de behoefte om de wereld “alvast” te hacken is ronduit eng. Zo verzwakken we de beveiliging van belangrijke infrastructuur, en maken we zo een gatenkaas van het internet.

De diensten zien dit niet zo, en in de nieuwe wet hoeft er geen externe toestemming gevraagd te worden voor dit soort “positioneren”, en dat is doodeng.

Er komt helemaal geen “extra toezicht”

Je moet erop kunnen vertrouwen dat je geheime diensten de kluit niet belazeren. Deze wet begint in dat opzicht slecht. Men kondigde aan:

Nieuwe set aan waarborgen

*De diensten in staat stellen sneller en beter te handelen, gaat hand in hand met het beschermen van de rechtsstaat en burgerrechten. Daarom horen bij een nieuwe wet ook **nieuwe waarborgen**. Bijvoorbeeld voor het gebruik van bulkgegevens en de inzet van nieuwe technologieën zoals **AI**.*

*Er komt een **nieuw onafhankelijk college** dat toeziet op de rechtmatige inzet van bevoegdheden door de diensten: het College van Toetsing en Toezicht (CTT). Dit college kan onderzoeken stopzetten bij onrechtmatigheden.*

De werkelijkheid is dat er **helemaal geen nieuw toezicht** komt, of extra waarborgen. De huidige twee toezicht/toetsingscommissies worden samengevoegd, verliezen 30% van hun leden, en mogen op heel veel dingen

geen toezicht meer houden. Ook zijn juist de regels over AI verwijderd. Ow. Dat klinkt toch heel anders dan 'Nieuwe set aan waarborgen'.

Het is echt jammer dat het eerste document wat we lazen over de wet de kluit gelijk belazert.

Ook mag de toetsingscommissie na deze nieuwe wet geen rekening meer houden met het verleden. Ieder verzoek om toestemming, moet geheel 'op zich' behandeld worden. Het oordeel mag alleen geveld worden op basis van wat de diensten *nu* op papier aanleveren. Als de toezichthouder bekend is met eerdere problemen met de rechtmatigheid, dan mag die kennis niet gebruikt worden.

Een absolute giller is ook artikel 188 lid 5, waarin we lezen dat het 'CTT' wel operaties stop mag zetten, maar niet als het een belangrijke operatie was.

Onbegrijpelijk is ook dat men eist dat individuele leden van de CTT in hun eentje dingen mogen beoordelen (artikel 50). Dit maakt die individuele leden erg kwetsbaar voor druk.

Verder is het ook zo dat het CTT sowieso niet zo vaak meer toestemming hoeft te verlenen, zoals te lezen in het volgende stuk.

Toestemming zonder toestemming te vragen

De diensten moeten nu per inzet vragen wat ze mogen doen qua hacken, volgen, af luisteren, etc. In de nieuwe wet mag men een hele organisatie aanwijzen als 'evidente opponent', en nadat dat gebeurd is kan iedereen die voor zo'n opponent werkt, of er actief voor is, **zonder verdere procedure aangepakt worden**. Dit klinkt op zich wel logisch, het zijn engerds daar bij de FSB in Rusland, maar het is toch wel spannend om hele organisaties zo vogelvrij te verklaren.

In de wet zit in artikel 55 al een forse opsomming van lijsten van clubs die evidente opposanten zijn, als bepaald door de Europese Unie. Dit is overigens wel heel veel vertrouwen in de EU instellingen.

Waar dit spannend wordt is dat natuurlijk onduidelijk is wie er allemaal 'lid' zijn van ISIS. Het lijkt erop dat de diensten geheel zelfstandig mensen kunnen koppelen aan organisaties. Gezien de enorme hoeveelheid organisaties die aangewezen is als 'evidente opponent' is het wel belangrijk om te weten wie er vervolgens allemaal zonder verdere toestemming onderzocht mag worden.

Op pagina 54 van de memorie van toelichting vinden we overigens dat ook ‘hackerverbanden’ evidente opposenten kunnen zijn. Hier lezen we ook hoe breed men denkt individuen te koppelen aan dit soort organisaties. Zo kan je al geacht worden bij een hackerverband te horen als je een techniek toepast waarvan bekend is dat Noord Koreaanse hackers die ook gebruiken.

