

# Consultatie WIV

## Document info

Titel: Consultatie WIV

Onderwerp: Internetconsultatie Wet op de inlichtingen- en veiligheidsdiensten 20XX

Eigenaar: Florian Overkamp

Classificatie: Publiek

SpeakUp BV  
Postbus 1330  
7500 BH Enschede  
t: +31 88 77 32 587  
f: +31 88 77 32 588  
e: info@speakup.nl  
Kvk: 08141739  
BTWnr: NL8153.86.837.B01  
Bank: 53.60.41.032  
IBAN: NL30ABNA0536041032  
BIC: ABNANL2A

## Document historie

Versie	Status	Toelichting	Auteur	Datum
1.0	Definitief		FO	31-08-15

## Distributielijst

Alle medewerkers van SpeakUp

## Inhoudsopgave

1 Inleiding.....	3
2 De Wet Inlichtingen- en Veiligheidsdiensten 20xx.....	4
2.1 Ongerichte informatievergaring.....	4
2.2 Toezicht.....	5
2.3 Maatschappelijke impact.....	5
3 Tot slot.....	6

# 1 Inleiding

SpeakUp heeft kennis genomen van het wetsvoorstel voor een 'Wet op de inlichtingen en veiligheidsdiensten 20xx'. In onze reactie op dit wetsvoorstel zullen wij ons toespitsen op de aspecten die ons als aanbieder van elektronische communicatiediensten raakt. Daarnaast plaatsen we enkele opmerkingen vanuit algemeen maatschappelijk perspectief. Overigens gaan wij in op de meest primaire bezwaren, op grond waarvan wij van mening zijn dat dit voorstel eigenlijk al geheel onhoudbaar is: **there is no easy fix**. Wij hopen dat op basis van de reacties op de consultatie (waaronder deze) een nadere dialoog geopend kan worden om wel tot werkbare voorstellen te komen. De secundaire zaken laten we dan ook voor wat het is.

In zijn algemeenheid is onze conclusie het volgende: Het wetsvoorstel in haar huidige vorm voorziet in een verregaande uitbreiding van bevoegdheden en medewerkingsplichten waarbij, naar onze mening, onvoldoende invulling wordt geven aan de randvoorwaarden die daar vanuit nationale en Europese (grond)wetten en verdragen bij horen. Daarnaast leidt het wetsvoorstel tot een big-brother samenleving die in de beste zin des woords niet wenselijk is:

- Zeer grote impact op privacy van burgers, en geen zicht op effectiviteit: proportionaliteit is onvoldoende;
- Toezicht verloopt via CTIVD achteraf: toetsing door rechterlijke macht of onafhankelijke autoriteit vooraf ontbreekt;
- Doordat wordt aangehaakt op de bredere definitie uit de Convention on Cybercrime voldoet nagenoeg ieder netwerk, iedere communicatiedienst (en daarmee nagenoeg ieder bedrijf in Nederland) tot het informatiedoel van de inlichtendiensten. Door de enorme hoeveelheid en het gebrek aan standaardisatie werkt dit kostenopdrijvend voor het bedrijfsleven en in het verlengde daarvan burgers

