Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

32 761 Verwerking en bescherming persoonsgegevens

Nr. 83 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 mei 2015

In een brief van 16 april jl. (kenmerk 2015Z06289/2015D14223) heeft de vaste commissie voor Veiligheid en Justitie van uw Kamer mij om een reactie gevraagd op het bericht op de website «nu.nl» van 2 april 2015 onder de kop «Privacygroepen roepen Van der Steur op tot delen visie rond privacy». Dit bericht houdt verband met een open brief van een coalitie van 32 organisaties, bedrijven en personen – hierna kortheidshalve aangeduid als: de privacycoalitie – aan mij, waarin zij hun zorgen uiten over de privacybescherming van burgers in onze informatiemaatschappij. Zij roepen mij in die brief op om hierover een visie te ontwikkelen, daarna een publiek debat erover te faciliteren en tot die tijd de behandeling op te schorten van wetten die naar hun oordeel ertoe leiden dat burgers zonder een specifieke en concrete verdenking toch worden gevolgd.

Mede namens mijn ambtgenoot van Binnenlandse Zaken en Koninkrijksrelaties geef ik u hierbij onze reactie op deze oproep. Deze reactie geldt tevens als beantwoording van de vragen die het Lid Thieme naar aanleiding van deze oproep op 9 april jl. heeft gesteld over het ontbreken van een visie op privacybescherming.

Direct nadat de privacycoalitie haar oproep had gedaan heb ik aangekondigd deze coalitie voor een gesprek uit te zullen nodigen. Daaraan heb ik onmiddellijk gevolg gegeven. Dit gesprek heeft 13 april jl. plaatsgevonden met een aantal vertegenwoordigers van de privacycoalitie. In dat gesprek hebben zij hun oproep toegelicht. Zij hebben bepleit niet ongericht gegevens rond de telecommunicatie van burgers te bewaren maar die bewaring te beperken tot bijvoorbeeld gegevens rond de telecommunicatie van reeds veroordeelde personen. Zij hebben verder onder meer gepleit voor onafhankelijk toezicht op de wijze waarop opsporingsdiensten bepaalde opsporingsmiddelen inzetten waarbij moderne technieken op het gebied van ICT worden toegepast.

kst-32761-83
ISSN 0921 - 7371
's-Gravenhage 2015

In het gesprek heb ik op deze oproep gereageerd en naar voren gebracht dat mijn visie en die van het kabinet op privacybescherming zich concentreert op een achttal toetsstenen. Deze zijn verweven in de volgende vragen:

1. Is de verwerking van persoonsgegevens noodzakelijk voor een legitiem doel?
2. Voldoet de verwerking van persoonsgegevens aan de eisen van proportionaliteit en subsidiariteit?
3. Is de doelbinding wettelijk vastgelegd en voldoende ingekaderd?
4. Is er een adequate regeling van toegang tot de persoonsgegevens?
5. Zijn de persoonsgegevens goed beveiligd?
6. Zijn de bewaartermijnen goed geregeld?
7. Is er, waar nodig, een Privacy Impact Assessment (PIA) uitgevoerd?[1]
8. Is het toezicht op de verwerking van persoonsgegevens goed geregeld?

Bij de voorbereiding van beleids- en wetgevingstrajecten die betrekking hebben op gegevensverwerking ten behoeve van de veiligheid van burgers spelen deze vragen een prominente rol. Zij dienen bij elk afzonderlijk traject van een deugdelijk antwoord te worden voorzien.

In dit gesprek heb ik ook gezegd dat een veilige samenleving borg staat voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer terwijl tegelijkertijd voor het garanderen van een veilige samenleving inbreuken op de persoonlijke levenssfeer noodzakelijk kunnen zijn.

Een thema dat dergelijke trajecten met elkaar verbindt, is «veiligheid en privacy». Anders dan de privacycoalitie lijkt te veronderstellen heeft het kabinet daarop een heldere visie. Daarin staat centraal dat veiligheid en privacy voor een samenleving allebei essentiële waarden zijn. Veiligheid en privacy worden evenwel vaak als uitersten gezien, alsof het een keuze betreft tussen het één of het ander. Zij liggen echter voor een belangrijk deel in elkaars verlengde, het gaat namelijk steeds om de bescherming van burgers.

