

# Zo wil de AIVD ook jouw e-mails en appjes aftappen



15 april 2016 15:18

Het kabinet wil een nieuwe wet introduceren waarmee de geheime dienst AIVD de internetkabel op grote schaal mag aftappen, waaronder jouw e-mails en appjes. Wat staat er precies in dit wetsvoorstel?

De regering werkt al jaren aan een herziening van de Wet op de inlichtingen- en veiligheidsdiensten. Deze wet is vijftien jaar geleden gevormd en geeft de geheime diensten volgens minister Plasterk van Binnenlandse Zaken te weinig bevoegdheden. Een belangrijke vernieuwing in het wetsvoorstel is dat de AIVD en militaire variant MIVD [voortaan de internetkabel mogen aftappen](#).

## **Kabelgebonden en niet-kabelgebonden communicatie**

De huidige wet maakt een onderscheid tussen kabelgebonden en niet-kabelgebonden communicatie. Onder laatstgenoemde valt bijvoorbeeld het satelliettelefoonverkeer, dat de AIVD al op grote schaal mag aftappen.

Het kabelverkeer is verantwoordelijk voor het Nederlandse internetverkeer en mobiele communicatie, zoals telefoongesprekken. Als je vanaf je laptop een e-mail verzendt of met je telefoon een appje stuurt of iemand belt: het gaat allemaal via de kabel.

De AIVD mag al een gerichte tap op de kabel plaatsen, bijvoorbeeld wanneer ze een computer van een verdachte willen aftappen. Met het wetsvoorstel wordt het voor de geheime diensten mogelijk om het kabelverkeer op grote schaal af te tappen.

### **Gerichte interceptie**

Het op grote schaal aftappen van het kabelverkeer gaat via 'onderzoekopdrachtgerichte interceptie'. Dit betekent dat de geheime dienst bijvoorbeeld al het kabelverkeer uit een Amsterdamse wijk mag aftappen als zich daar mogelijk een terreurverdachte schuilhoudt. Of dat de AIVD alle communicatie van en naar Syrië onderschept om terroristische netwerken in kaart te brengen.

Deze vorm van data onderscheppen wordt ook wel een sleepnet genoemd. De geheime dienst onderschept bij een gerichte zoekactie allerlei data die via de kabel gaat, het zogeheten sleepnet, om vervolgens te kijken of er iets bruikbaar tussenzit. De geheime dienst richt zich dan aanvankelijk op metadata, bijvoorbeeld wie er met wie communiceert. Als daar iets opvalt kan er worden beslist om de data in te zien.



*Medewerkers van de AIVD aan het werk*

### **Onafhankelijke toezichthouder**

Bij het inzetten van zo'n sleepnet wordt ook informatie over onschuldige burgers buitgemaakt. Als je alle communicatie uit een wijk aftapt, dan zit daar ook veel metadata bij die niet van de verdachte afkomstig zijn. Als jij in dezelfde wijk als de verdachte woont, ziet de AIVD bijvoorbeeld naar wie je een e-mail

stuurt en met wie je belt. In het geval van WhatsApp bevindt de metadata zich op de server van WhatsApp. Daar kunnen geheime diensten toegang tot krijgen. Via de kabel ziet de AIVD wel wanneer je een WhatsApp'je verstuurt en hoeveel je de app gebruikt.

Metadata kunnen een gedetailleerd beeld geven van iemands leven. Het kabinet wil daarom dat er een onafhankelijke toezichthouder de aftapverzoeken van de geheime diensten gaat keuren. Deze toezichthouder, genaamd Toetsingscommissie Inzet Bevoegdheden (TIB), bestaat uit rechters en kan een tap- of hackverzoek blokkeren als de inbreuk op de privacy van burgers zwaarder weegt dan het bestrijden van terrorisme.

De AIVD benadrukt dat de geheime dienst niet opeens met jouw e-mails en WhatsApp-berichtjes mee gaat lezen. "We hebben niet eens de capaciteit om iedereen in de gaten te houden", aldus een medewerker. "We tappen nooit ongericht af. Er is altijd een belangrijke aanleiding om informatie af te tappen."

### **Advocaten en journalisten afluisteren**

In de huidige wet staat dat de geheime diensten telefoongesprekken mogen afluisteren, ook als er advocaten of journalisten aan deelnemen. Het gerechtshof in Den Haag [bepaalde eind vorig](#) jaar dat de geheime diensten geen telefoongesprekken mogen afluisteren waaraan een advocaat deelneemt.

Omdat de geheime diensten het belangrijk vinden om advocaten en journalisten af te tappen, introduceert de regering met het wetsvoorstel strengere voorwaarden voor het aftapproces. Zo moet de rechtbank Den Haag voortaan toestemming geven om een tap op een advocaat of journalist te plaatsen, ondanks de maatschappelijke bezwaren. Gesprekken tussen advocaten en cliënten zijn vertrouwelijk, en ook journalisten moeten veilig met bronnen kunnen communiceren.



*Het hoofdkantoor van de AIVD in Zoetermeer*

### **Hoe vaak gaat de AIVD tappen?**

Het blijft de vraag hoe regelmatig de geheime diensten zijn nieuwe tapbevoegdheid - als ze die krijgen - in gaan zetten. In tegenstelling tot sommige anderen landen, zoals België, Duitsland en het Verenigd Koninkrijk, weigert de regering openheid te geven over het aantal taps in Nederland.

Volgens Plasterk geven de tapstatistieken inzicht in 'de aard en omvang van de werkwijze van de AIVD', ondanks dat de minister recentelijk [op de vingers is getikt](#) door de Raad van State. De hoogste bestuursrechter vindt dat Plasterk de reden voor het weigeren van het openbaar maken van de tapstatistieken niet voldoende onderbouwde.

### **Een kennis van een verdachte hacken**

De nieuwe wet geeft de AIVD ook de bevoegdheid om systemen van derden te hacken om informatie over een doelwit te verkrijgen. Dit kan variëren van smartphones van de vrienden van een doelwit tot een server van de internetprovider die het doelwit gebruikt. Op dit moment mag de AIVD alleen doelwitten hacken.

Daarnaast biedt het wetsvoorstel de mogelijkheid dat ook aanbieders van communicatie worden getapt. Dit zijn bijvoorbeeld partijen als Skype, WhatsApp en Facebook, die de geheime diensten verplicht toegang moeten geven tot hun systemen. Door de toenemende druk vanuit de overheid voeren steeds

meer techbedrijven end-to-end-encryptie in, waarmee de communicatie zodanig wordt versleuteld dat zelfs het bedrijf - en ook een geheime dienst - de communicatie niet in kan zien.

### **Hoe staat de wet er nu voor?**

Het wetsvoorstel is bij de Raad van State ingediend. Zij kunnen het kabinet advies over de wet geven en de wet aanpassen. Daarna wordt het wetsvoorstel in de Tweede en Eerste Kamer behandeld, waarvan eerstgenoemde ook nog de mogelijkheid heeft om de conceptwet aan te passen. Plasterk wil de herziende Wet op de inlichtingen- en veiligheidsdiensten dit jaar in laten gaan.

Bron: RTL Nieuws

URL: <http://www.rtlnieuws.nl/economie/home/zo-wil-de-aivd-ook-jouw-e-mails-en-appjes-aftappen>