Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2012–2013

31 145 Wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens)

X

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 11 januari 2013

De vaste commissie voor Veiligheid & Justitie dankt de minister van Veiligheid en Justitie voor zijn brief van 18 april 2011l. Deze brief is een reactie op het verzoek van de commissie om nader geïnformeerd te worden over de beveiliging van gegevens, het waarborgen van de integriteit van gegevens en de gegevensinwinning door opsporingsdiensten. Naar aanleiding daarvan heeft de commissie de minister op 21 juni 2011 een brief gestuurd.

De minister heeft op 19 december 2012 gereageerd.

De commissie brengt bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier van de vaste commissie voor Veiligheid en Justitie,
K. van Dooren

kst-31145-X
ISSN 0921 - 7371
's-Gravenhage 2013

BRIEF AAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Den Haag, 21 juni 2011

De vaste commissie voor Veiligheid & Justitie dankt u voor uw brief van 18 april jl. Deze brief is een reactie op het verzoek van de commissie om nader geïnformeerd te worden over de beveiliging van gegevens, het waarborgen van de integriteit van gegevens en de gegevensinwinning door opsporingsdiensten. Meer in het bijzonder wenste zij nader geïnformeerd te worden over de uitkomsten van de reviews bij drie opsporingsdiensten op ingeleverde «in-control-verklaringen». Dit verzoek had zij gedaan omdat de beveiliging van gegevens en meer in het bijzonder het waarborgen van de integriteit en de exclusiviteit van gegevens, zo'n belangrijke voorwaarde is voor de effectiviteit van de Wet bewaarplicht telecommunicatiegegevens, en ook zo'n belangrijk onderdeel is van de bescherming van de persoonlijke levenssfeer van de personen om wiens gegevens het gaat.

In uw brief van 18 april jl. beperkt u uw reactie tot de uitkomsten van de reviews die betrekking hebben op bevragingen van gegevens via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Niet alle bevragingen lopen echter via het CIOT. Ook is voor de beveiliging van gegevens en het waarborgen van de integriteit van gegevens en gegevensinwinning niet alleen het *proces* van de bevragingen zelf relevant, maar ook de procedures en maatregelen die in de organisaties van de Bijzondere Opsporings-, Inlichtingen- en veiligheidsDiensten (BOID-en) worden ingesteld en getroffen.

Graag vernemen de vaste commissies voor de JBZ-Raad en Veiligheid & Justitie dan ook of de reviews waaraan de minister in zijn brief van 18 april refereert, ook betrekking hebben op de organisatie van de BOID-en en de verwerkingen van persoonsgegevens door de BOID-en zelf. Zo ja, wat zijn de uitkomsten van deze reviews? Zo nee, dan wensen deze commissies nog nader geïnformeerd te worden over de mate waarin de organisatie van de BOID-en en hun verwerkingen van persoonsgegevens voldoen aan de geldende beveiligingsvereisten.

De voorzitter van de vaste commissie voor Veiligheid & Justitie,
A. Broekers-Knol

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 19 december 2012

Hierbij treft u in afschrift mijn brief[1] met bijlage[2] aan die ik de Tweede Kamer stuurde naar aanleiding van het onderzoek van de Inspectie Veiligheid en Justitie en de Departementale Audit Dienst naar het proces en de rechtmatigheid van CIOT-bevragingen bij de politie. De jaarlijkse audits zijn eerder in de vaste commissie voor Veiligheid en Justitie van uw Kamer aan de orde geweest en ik maak graag van de gelegenheid gebruik om, met verontschuldigingen voor de opgelopen vertraging, een openstaande toezegging over dit onderwerp aan uw commissie gestand te doen[3].

Het CIOT beheert een geautomatiseerd informatiesysteem met NAW-gegevens van klanten van telefoon- en internetproviders, dat op vordering van een officier van justitie of een opsporingsambtenaar kan worden bevraagd. Op die manier kan worden achterhaald op wiens naam een specifiek telefoonnummer of een IP-adres staat. Dit systeem zorgt ervoor dat opsporingsdiensten niet langer met alle telecom- en internet-aanbieders contact hoeven op te nemen om na te gaan of een persoon in de klantenbestanden voorkomt, en het leidt ook tot een betere bescherming van de privacy van burgers doordat bedrijven geen kennis krijgen van een opsporingsonderzoek.

De voorzitter van de vaste commissie voor Veiligheid en Justitie heeft bij brief van 21 juni 2011[4] gevraagd of de reviews waar ik in mijn brief van 18 april 2011[5] aan refereer, ook betrekking hebben op de organisatie van de (bijzondere) opsporings-, inlichtingen- en veiligheidsdiensten (hierna BOID-en) en de verwerkingen van persoonsgegevens door de BOID-en zelf. Het antwoord daarop is als volgt. De normen waaraan de BOID-en moeten voldoen bij het bevragen van het CIOT-systeem, stellen inderdaad voorwaarden die direct of indirect gevolgen hebben voor de organisatie. Zo is het systeem alleen toegankelijk voor personen die daarvoor zijn aangewezen en worden er eisen gesteld aan de ruimte van waaruit zij werken. De regels hebben daarnaast ook betrekking op zaken als de faxprocedure bij calamiteiten of de alternatieve werkwijze in geval van een no-hit via het CIOT. De jaarlijkse audits en eventuele reviews richten zich daarmee niet alleen op het bevragingsproces zelf, maar ook op de organisatie van de betrokken diensten. Een samenvatting van de resultaten van de reviews stuurde ik uw Kamer toe met de brief van 18 april 2011. Het meest recente rapport van de Inspectie van Veiligheid en Justitie en de Departementale Audit Dienst treft u als bijlage aan bij de brief aan de Tweede Kamer.

Voor de verwerking van persoonsgegevens geldt dat de Wet politiegegevens, die sinds 2008 van kracht is, elke vier jaar een externe privacy-audit bij de politiekorpsen en bijzondere opsporingsdiensten voorschrijft. Deze vierjaarlijkse audit is eind 2011 conform planning uitgevoerd en ziet toe op de naleving van de regels die als gevolg van die wet van toepassing zijn op het verwerken van politiegegevens. Ook in dit geval is er aandacht voor organisatorische maatregelen die bijvoorbeeld moeten

---

[1] Ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 151917.
[2] Ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 151917.
[3] Toezegging T01063
[4] Kenmerk 145668.05u
[5] Kamerstukken I, 2010/11, 31 145, U

worden getroffen om politiegegevens te beveiligen tegen ongeoorloofde toegang. Naar aanleiding van de privacyaudit over de periode 2008–2011 hebben de korpsen een verbeterplan opgesteld. De toezichthoudende taak ligt bij het College bescherming persoonsgegevens (CBP).

De minister van Veiligheid en Justitie,
I.W. Opstelten