Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Eerste Kamer
der Staten-Generaal
Postbus 20017
2500 EA DEN HAAG

Directie Cyber Security
Beleid

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag
www.nctv.nl

Ons kenmerk
568678

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 3 oktober 2014
Onderwerp Reactie op ingediende moties beleidsdebat d.d. 23 september 2014

Naar aanleiding van het beleidsdebat over privacy en het toezicht op de inlichtingen- en veiligheidsdiensten, dat op 23 september jl. plaatsvond met Uw Kamer, bied ik Uw Kamer met deze brief, mede namens de minister van Economische Zaken en de staatssecretaris van Veiligheid en Justitie, reactie aan op de door uw Kamer ingediende moties.

Reactie op motie De Vries c.s. aangaande de veiligheid van protocollen
De motie van de heer De Vries verzoekt de regering onderzoek te laten doen naar de onafhankelijkheid en betrouwbaarheid van organisaties die onder andere internetprotocollen opstellen en de Kamer hierover te informeren (CVIII nr).
De governance van het internet wordt vormgegeven in een complexe structuur van verschillende partijen die onderdelen van het internet reguleren. Overheden, technische experts en bedrijfsleven vervullen allen een rol in dit multistakeholder model. Nederlandse experts zijn hierbinnen overigens goed vertegenwoordigd. Dit multi stakeholder model sluit aan bij de benadering van de Nederlandse Cyber Security Strategie 2, die transparantie, kennis en (zelf)regulering als de belangrijkste sturingsmechanismen onderkent. Een organisatie als de IETF werkt ook volgens dit model.
De IETF is een organisatie waarin een groot aantal specialisten uit de internetgemeenschap samenwerkt aan de ontwikkeling van standaarden en protocollen. IETF is transparant georganiseerd: de werkzaamheden vinden plaats op e-maillijsten die openbaar zijn en gearchiveerd. Beslissingen worden gebaseerd op basis van een consensus model en er is een bestuurlijke structuur met mogelijkheid tot beroep op beslissingen. In een organisatie waarin een groot aantal specialisten samenwerkt, heeft een aantal deelnemers ongetwijfeld banden met veiligheidsdiensten (er is binnen de IETF een aantal deelnemers transparant over banden met de NSA). De open en transparante structuur van de IETF sluit de mogelijkheid van oneigenlijke sturing niet uit, maar geeft de maximale garantie van kundige peer review, door experts van de IETF.

Beveiligde verbindingen op het internet worden tot stand gebracht door encryptie protocollen. De encryptiebewerkingen die in deze protocollen worden gebruikt, worden over het algemeen niet door de IETF ontwikkeld maar door andere

standaardisatieorganisaties. Specialisten in IETF beoordelen deze op geschiktheid en onderzoeken deze protocollen op zwakheden. Actieve participatie van Nederlandse experts (overheid, wetenschap en bedrijfsleven) in de beschreven organisaties en het bij voortduring agenderen van het belang van veilige standaarden zoals Nederland doet, lijkt dan ook het meest passende antwoord op mogelijke ongewenste inmenging. Tegen deze achtergrond lijkt een nationaal onderzoek naar de onafhankelijkheid en betrouwbaarheid van deze organisaties als geschetst in de motie niet opportuun, blijf ik bij de met de NCSS2 ingezette lijn, en ontraad ik daarom de motie.

Reactie op motie Strik c.s. over onafhankelijk toezicht op overheidsinstanties
Mevrouw Strik c.s. heeft een motie ingediend waarin zij de regering verzoekt onderzoek te verrichten naar nut en noodzaak van onafhankelijk toezicht op overheidsinstanties die nu niet onder toezicht van de CTIVD vallen, maar die wel soortgelijke taken verrichten die de bescherming van de persoonlijke levenssfeer van burgers kunnen raken, en de Kamer hierover te informeren (motie CVIII nr. J). Het onafhankelijke toezicht waarop deze motie doelt, is er al. Het College bescherming persoonsgegevens (Cbp) ziet op grond van artikel 35 van de Wet politiegegevens (Wpg) erop toe dat de verwerking van politiegegevens – daaronder vallen ook gegevens die door de criminele inlichtingeneenheden worden verkregen – overeenkomstig die wet geschiedt. Op grond van artikel 46 Wpg geldt hetzelfde met betrekking tot de gegevensverwerking door bijzondere opsporingsdiensten. En op grond van de artikelen 27 en 39r van de Wet justitiële en strafvorderlijke gegevens houdt het Cbp ook toezicht op de verwerking van justitiële en strafvorderlijke gegevens. Het Cbp beschikt als toezichthouder over tenminste dezelfde bevoegdheden als de CTIVD: het vragen van inlichtingen, het opvragen van gegevens, het uitvoeren van onderzoek en het recht om plaatsen te betreden. Het Cbp heeft bovendien de bevoegdheid ook woningen te betreden, bestuursdwang toe te passen en in bepaalde gevallen een bestuurlijke boete op te leggen. Het Cbp staan dus ten opzichte van de CTIVD meer dan voldoende toezichtinstrumenten ter beschikking. Het kijkt daarbij naar alle aspecten van gegevensverwerking door de opsporingsdiensten. Hoe vindt de informatieverzameling plaats? Hoe vindt de opslag van gegevens plaats? Wie heeft toegang tot die gegevens?