Cruciaal is dat alleen achteraf onderzocht kan worden of iemand terecht is afgeluisterd omdat hij lid zou zijn van ISIS.

Het ligt voor de hand dat de diensten via deze route veel bevoegdheden in zullen zetten tegen deze gekende opposenten, maar waarbij lastig is te controleren of de getroffen partijen wel echt deel uitmaakten van die omgevingen.

Ook kunnen er algemene bevoegdheden ingezet worden tegen dit soort organisaties, waaronder AI-zoekopdrachten in bestanden die zo gevoelig zijn dat ze niet door mensen ingezien mogen worden (!).

Alles met AI

In artikel 32 staat het volgende zinnetje:

- 1. De diensten zijn bevoegd de uitvoering van deze wet en de Wet veiligheidsonderzoeken te automatiseren*

Ok dan. In de Memorie van Toelichting lezen we op pagina 40 wat deze automatisering is:

“Het begrip omvat zowel reguliere kantoorautomatisering, als ook bijvoorbeeld algoritmes, AI en quantumtechnologie.”

En wat mag er dan met die AI?

“Het [gaat] om toepassingen die gericht zijn op het identificeren van nieuwe en ongekende personen en organisaties die in aanmerking komen voor onderzoek door de diensten.” (pagina 43). Ow.

Er staan wel woorden dat dit heel voorzichtig moet gebeuren, en dat je niet op basis van alleen de AI maatregelen mag nemen tegen personen. Maar in de praktijk blijken mensen de computer toch best snel te gaan geloven, en men mag dus met AI op hun enorme bulkdatasets (zie onder) losgaan om nieuwe *targets* te identificeren.

Ik vind dit persoonlijk doodeng, hoe vaak je ook opschrijft dat je heel kritisch gaat zijn. In de bestaande wetgeving (Wiv 2017) staat dat er gedetailleerde plannen en toetsen ontwikkeld moeten worden voordat men AI (“GDA”) mag gebruiken. Dat alles is nu weg.

Specifiek eng is dat men meegaat in het moderne frame dat de AI een soort onafhankelijke entiteit is, die je dingen kan laten doen die mensen niet mogen doen. “Want het was de AI die het deed, wij waren het niet”. Verderop meer over dit probleem.

Bulkinterceptie

Zoals de diensten je kunnen hacken zonder dat hacken te noemen, zo kan men ook hele datakabels aftappen, opnemen, analyseren, bestuderen, zonder dat men het afluisteren noemt.

Internet en overige data komt dan wel op de harde schijf van de AIVD/MIVD, maar mag nog niet gebruikt worden in het inlichtingenproces. Hiervoor is weinig toestemming nodig, maar het mag wel een jaar lang gedaan worden.

Een stapje verder is het “verkennen” (artikel 81) van die data, waar wel externe toestemming voor nodig is, maar het lijkt erop dat die toestemming nooit geweigerd kan worden.

En de derde stap is dan daadwerkelijk de inhoud van een getapte kabel beschikbaar maken als “Speciale bulkdataset” (artikel 82), waar met AI of door mensen in gezocht kan worden. Hier moet extern toestemming voor gevraagd worden, maar het is lastig te bepalen of die ooit geweigerd kan worden. De diensten hoeven maar heel globaal aan te geven welke data ze willen hebben of waarom.

Bulkdatasets

De diensten mogen op allemanieren ‘bulkdata’ verzamelen, bijvoorbeeld door geëkte datasets van locatiegegevens in te kopen op dark markets. Ook de bulkinterceptie leidt tot dit soort “bijzondere bulkdata”. Dit gaat om onvoorstelbare hoeveelheden gegevens die ook internationaal uitgewisseld worden tussen diensten.

