Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

De Voorzitter van de
Wetenschappelijke Raad voor het Regeringsbeleid
Prof. dr. J.A. Knottnerus
Postbus 20004
2500 EA Den Haag

Directoraat-Generaal Rechtspleging en Rechtshandhaving

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Ons kenmerk
504054

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

Datum 26 mei 2014
Onderwerp Big data, veiligheid en privacy

Op 13 december jl. heeft het kabinet de notitie "Vrijheid en veiligheid in de digitale samenleving. Een agenda voor de toekomst" aan de beide kamers aangeboden (kamerstukken II 2013/14, 26643, nr. 298; kamerstukken I 2013/2014, 33750, O).

In deze notitie heeft het kabinet aangegeven dat de ontwikkelingen en vraagstukken die in die notitie geagendeerd worden, op sommige punten nog verder doordacht moeten worden. Het gaat daarbinnen specifiek om de ontwikkelingen en vraagstukken die onder het overkoepelende thema "big data, veiligheid en privacy" vallen. De drie hoofdvragen worden hieronder uiteengezet. Daarbij past de kanttekening dat deze vragen in lijn met eerdergenoemde kabinetsnotitie geen betrekking hebben op het werk van de inlichtingen- en veiligheidsdiensten,
De eerste hoofdvraag die in de notitie wordt opgeworpen, is of er een sterker onderscheid moet worden gemaakt tussen toegang tot en gebruik van gegevens bij "big data". Traditioneel omvat gegevensbescherming zowel de toegang tot als het gebruik van persoonsgegevens. Echter, in tijden van "big data" kan het lastig zijn om de toegang tot gegevens te beschermen. Zo speelt bij regulering van de toegang bijvoorbeeld mee dat de gegevensstromen zich niet aan landsgrenzen houden en de locatie waar gegevens zich bevinden (mede als gevolg van de groei van "cloud-computing"), een steeds meer fluïde karakter krijgt. Daarom zal men sterker zijn toevlucht willen nemen tot het reguleren van het gebruik van gegevens.

Deze ontwikkeling roept ook een aantal vervolgvragen op:
- Welke gevolgen zullen ontstaan voor de regievoering door de staat ten aanzien van zowel de bescherming van persoonsgegevens als het gebruik daarvan voor het bevorderen van de veiligheid?
- Waar liggen kansen om "big data" zo te gebruiken dat dit gebruik zowel de effectiviteit van het veiligheidsbeleid vergroot als de bescherming van persoonsgegevens beter waarborgt?
- Hoe kunnen de beginselen van doelbinding en dataminimalisatie, die aan het huidige Europese en Nederlandse gegevensbeschermingsrecht ten grondslag liggen, hun functie behouden?
- Hoe verhoudt het reguleren van het gebruik van gegevens op nationaal of Europees niveau zich toch het verschijnsel dat datastromen niet binnen de

landsgrenzen blijven. Wat voor toegevoegde waarde levert het reguleren van het gebruik van data tegen deze achtergrond? En is er aanvullend beleid nodig dat voldoende technologische soevereiniteit waarborgt zodat het reguleren van het gebruik van data op nationaal of Europees niveau zinvol wordt?
- Als het enkel gaat om verzamelen en opslaan van persoonsgegevens, zonder dat van die gegevens kennis wordt genomen, welk gewicht moeten we dan toekennen aan deze beperking van het recht op bescherming van persoonsgegevens? Bij deze vraag is ook van belang op te merken dat bij "big data" men van tevoren soms niet kan uitsluiten of een gegeven op een later moment een persoonsgegeven zal worden.
- Hoe verhoudt zo'n beperking, gelegen in het verzamelen en opslaan van persoonsgegevens, zich tot de beperking van het recht op bescherming van persoonsgegevens die gelegen is in het verder verwerken van een deel van die gegevens, waarbij van de inhoud van de gegevens wèl kennis wordt genomen?

De tweede hoofdvraag uit de notitie is hoe bij het gebruik van "big data" ervoor kan worden gezorgd dat het proces van "profiling", "datamining" en andere analyse-technieken ten behoeve van de veiligheid voldoende transparant zijn. Het vermogen om uit een enorme hoeveelheid digitale gegevens snel en precies relevante patronen in kaart te brengen, vormt een belangrijk kenmerk van de huidige technieken voor "big data"-analyses. Daarbij kan zowel *ongericht* worden 'gegraven' naar datapatronen in grote hoeveelheden gegevens (ook wel: "datamining") als *gericht* worden "gegraven" naar dergelijke datapatronen ("profiling").