Los van het feit dat met het Cbp al een voldoende geëquipeerde toezichthouder bestaat, heeft het verzamelen van informatie door de inlichtingen- en veiligheidsdiensten (IVD) een wezenlijk ander doel dan het verzamelen van informatie door de opsporingsdiensten. Het verzamelen daarvan vindt mede om die reden plaats binnen verschillende wettelijke kaders. Een belangrijk verschil daarbij is dat het verzamelen van informatie door de opsporingsdiensten, als het tot vervolging komt, ook nog wordt getoetst door een rechter-commissaris in een gerechtelijk vooronderzoek of door de strafrechter ter terechtzitting. Dat geldt zeker in het geval dat voor het verzamelen van informatie gebruik is gemaakt van bijzondere opsporingsbevoegdheden. Deze verschillen impliceren dat de toezichtfunctie van de CTIVD niet zo maar naar de gegevensverwerking door de opsporingsdiensten zou kunnen worden getransplanteerd. Voor zover in strafzaken informatie van de IVD wordt gebruikt, verschilt die ook wezenlijk van de informatie die door opsporingsdiensten in dergelijke zaken wordt ingebracht. De IVD brengen hun informatie in door middel van een ambtsbericht, waarin de

methoden waarmee deze informatie is verzameld, geheim blijven. De opsporingsdiensten brengen hun informatie in door middel van een proces-verbaal, waarin ook de methoden waarmee de informatie is verzameld, uit de doeken worden gedaan. Tot slot lijkt het mij allesbehalve opportuun om twee onafhankelijke toezichthouders – CBP en CTIVD – met betrekking tot de gegevensverwerking door dezelfde diensten werkzaam te laten zijn. Dat zou niet alleen inefficiënt zijn, maar ook tot competentieconflicten kunnen leiden.
Tegen de achtergrond van deze overwegingen ontraad ik de aanvaarding van de motie Strik c.s. (motie CVIII nr. J).

Reactie op motie Gerkens c.s aangaande de ethische kant van digitalisering
Mevrouw Gerkens c.s. heeft een motie ingediend waarin zij de regering verzoekt het Rathenau Instituut te vragen een onderzoek te doen naar de wenselijkheid van een commissie die kan adviseren over de ethische kant van de digitalisering van de samenleving (CVIII nr. E). Ik heb de kamer in reactie op deze motie al laten weten dat ik de opvatting van mevrouw Gerkens deel dat het kabinet en de kamer over een zo belangrijk onderwerp als door haar is aangekaart, een discussie voeren. Met het oog daarop heb ik erop gewezen dat het kabinet in mei van dit jaar al een adviesaanvraag tot de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) heeft gericht over het thema "big data, veiligheid en privacy", waarin ook de ethische kant van de digitalisering van de samenleving aan de orde komt. Ik verwijs daarvoor naar het slot van de adviesaanvraag waarin een aantal onderzoeksvragen zijn geformuleerd die een uitvloeisel zijn van het debat dat de kamer op 11 maart jl. over de Staat van de rechtsstaat heeft gevoerd. Op verzoek van de kamer zijn deze vragen naderhand meegenomen in de adviesaanvraag aan de WRR. Het gaat hier om de volgende vragen:

1. Hoe zorgen we ervoor dat, nu de informatie over personen in databases steeds belangrijker wordt, de kwaliteit van de informatie in de gegeven context op een navenant niveau wordt gewaarborgd?
2. Hoever strekt de eigen verantwoordelijkheid van de burger voor de kwaliteit van zijn gegevens in databases?
3. Hoe slagen we er dan in de burger zelf meer effectieve controle te geven over zijn gegevens?
4. Is het voor de burger mogelijk om steeds op basis van "informed consent" te beslissen?

De WRR heeft mij desgevraagd laten weten van plan te zijn in zijn advies bij de beantwoording van vragen als deze alle relevante aspecten mee te nemen, met inbegrip van de ethische aspecten. De ethische kant van de digitalisering van de samenleving zal in het advies dus genoegzaam aan de orde komen. Tegen deze achtergrond lijkt mij een verzoek aan het Rathenau Instituut als bedoeld in de motie niet opportuun en blijf ik bij mijn verzoek de motie aan te houden tot het moment waarop het kabinet zijn standpunt over het advies van de WRR heeft bepaald. Voor het geval dat de motie toch in stemming wordt gebracht, ontraad ik op grond van dezelfde overwegingen de aanvaarding daarvan.

De Staatssecretaris van Veiligheid en Justitie,

F. Teeven