De vraag is vervolgens wat je met die datasets mag doen. De theorie is dat “de bak” met bijzondere bulkdata in principe dicht zit, en alleen een speciale afdeling hier vrij in mag zoeken om te kijken of er wat in zit (artikel 83). Ze mogen op

zoek naar nieuwe mensen en organisaties die aandacht behoeven in het kader van lopende onderzoeken. Dit gebeurt niet door de dienst in het algemeen, maar door speciaal aangewezen ambtenaren. Maar onduidelijk is hoeveel mensen er aangewezen worden.

In het verlengde hiervan mag men met artikel 84 de hele bulkdataset “bevragen”, en wat er daarmee gevonden wordt kan daarna door alle teams gebruikt worden voor het inlichtingenwerk.

Dit “bevragen” mag dus ook met AI. Voor het bevragen is op zich externe toestemming nodig, behalve als de bevraging te maken heeft met een van de aangewezen gevaarlijke organisaties uit artikel 55. En dan is het vrij spel, en dit zal meestal het geval zijn.

De AI mag dan op basis van al die afgetapte informatie en alle verzamelde bulkdatasets op zoek naar enge dingen of mensen die nader onderzoek behoeven.

We waren in 2017 boos over de “sleepwet”. En nu hebben we een wet waarmee de AI mag gaan zoeken naar rare dingen. De gedachte hierbij is dat de AI geen mens is, en dus vrij mag zoeken in de data, want er wordt dan nog geen “kennis genomen” van de informatie.

Hoe knapper de AI wordt hoe enger het idee is dat de computer vrij mag zoeken naar rare dingen, en daarmee meer mag dan mensen die voor de diensten werken!

Doorkomen met die data

In artikel 94 krijgen de diensten de algemene bevoegdheid om, als het echt moet, informatie op te eisen bij *iedereen*. En de data moeten ook direct geleverd worden, anders volgt een gevangenisstraf van zes tot 24 maanden.

Onduidelijk is wat je zou moeten doen als de AIVD mensen data komen opeisen die jij echt niet wil geven. Kan je dan in beroep? Is het bestuursrecht? Kan er een voorlopige voorziening getroffen worden bij een rechtbank? Het lijkt van niet. Nu leveren graag.

Essentieel hierbij is dat je data bij een rechtsgang later wel ‘teruggegeven’ kan worden, maar tegen die tijd heeft men er al kennis van genomen. Een rechter kan achteraf de kennisname niet ongedaan maken, eens gelezen blijft gelezen. Het is knap onduidelijk hoe dit moet werken.

Men omschrijft in de MvT dat ze dit artikel alleen inzetten als het echt moet, maar ze zeggen ook (op pagina 100) dat artikel 94 er ook is ‘voor situaties waarin een kwaadwillende actor voorbereidingshandelingen treft zonder direct tot maatschappelijke ontwrichting, spionage of sabotage over te gaan’. Dat lijkt al best snel eigenlijk.

Staatsnoodrecht

Nou als er een crisis is hoeft de wet niet echt meer (artikelen 224-229). In andere landen (VS, Frankrijk) zijn al decennia geleden crises uitgeroepen die nog steeds actief zijn. Het is daarom raadzaam aan te nemen dat we hier ooit ook wel in een crisis komen, en dat deze dan de nieuwe situatie is.

Onder “bijzondere omstandigheden” kunnen de ministers zelf nieuwe toezichthouders aanwijzen. Het is ook niet meer nodig de toetsingscommissie nog toestemming te vragen voor dingen die te maken hebben met de crisis, dat hoeft dan ook niet meer (artikel 226).

Ook hoeft er geen jaarverslag meer te komen.

De Tweede Kamer kan een einde maken aan een verklaarde crisissituatie, maar de vraag is of ze dat zullen doen.

Het “net geen moord” artikel 97

Ik kan het echt niet anders zeggen. Al decennia hebben de AIVD en MIVD een heel raar artikel in hun wet waarmee ze “maatregelen” kunnen nemen ter bevordering van de nationale veiligheid. En al tientallen jaren wil men niet zeggen wat die maatregelen allemaal kunnen zijn, behalve dat er niemand mee vermoord kan worden. Je zou denken dat ik dit verzon, maar ze zeiden het echt.