## 2 De Wet Inlichtingen- en Veiligheidsdiensten 20xx

### 2.1 Ongerichte informatievergaring

- De huidige wet- en regelgeving voorziet al afdoende in mogelijkheden om gericht informatievergaring (metadata en aftappen) toe te passen. Het wetsvoorstel voorziet echter ook in mogelijkheden om ongerichte informatievergaring toe te passen. Daarnaast worden veel meer organisaties onderworpen aan medewerkingsplicht ten behoeve van deze informatievergaring. **Vervolgens is in het wetsvoorstel en het memorie van toelichting nauwelijks onderbouwing waarom deze zeer ingrijpende maatregel noodzakelijk is terwijl het zeer goed mogelijk is dat er minder ingrijpende alternatieven voorhanden zijn.**
- Het wetsvoorstel voorziet in ruime bevoegdheden om data van communicatiedienst-aanbieders te vergaren. Sterker nog, het wetsvoorstel gebruikt een definitie die veel meer bedrijven kan aanspreken dan voorheen het geval was. In het memorie van toelichting wordt al opgemerkt dat de diensten momenteel niet in staat zijn om deze informatie te verwerken. **Dit betekent dat men zoekt naar een speld in een hooiberg – de doelmatigheid is twijfelachtig.**
- Desalniettemin worden de kosten voor inrichting geheel op de bedrijven afgewenteld. **Dit zal leiden tot een situatie waar deze kosten de concurrentiekracht van bedrijven ten opzichte van andere landen aantast.**
- Het wetsvoorstel biedt bedrijven onzekerheid ten aanzien van deze te maken kosten: De toelichting stelt dat medewerking een beperkt aantal aanbieders zal raken. Het is dus onzeker of de diensten ooit gebruik zullen maken van de mogelijkheid om informatie te vergaren bij een netwerk, maar het netwerk dient daartoe wel ingericht te zijn of te kunnen zijn op enige korte termijn. **Bedrijven investeren dus mogelijk 'verplicht' in inrichting die niet gebruikt wordt.**
- De toelichting geeft weer dat men nog ervaring moet opdoen op grond waarvan vervolgstappen door de diensten genomen kunnen worden. Hieruit valt af te leiden dat men zelf ook nog niet precies weet hoe dit alles effectief moet worden ingezet, en bedrijven moeten maar gewoon meedoen. **Dit betekent een carte blanche waardoor bedrijven niet eens weten waar en wanneer zij voor financiële verrassingen komen te staan.**
- De bewaartermijnen van vastgelegde communicatie is zeer ruim. Voor ongericht vergaarde informatie is sprake van een termijn van 3 jaar, en onder voorwaarden nog langer. **Deze termijn van bewaring van ongerichte informatie is bijzonder lang.**

## 2.2 Toezicht

- Het wetsvoorstel voorziet in ruime bevoegdheden om data van communicatiedienst-aanbieders te vergaren. Zoals we al (onder andere) gezien hebben in de casus rondom de WBT (ECLI:NL:RBDHA:2015:2498) meent ook onze rechterlijke macht dat toetsing door een rechterlijke instantie of onafhankelijke administratieve instantie vooraf noodzakelijk is. Dit is in het wetsvoorstel niet geregeld. **Deze aanpak is niet in lijn met de begrippen proportionaliteit en doelmatigheid.**

## 2.3 Maatschappelijke impact

- Het wetsvoorstel ziet toe op een zeer brede toegang van de inlichtendiensten tot algemene (ongerichte) gegevens, gecombineerd met een zeer lange bewaartermijn. In het licht van art. 8 van het EVRM werd al overwogen dat slechts het opslaan van gegevens al een inbreuk vormt. Het is nadrukkelijk niet zo dat pas het gebruik van de gegevens een inbreuk kan vormen. **Het opslaan op zichzelf al vormt een zeer ingrijpende inbreuk op de privacy van burgers.**
- Naast deze inbreuk op zich leidt deze aanpak ook tot een maatschappelijk effect dat iedere burger zich 'in de gaten gehouden' voelt. Het ondermijnt rechtstreeks alle communicatieplatformen die juist steunen op de vertrouwelijkheid, zoals klokkenluidersplatformen. **Het voorstel ondermijnt de vertrouwelijkheid van burgers bij geheimhouders (journalisten, advocaten etc.).**
- Toezicht vooraf versus achteraf: CTIVD kan achteraf besluiten dat een bevraging of tap-actie niet proportioneel was. Echter, in dat geval is het kwaad al geschied. Het is in het verleden al meermaals aan de orde geweest dat diensten te ver zijn gegaan bij bijvoorbeeld het aftappen van journalisten. Ondanks uitspraken van onder meer het EHRM tegen dit soort inbreuken is ook in het onderhavige wetsvoorstel geen sprake van toetsing vooraf. **Dit leidt tot een chilling effect.**
- De brede vergaring lijkt ook te worden aangewend als ruilhandel van gegevens met andere (buitenlandse) inlichtingendiensten. Toezicht op wat er daarna met die gegevens gebeurt is praktisch onmogelijk. **Deze vorm van koehandel met de privacy van burgers is volstrekt onacceptabel.**

### **3 Tot slot**

Zoals in de inleiding al aangegeven is er in onze optiek geen easy fix om dit wetsvoorstel in acceptabele vorm te krijgen. Onze volksvertegenwoordiging moet zich serieus afvragen hoe het kan dat zij enerzijds ageert op schendingen van mensenrechten in andere landen en anderszijds zelf wetsvoorstellen indienen die net zo hard hiermee de handen licht. En als wij buitenlandse diensten aanspreken op hun activiteiten jegens onze burgers, dan ligt het zeker niet voor de hand om in ruil daarvoor zelf die inlichten maar te vergaren.