Het is voor burgers essentieel dat zij zich in het maatschappelijk verkeer vrij kunnen bewegen en vrij kunnen communiceren. De persoonlijke veiligheid van burgers wordt echter aangetast door misdragingen van anderen. De overheid heeft als taak die veiligheid te waarborgen. De burger die wordt geconfronteerd met een aantasting van zijn veiligheid zal er weinig begrip voor hebben dat informatie die had kunnen bijdragen aan de opsporing van de daders niet gebruikt kan worden terwijl dit wel beschikbaar is of zou kunnen zijn. Het gebruiken van die informatie mag dan ook niet enkel gezien worden als een inbreuk op de persoonlijke levenssfeer. Die inbreuk kan noodzakelijk zijn om te waarborgen dat anderen gevrijwaard blijven van een aantasting van hun persoonlijke veiligheid. Een ieder die slachtoffer kan worden van strafbare feiten heeft daar belang bij. Het gebruik van die informatie kan onder omstandigheden een gerechtvaardigde inperking van het recht op bescherming van de persoonlijke levenssfeer zijn, onder meer als dit nodig is in het belang van de nationale veiligheid, het voorkomen van wanordelijkheden en strafbare feiten of voor de bescherming van de rechten en vrijheden van anderen (artikel 8 EVRM).

Voor de effectiviteit van de criminaliteitsbestrijding kan het van essentieel belang zijn gegevens van personen te bewaren ten aanzien van wie er op

[1] Zie ook motie Franken (Kamerstuk 31 051, D); aan deze motie is in combinatie met het regeerakkoord uitvoering gegeven met het ontwikkelen van het toetsmodel Privacy Impact Assessment Rijksdienst (Kamerstuk 26 643, nr. 282.

het moment van de bewaring geen concrete vermoedens bestaan van betrokkenheid bij ernstige strafbare feiten. Dit geldt vooral voor gegevens die kunnen leiden tot de identificatie van personen die mogelijk betrokken kunnen zijn bij het plegen van ernstige misdrijven of daarvan slachtoffer zijn. Voor wat betreft gegevens over telecommunicatie blijkt dit belang uit het rapport van het Openbaar Ministerie en de politie over het nut van het bewaren van die gegevens dat ik op 31 maart jl. naar de beide Kamers heb gezonden (Kamerstuk 33 870, nr. 3; Kamerstuk 33 145, AC). Uit dit rapport valt af te leiden dat bijvoorbeeld een zaak als het kinderpornonetwerk rond Robert M. zonder gebruik van historische internetgegevens niet zou kunnen worden opgelost. Ik noem deze zaak bewust, omdat een discussie over abstracte principes als veiligheid en privacy pas echt betekenis kan krijgen als zij wordt verbonden met concrete casuïstiek.

Beperking van de opslag van gegevens tot louter de gegevens van verdachte burgers is niet goed denkbaar met het oog op het doel van die opslag, namelijk de doeltreffende opsporing van ernstige criminaliteit. In het geval van een «first offender» kan niet reeds op voorhand een onderscheid worden gemaakt tussen verdachte en niet-verdachte burgers. Dit is wat betreft telefoon- en internetgegevens ook erkend door de rechter in het kort geding dat een aantal organisaties had aangespannen tegen de Staat om de Wet bewaarplicht telecommunicatiegegevens buiten werking te stellen. Daarbij is wel van belang dat er voldoende nauwkeurige, wettelijke waarborgen zijn die ervoor zorgen dat de toegang tot de bewaarde gegevens ten behoeve van de opsporing daadwerkelijk is beperkt tot wat strikt noodzakelijk is (Rb Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498).

Dit is een belangrijk uitgangspunt dat ook voor andere voorstellen van betekenis is. Het opslaan of doen bewaren van grote hoeveelheden gegevens van burgers voor veiligheid en rechtshandhaving, zonder dat er op het moment van de bewaring sprake is van vermoedens van betrokkenheid bij ernstige strafbare feiten, is op grond van Europese jurisprudentie niet per definitie ontoelaatbaar. Het EHRM heeft verschillende criteria geformuleerd die in hun onderlinge samenhang in de beoordeling van de bewaring worden betrokken, zoals het bestaan van adequate waarborgen met betrekking tot de bescherming van de persoonlijke levenssfeer. De noodzaak van waarborgen is des te groter in het geval van geautomatiseerde verwerking van persoonsgegevens, niet in het minst als de gegevens worden gebruikt voor politiedoeleinden. De nationale wetgeving dient in het bijzonder te verzekeren dat dergelijke gegevens relevant zijn, het bewaren niet buitensporig is in relatie tot de doelen waarvoor ze worden opgeslagen en bewaard worden in een vorm die de identificatie van de betrokkene niet langer toelaat dan noodzakelijk voor het doel waarvoor de gegevens zijn opgeslagen. Het EHRM eist een redelijke bewaartermijn en waarborgen omtrent de opslag en het gebruik van de gegevens, in het bijzonder wanneer het gaat om niet-veroordeelde personen.

