Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2013–2014

33 169 EU-voorstel: Richtlijn bescherming persoonsgegevens bij gebruik door politiële en justitiële autoriteiten (COM(2012)10) en EU-voorstel Verordening algemeen kader bescherming persoonsgegevens (COM(2012)11)[1]

P

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 15 november 2013

Hierbij bied ik u, mede namens de minister van Buitenlandse Zaken, de minister van Defensie, de minister van Economische Zaken en de minister van Veiligheid en Justitie, de antwoorden aan op de vragen die de vaste commissie voor Immigratie en Asiel en de vaste commissie voor Veiligheid en Justitie hebben gesteld per brief van 15 oktober jl. (kenmerk 153745.01u) over NSA, privacy en (economische) spionage.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk

[1] Zie dossiers E120003 en E120004 op www.europapoort.nl

kst-33169-P
ISSN 0921 - 7371
's-Gravenhage 2013

1. Kwamen de onthullingen van de heer Snowden voor de regering als een verrassing?

Ja.

2. Heeft de regering zich diepgaand op de hoogte gesteld van de betekenis van de onthullingen van de heer Snowden voor de grondrechtelijke bescherming van de persoonlijke levenssfeer van de burgers?

Ja. Het Kabinet hecht aan zorgvuldige en deugdelijke bescherming van persoonsgegevens. Dit is een punt van aandacht in de gesprekken die momenteel bilateraal worden gevoerd met de Amerikaanse overheid naar aanleiding van de onthullingen over de NSA. Zo heeft de minister van Buitenlandse Zaken reeds zijn zorgen over de activiteiten van de NSA overgebracht aan zijn Amerikaanse collega Kerry en heb ik gesproken met de directeur van de NSA. Daarnaast beoordeelt Nederland het initiatief van Duitsland en Frankrijk om te komen tot afspraken met de Amerikanen als positief, heeft hierover contact met beide landen, en zal waar mogelijk een actieve bijdrage leveren.

Er is een EU-VS expertgroep gestart die zich buigt over de bescherming van de persoonlijke levenssfeer en van elektronische gegevens van burgers. Het doel van deze expertgroep is inzicht krijgen in elkaars programma's en de wijze waarop deze zijn verankerd in de rechtstaat. Tevens zijn de staatssecretaris van Veiligheid en Justitie en ik actief betrokken bij de onderhandelingen over de nieuwe Europese wetgeving voor de bescherming van de persoonlijke levenssfeer. De betekenis van de onthullingen van de heer Snowden zal hierbij worden meegenomen. Zie ook het antwoord op vraag 3.

3. Welke gevolgen hebben de onthullingen voor de onderhandelingen over de te wijzigen EU-wetgeving ten aanzien van de bescherming van persoonsgegevens?

Tijdens de JBZ-Raden van juli en van oktober 2013 is – telkens informeel – van gedachten gewisseld over de consequenties die aan de onthullingen verbonden zouden kunnen worden. Besluiten zijn terzake niet genomen. Ik verwijs de Kamer naar de verslagen over de raadsvergaderingen.

Op 16 september 2013 is er een zogeheten Friends of the Presidency-vergadering (een informele vergadering waarin geen formele besluitvorming plaatsvindt) gewijd aan twee voorstellen tot aanpassing van hoofdstuk V van de EU verordening gegevensbescherming. In dat hoofdstuk wordt de doorgifte van persoonsgegevens uit de EU naar derde landen geregeld. Voor een verslag van dat beraad, verwijs ik graag naar de rapportage over de onderhandelingen die betrekking heeft op het derde kwartaal van dit jaar. De discussie over Hoofdstuk V van de verordening zal nog worden voortgezet. Daarbij zullen de uitkomsten van het nog lopende beraad tussen de EU en de VS over de verzameling van gegevens en de daaraan ten grondslag liggende wetgevingssystemen betrokken worden.

Naast de Raad beraadslaagt ook het Europees Parlement over het wetgevingspakket. Het Europees Parlement schenkt nadrukkelijk aandacht aan de doorgifte van persoonsgegevens uit de EU aan de overheden van derde landen. Het spreekt voor zich dat het onderwerp te zijner tijd in de triloog tussen Commissie, Raad en Europees Parlement nadrukkelijk aan de orde komt.

4. Welke gevolgen hebben de onthullingen voor de onderhandelingen tussen de EU en de VS over een te sluiten vrijhandelsverdrag? Eist de EU dat de EU-normen ten aanzien van privacy van toepassing zijn voor zover Unieburgers betrokken zijn bij de toepassing van het verdrag?

Het kabinet vindt het nog steeds van belang dat we spoedig tot een ambitieus en veelomvattend akkoord met de Verenigde Staten komen. Juist Nederland heeft daar veel bij te winnen: naast een structurele verwachte groei van het Nederlandse BNP met 4 miljard per jaar, levert het akkoord ook nieuwe banen en lagere prijzen op. Het kabinet legt geen verband tussen EU-normen ten aanzien van privacy en het verdrag.

5. Op welke wijze heeft de regering gereageerd op de onthulling dat ook de bankgegevens via SWIFT, waarvan er in Nederland servers staan, getapt worden door de NSA? Welke maatregelen ter voorkoming zijn er getroffen? Kan de regering aangeven of deze gegevens nog steeds getapt worden door de NSA?

