Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

TOELICHTING ZIENSWIJZE CTIVD

T.b.v. technische briefing Tweede Kamer 13 december 2016 over wetsvoorstel Wiv 20..

Meneer de voorzitter,

Het voorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten is niet over één nacht ijs gegaan. Het is een resultante van bijna anderhalf decennium praktijkervaring die is opgedaan met de Wiv 2002, met het toezicht dat gedurende die tijd door de CTIVD op de praktijk is uitgeoefend alsmede met een evaluatie van die wet in 2012. Het voorstel komt ook in een aantal opzichten tegemoet aan de reacties uit de in 2015 gehouden internetconsultatie, aan het door de Tweede Kamer gevraagde Privacy Impact Assessment (PIA) en aan het advies van de Raad van State. Het is een complex geheel dat op een aantal terreinen desondanks toch duidelijke kaders schept voor de uitvoering van de wettelijke taak die aan de AIVD en MIVD is opgedragen.

Als onafhankelijk toezichthouder die rechtstreeks toegang heeft tot de AIVD en de MIVD en bekend is met de dagelijks praktijk binnen die diensten, heeft de CTIVD zich met name afgevraagd of zij met dit wetsvoorstel effectief toezicht kan uitoefenen. Effectief toezicht dat het noodzakelijke tegenwicht vormt voor de uitgebreide en diep ingrijpende bevoegdheden die de diensten in het geheim inzetten. Onze conclusie: **Het wetsvoorstel voorziet in bevoegdheden voor de diensten die passen bij de 21ste eeuw, maar in waarborgen tegen ongeoorloofd gebruik van die bevoegdheden die nog passen bij de 20ste eeuw. Het wetsvoorstel is daarmee niet in balans en geeft onvoldoende mogelijkheden voor effectief toezicht door de CTIVD. D**at is de boodschap die ik u allen hier vanmiddag wil meegeven.

De voorgestelde uitbreiding en modernisering van de bevoegdheden van de AIVD en MIVD zijn o.i. noodzakelijk. De diensten moeten mee kunnen bewegen met de maatschappelijke en technologische ontwikkelingen van de afgelopen en komende jaren. Als zij stil blijven staan, ontstaan in hun informatie-posities blinde vlekken. De bestaande gerichte en ongerichte bevoegdheden van de diensten zijn niet langer toereikend.

De samenleving is steeds meer gedigitaliseerd. Communicatie vindt hoofdzakelijk plaats via het internet. Ook het handelen en gedrag van personen en organisaties wordt in toenemende mate digitaal vastgelegd. Grote hoeveelheden gegevens (bulk) worden in dat verband wereldwijd getransporteerd en opgeslagen. Gegevens die voor de diensten bepalend kunnen zijn in het tijdig onderkennen van bedreigingen voor onze nationale veiligheid en dus voor hen onder strikte voorwaarden en omstandigheden toegankelijk moeten kunnen zijn.

Deze grote hoeveelheden gegevens zijn niet alleen waardevol voor een goede taakuitvoering door de diensten, ze brengen ook risico's met zich mee. Risico's voor de uitoefening van onze grondrechten waaronder de bescherming van de persoonlijke levenssfeer. Het gaat bij die grote hoeveelheden immers ook om gegevens van personen en organisaties die géén doelwit van de diensten zijn. Hun gegevens zullen in die bestanden zelfs de overgrote meerderheid vormen. Risico's bovendien, die niet alleen te maken hebben met het verzamelen van die gegevens, maar ook met de verdere verwerking

daarvan. Er zullen steeds meer complexe technieken worden ontwikkeld, die de analyse en het gebruik van grote hoeveelheden gegevens mogelijk maken. Het is daarbij steeds minder transparant of navolgbaar dat dit op een kwalitatief goede en rechtmatige manier gebeurt. Terwijl juist dáár, bij de analyse en het gebruik van de gegevens, de zwaarste inbreuk op grondrechten plaatsvindt. Risico's voor de bescherming van onze grondrechten dus.

Het wetsvoorstel voorziet in een versterking van waarborgen door de introductie van de TIB. Bindende toetsing voorafgaande aan de inzet van bevoegdheden is een klassieke waarborg. Klassieke waarborgen hebben vooral waarde bij gerichte bevoegdheden zoals het tappen van iemands telefoon of het hacken van een e-mailaccount. Maar bij het verzamelen en verder verwerken van grote hoeveelheden gegevens van nog te identificeren personen en organisaties, heeft het beperkte betekenis. Klassieke waarborgen alléén zijn dan niet meer toereikend.

Wat dan wel? Hoe kan er voor worden gezorgd dat de verwerking van die grote hoeveelheden gegevens (bulk) – die noodzakelijk is voor de taakuitvoering door de diensten – van voldoende waarborgen wordt voorzien? En hoe kan daar dan effectief toezicht op worden gehouden? Ik geef u daarvoor twee kernbegrippen: **(verantwoorde) databeperking en zorgplicht voor geautomatiseerde gegevensverwerking (compliance)**.

Verantwoorde databeperking betekent allereerst dat voorafgaande aan de interceptie van bulk moet worden bepaald of het niet gerichter kan, dat wil zeggen dat er geen valide gerichtere alternatieven zijn voor de bulkinterceptie. Het betekent daarnaast, dat die grote hoeveelheden gegevens zo snel mogelijk moeten worden beperkt tot die gegevens die écht noodzakelijk zijn voor de bescherming van de nationale veiligheid. Steeds weer moet in het verwerkingsproces het kaf van het koren gescheiden worden, waarbij het kaf terstond vernietigd moet worden. Het wetsvoorstel geeft daar weliswaar aanknopingspunten voor, door de interceptie 'onderzoeksopdrachtgericht' te noemen en in de MvT uit te leggen hoe dataminimalisatie plaatsvindt. Maar wéttelijke waarborgen worden niet gegeven. Dat is wel essentieel, want zonder wettelijke waarborgen is de beperking van de inbreuk op grondrechten te veel afhankelijk van de praktijk en kan de toezichthouder daarvoor onvoldoende tegenwicht bieden.

Naast verantwoorde databeperking, benoem ik een in de wet op te nemen zorgplicht voor geautomatiseerde gegevensverwerking. Deze zorgplicht betekent dat de diensten zelf verantwoordelijkheid moeten nemen voor de kwaliteit van de processen die voor hen core business zijn. Het gaat hier om automatische verwerkingsprocessen waarmee inbreuk wordt gemaakt op grondrechten, bijvoorbeeld door het geautomatiseerd verzamelen of analyseren van persoonsgegevens. De diensten moeten er op basis van een wéttelijke plicht voor instaan dat de geautomatiseerde gegevensverwerkingsprocessen voldoen aan juridische en technische kwaliteitsstandaarden. Zoals de authenticiteit van de gebruikte gegevensbestanden of de deugdelijkheid van de analysemethoden. Ook moeten zij zélf periodiek controleren, dat de werking van deze processen in de praktijk kwalitatief goed en rechtmatig is. De CTIVD dient de taak te krijgen daar toezicht op te houden, zowel m.b.t. de rechtmatigheid als de kwaliteit van de verwerkingsprocessen en de daarbij toegepaste techniek. Dat is essentieel, want effectief toezicht moet zich kunnen laten gelden daar waar de inbreuk op grondrechten zich het sterkst doet voelen.

De CTIVD, voorzitter, bespreekt deze en andere essentiële waarborgen in haar Zienswijze en geeft concrete adviezen voor verbetering van het wetsvoorstel.