Op de achtergrond speelt mee dat het EVRM voor de bescherming van grondrechten uitgaat van het individuele belang van de klager en persoonlijke schade. De jurisprudentie van het EHRM geeft als gevolg daarvan geen eenduidig beeld van de grenzen die vanuit privacy-oogpunt moeten worden gesteld aan grootschalige opslag van gegevens van burgers zonder dat er op het moment van de bewaring sprake is van vermoedens van betrokkenheid bij ernstige strafbare feiten. Die opslag betreft immers per definitie niet een specifiek individu, maar in beginsel een ieder (Vgl. Rb Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966, r.o. 5.24). Dit laatste aspect neemt niet weg dat grootschalige opslag van gegevens van burgers ten behoeve van de opsporing van ernstige

strafbare feiten in het licht van internationale en nationale jurisprudentie een gedegen onderbouwing van de noodzaak vergt en hoge eisen stelt aan de waarborgen rond het gebruik van de gegevens. De eerdergenoemde toetsstenen zijn hiervoor in het bijzonder van belang.

Omdat aan de eerdergenoemde bewaarplicht en ook de overige voorstellen die de privacycoalitie in haar oproep noemt wel degelijk een visie ten grondslag ligt, en deze voorstellen van essentieel belang zijn voor de waarborging van de veiligheid in de samenleving, ziet het kabinet geen aanleiding de voorbereiding en verdere behandeling van deze voorstellen op te schorten. De discussie over de adequate waarborgen voor de bescherming van de privacy kan en zal in uw Kamer steeds in de context van deze afzonderlijke wetsvoorstellen worden gevoerd. Dit heb ik ook aan de bij het gesprek aanwezige vertegenwoordigers van de privacycoalitie laten weten.

Ik acht het van belang dat het draagvlak voor deze voorstellen zo breed mogelijk is. Daarom zet ik graag de dialoog voort over het evenwicht tussen het belang van de veiligheid en de bescherming van de privacy bij de brede opslag van gegevens van burgers en de invulling van de garanties en waarborgen ten behoeve van dat evenwicht.

Het kabinet heeft zijn visie op het bredere thema «veiligheid en privacy» vastgelegd in de notitie «Vrijheid en veiligheid in de digitale samenleving. Een agenda voor de toekomst» van 13 december 2013 (Kamerstukken II 2013/14, 26 643, nr. 298). In deze notitie heeft het kabinet gewezen op het dynamische en complexe karakter van dit thema. De dynamiek van het thema brengt mee dat het denken niet kan worden beperkt tot een bepaald statisch kader maar dat het denken hierover – gevoed door de technologische ontwikkelingen – voortdurend zal moeten worden getoetst en tegen het licht gehouden, zo nodig te herijken en waar mogelijk te verfijnen. De complexiteit van een aantal vraagstukken heeft tot gevolg dat deze nog verder doordacht moeten worden. De kabinetsnotitie noemt de volgende vragen: «Moet er niet een sterker onderscheid worden gemaakt tussen het verzamelen en opslaan van data en het gebruik daarvan?», «Hoe kan ervoor worden gezorgd dat het proces van «profiling» voldoende transparant is?» en «Wat betekent de komst van kwantumcomputers voor dataverwerking ten behoeve van de veiligheid?». Deze vragen heeft het kabinet op 26 mei 2014 voor advies voorgelegd aan de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) met het verzoek uiterlijk 1 juli 2015 advies uit te brengen.

Bij het opstellen van een kabinetsstandpunt over het advies van de WRR zal ik ook de inbreng van de privacycoalitie betrekken. Verder zal ik suggesties van deze coalitie, zoals gedaan in het gesprek van 13 april jl., betrekken bij de verdere voorbereiding van het wetsvoorstel tot aanpassing van de Wet bewaarplicht telecommunicatiegegevens, mede in het licht van het advies van de Raad van State over dit wetsvoorstel. Ingeval zich andere trajecten aandienen om met de privacycoalitie een dialoog aan te gaan over de privacybescherming van burgers in onze informatiemaatschappij zal ik dat graag doen.

Het is immers in ons aller belang dat het denken over het thema «veiligheid en privacy» verder wordt ontwikkeld, op een wijze die recht doet aan de verschillende inzichten en overtuigingen, zodat mogelijke oplossingsrichtingen zo breed mogelijk worden gedragen.

De Minister van Veiligheid en Justitie,
G.A. van der Steur