Ik kan de juistheid van de berichten over het aftappen van SWIFT door de NSA niet bevestigen.
Het is mij bekend dat Eurocommissaris Malmström de Amerikaanse autoriteiten op 12 september jl. per brief om opheldering heeft gevraagd naar aanleiding van de berichtgeving over de het aftappen van SWIFT door de NSA en dat dit onderwerp deel uit maakt van het beraad tussen de VS en de EU. Zie ook het antwoord op de Kamervragen van de leden Koolmees en Schouw(beiden D66) inzake over het bericht dat de servers van de Society for Worldwide Interbank Financial Telecommunication (SWIFT) mogelijk zijn afgetapt door de NSA (publicatiedatum 16 oktober 2013, kenmerk 2013D41109).

6. Heeft de regering zich een beeld gevormd van de economische schade die het bedrijfsleven lijdt door de diefstal van vertrouwelijke gegevens? Zo ja, welke stappen zal de regering hierin nemen?

Het Kabinet heeft geen inzicht in de kwantitatieve economische schade die het bedrijfsleven lijdt door diefstal van vertrouwelijke gegevens. Wel bestaan er diverse inzichten in de kwalitatieve economische schade als gevolg van diefstal van vertrouwelijke gegevens en industriële spionage. In een onderzoek uit 2011 dat is uitgevoerde in opdracht van de Britse overheid[2], wordt de jaarlijkse economische schade in het Verenigd Koninkrijk als gevolg van cybercrime geschat op 27 miljard pond. Dit is een conservatieve schatting; waarschijnlijk is het bedrag hoger en neemt het ieder jaar toe. Industriële spionage neemt 28% (7,6 miljard pond) voor zijn rekening en *identity theft* 6,3% (1,7 miljard pond). Geschat wordt dat het bedrijfsleven 75% van de schade draagt. TNO[3] heeft deze bevindingen geschaald naar de Nederlandse situatie en schat de totale nationale schade als gevolg van cybercrime, met als onderdeel daarvan digitale spionage, op minimaal 10 miljard euro. Binnen dit bedrag neemt industriële spionage ca. 2 miljard euro voor zijn rekening. Het gaat hier om schattingen, de exacte schade is lastig of niet vast te stellen.

---

[2] https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-governmentand-industry-report

[3] http://www.tno.nl/content.cfm?context=thema&content=prop_nieuwsbericht&laag1=897&laag2=920&laag3=115&item_id=2012-04-10 11:37:10.0

De Nederlandse overheid zet in op verschillende vlakken om digitale spionage en diefstal van vertrouwelijke gegevens te voorkomen en te bestrijden:

– De AIVD en de MIVD geven briefings om bewustzijn te creëren bij overheden en het bedrijfsleven voor de dreiging van digitale spionage en geeft advies over informatiebeveiliging.
– Binnen het Nationaal Cyber Security Centrum (NCSC) wordt actief informatie uitgewisseld tussen overheidsdiensten en bedrijfsleven – zoals de vitale sectoren – over (directe) dreigingen en kwetsbaarheden.
– In de Tweede Nationale Cyber Security Strategie (NCSS2) die het kabinet recent heeft aangeboden aan de Tweede Kamer, is een actie opgenomen om een detectie- en responsenetwerk te ontwikkelen. Met dit samenwerkingsverband tussen publieke en private partijen zal een belangrijke stap gezet worden bij het digitaal veiliger en weerbaarder maken van Nederland.
– Het kabinet heeft de Kwetsbaarheidsanalyse Spionage (KWAS) en een bijbehorende handleiding en e-learningmodule laten ontwikkelen. De Handleiding Kwetsbaarheidsonderzoek spionage helpt bedrijven en organisaties zelf onderzoek te doen naar de risico's van spionage.
– Hard- en software zijn kwetsbaar voor cybercriminaliteit; computers met besmette componenten of waar malware is binnengedrongen, worden ook ingezet voor spionage. Naast bewustwordingsprogramma's wordt gewerkt aan de ontwikkeling van een keurmerk voor veilige software.
– De minister van Veiligheid en Justitie heeft als coördinerend minister voor cyber security de nieuwe kabinetsbrede Nationale Cyber Security Strategie aan de Kamer gezonden. Hierin is uitgebreid aandacht voor maatregelen ter verhoging van de algehele weerbaarheid in het digitale domein.

Zie ook het antwoord op de Kamervragen van de leden Schouw en Sjoerdsma (beiden D66) inzake bericht dat Russische spionnen erg actief zijn in Nederland (publicatiedatum 23 mei 2013, kenmerk: 2013D20939).

7. Welke stappen heeft de regering genomen om de voortgaande inbreuken op de privacy tegen te gaan?

Zie het antwoord op vraag 2.

8. Welke diplomatieke stappen neemt de regering doorgaans als van economische spionage sprake is? Heeft de regering die thans ook genomen?

Het kabinet acht enig optreden buiten de kaders van de Nederlandse wet niet aanvaardbaar. Spionage om economische redenen van buitenlandse mogendheden in Nederland, valt hier ook onder. De AIVD en de MIVD doen om die reden structureel onderzoek naar spionage van buitenlandse mogendheden in Nederland.
Indien dergelijke spionage wordt geconstateerd, dan volgen altijd maatregelen, zowel diplomatiek of op andere terreinen.

9. Heeft de regering zelf en in samenwerking met andere landen maatregelen genomen om de landen die zich aan deze inbreuken schuldig maken ertoe te brengen deze te beëindigen?

Zie de antwoorden op vraag 2 en 8.