Al heel lang is er de behoefte om dit eens duidelijk te krijgen. Ook het Openbaar Ministerie had ooit een mening over dat de dienst van de wet strafbare feiten mag plegen, en die wilden ook al heel lang dat daar een beter systeem voor komt.

Vreemd is ook dat dit artikel geen enkele vorm van externe toestemming nodig heeft, en de bevoegdheid kan zelfs omlaag gemandateerd worden naar een teamhoofd (!). In de nieuwe wet is er niets wezenlijk aangepast over dit curieuze artikel:

| *Artikel 97. De diensten zijn bevoegd tot het bevorderen of treffen van maatregelen*

voor de bescherming van door de desbetreffende dienst te behartigen belangen. (...) [Daarbij] kan de medewerker ook worden belast met het verrichten van handelingen die het plegen of medeplegen van een strafbaar feit tot gevolg kunnen hebben, of de medewerking daaraan.

Een gemiste kans, want dit is een gapend gat in de wet.

Samenwerking en samen hacken met het bedrijfsleven

In artikel 145 lezen we over “Publiek-private samenwerking multilateraal”:

*2. De samenwerking kan bestaan uit: a. de uitwisseling van gegevens; b. gezamenlijke analyse van gegevens; c. **wederzijdse technische of operationele ondersteuning.***

Dit maakt heel erg veel mogelijk. De Memorie van Toelichting verschaft (op pagina 303) niet veel duidelijkheid wat dit inhoudt allemaal. Dat kan dus vanalles zijn. Bedrijven als Palantir leveren graag mensen ter ondersteuning, en doen dat al bij de Nederlandse politie. Mogelijk heeft men dit in gedachten.

Ook zou je kunnen denken aan bedrijven als Fox-IT, Eye Security en Hunt & Hackett, die best mee zouden willen doen bij operaties gok ik. Verder kan je je ook veel voorstellen bij dat de diensten relevante bedrijven bijstaan in hun cybersecurity.

Het is voorstelbaar dat het nuttig kan zijn de samenwerking met het bedrijfsleven (en onderzoeksinstellingen) te intensiveren. Maar het is wel een traject wat meer beschrijving vergt dan de paar paragrafen in de MvT die we nu hebben. De minister van Binnenlandse Zaken heeft op 3 september in de Tweede Kamer toegezegd dat er ook meer informatie over gaat komen.

En dat is goed, want private bedrijven deel maken van je inlichtingendiensten is toch wel wat.

Afluisteren, hacken, ter taakondersteuning

Dat Piet de Terrorist afgeluisterd mag worden snappen we wel. Maar, men mag ook hacken en tappen om andere redenen (artikel 38):

Een bijzondere bevoegdheid kan, in afwijking van het eerste lid, ook worden uitgeoefend voor de ondersteuning van de taakuitvoering van de diensten, voor zover dat noodzakelijk is om: a. de uitoefening van operationele bevoegdheden

mogelijk te maken; b. capaciteiten die diensten nodig hebben voor de taakuitvoering te ontwikkelen en te onderhouden

Dit maakt het mogelijk om bijvoorbeeld een systeembeheerder bij een softwarebedrijf onder de tap te zetten, om zo met gekaapte SMS-codes toegang te krijgen tot dat softwarebedrijf. En om dan via dat softwarebedrijf weer toegang te krijgen tot daadwerkelijke targets.

Ook kan de broncode van de software dan achterhaald worden, om dan bijvoorbeeld naar zwaktes te zoeken waarmee weer verder gehacked kan worden.

Op deze manier kan er op grote afstand van daadwerkelijke targets inbreuk gemaakt worden, allemaal omdat dit bij kan dragen aan (toekomstige) inzet op daadwerkelijke targets.

Later meer

Er volgen vermoedelijk nog aanvullingen op deze pagina.

Ter context is het mogelijk nuttig het eerdere stuk te bekijken, met daarin wat meer beschouwing over hoe het nu staat met onze democratische rechtsorde.



← Previous

Nieuwe wet Inlichtingen- en veiligheidsdiensten: wat mogen ze nu al en waar zijn ze voor



© 2014-2026 bert hubert