Bij het gebruik van dergelijke technieken rijst de vraag op welke wijze in het analyseproces afwegingen plaatsvinden met betrekking tot beginselen als doelbinding en dataminimalisatie De vragen met betrekking tot transparantie, doelbinding en dataminimalisatie gelden temeer, indien personen bij zowel het dataminen als het profileren worden gecategoriseerd en indien op grond daarvan bepaalde beslissingen ten aanzien van individuele personen worden genomen.

Ten aanzien van de processen van "profiling" en "datamining" speelt een aantal vragen:
- In hoeverre en op welke wijze kunnen deze processen transparant zijn?
- Kan de transparantie van dergelijke processen op zo'n manier worden geborgd dat het niet het belang van een effectieve uitvoering van bijvoorbeeld de politietaak doorkruist?
- In hoeverre kan daaraan bijdragen dat de technologie die voor "profiling" en "datamining" wordt gebruikt, open source software is?
- Is het noodzakelijk dat persoonsgegevens eerst moeten worden opgeslagen, voordat je tot een vorm van "profiling" en "datamining" kan komen en, zo ja, op welke wijze zou dit kunnen worden voorkomen?
- Voor zover dat bij "big-data-analyses" niet voorkomen kan worden, zijn daarvoor dan effectieve waarborgen te creëren?

Naast de technologische kant verdient bij "profiling" en "datamining" ook de maatschappelijke kant aandacht:
- In hoeverre kan aan de transparantie van deze processen worden bijgedragen door inzicht te bieden in de gedragswetenschappelijke vooronderstellingen die aan een specifieke vorm van "profiling" of "datamining" ten grondslag liggen?
- En hoe kan dit inzicht geboden worden zonder dat dit de effectiviteit van bijvoorbeeld het optreden van de politie nadelig beïnvloedt?
- In relatie tot deze processen komt ook de vraag op welke betekenis dient te worden gehecht aan het feit dat vele gegevens die daarvoor kunnen worden gebruikt, geplaatst zijn op internet in een openbare omgeving.

De derde en laatste hoofdvraag die verder doordacht moet worden, is wat de komst van quantum-computers voor het proces van gegevensverwerking ten behoeve van de veiligheid betekent:

- Op welke wijze kunnen we zowel de mogelijkheden die deze computers bieden, goed benutten als een adequaat niveau van gegevensbescherming handhaven?
- En hoe moeten we aankijken tegen de verwachting dat een quantumcomputer veel sneller dan nu encryptie-sleutels kan kraken?
- Hoe verhoudt zich dat tot de verwachting dat de komst van quantumcomputers ook een enorme impuls aan encryptietechnieken kan geven, die zelfs met behulp van quantumcomputers niet gemakkelijk te doorbreken zijn?

Het gaat hier om drie belangrijke hoofdvragen voor de Agenda voor de toekomst, zoals die in eerdergenoemde kabinetsnotitie is gelanceerd. Het gaat hier om een agenda met een dynamisch karakter: er kunnen andere vraagstukken aan worden toegevoegd, als bepaalde ontwikkelingen dat vergen.

Met dat uitgangspunt in het achterhoofd is in een debat in de Eerste Kamer over de Staat van de rechtsstaat op 11 maart jl. een vraagstuk aan de orde geweest dat in het teken staat van het thema "big data" en zich daarom goed leent voor opneming in deze agenda. Dit vraagstuk houdt verband met het verschijnsel dat het volgen en het beïnvloeden van gedrag met behulp van technologie, ook zonder dat we het merken, steeds gemakkelijker wordt.

Dit verschijnsel roept in dit tijdperk van "big data" de volgende vragen op:

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

Gelet op de brede expertise van uw raad op onder meer het terrein van technologie, veiligheid en grondrechten, leg ik mede namens de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties deze vragen graag aan u voor, met het verzoek ons uiterlijk 1 juli 2015 van advies te dienen. Tegelijkertijd verzoeken wij bij de opstelling van uw advies optimaal gebruik te maken van elders aanwezige bijzondere expertise op genoemde terreinen. Tot slot zouden wij het op prijs stellen, indien u bij de opstelling van uw advies de inzichten betrekt die voortvloeien uit vergelijkbare discussies en onderzoeken in het buitenland.

De Minister van Veiligheid en Justitie,

I.W. Opstelten