Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

26 643 Informatie- en communicatietechnologie (ICT)

32 761 Verwerking en bescherming persoonsgegevens

Nr. 430

BRIEF VAN DE MINISTERS VAN VEILIGHEID EN JUSTITIE EN VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 december 2016

Hierbij doen wij de toezegging gestand van de Staatssecretaris van Veiligheid en Justitie namens de Minister van Veiligheid en Justitie, op 4 oktober in het vragenuur, om uw Kamer te informeren inzake de berichtgeving in de Volkskrant van 30 september en 1 oktober waarin beweerd wordt dat de telefoon- en chatcommunicatie van duizenden Nederlanders in handen zou zijn gekomen van het Australische technologiebedrijf Appen. In het artikel beweert een oud-medewerker van het bedrijf Appen dat zij in 2010 en 2011 privécommunicatie van duizenden Nederlanders moest verwerken.

Meldingen

Navraag bij de verschillende bedrijven, het Nederlandse Vodafone en het Australische Appen, leert dat beide bedrijven zich niet in de strekking van het artikel herkennen. Daarbij hebben zij aangegeven dat de uitgangspunten en werkwijze van de bedrijven, en de informatie met betrekking tot dit specifieke geval er niet toe hebben geleid dat de bedrijven aanleiding voor melding of aangifte hadden. Voor het persbericht van Vodafone verwijs ik naar hun website.[1] Ook het bedrijf Appen herkent zich niet in het artikel; het bedrijf bevestigt dat zij in die periode in opdracht van een klant meerdere telefonische gesprekken met Nederlanders heeft verwerkt, maar niet zonder toestemming van de geïnterviewde personen. Het zou geautomatiseerde telefoongesprekken betreffen waarbij de respondent erop gewezen wordt dat hij/zij kan ophangen indien niet akkoord met het gesprek.

Het Openbaar Ministerie heeft ook geen aangifte ontvangen. Daarnaast kan de informatie niet afkomstig zijn van het Openbaar Ministerie en de Nationale Politie omdat zij dergelijke informatie niet verstrekken aan bedrijven.

[1] https://www.vodafone.nl/over-vodafone/wie-zijn-wij/nieuws/nieuws.html?post_id=272727

kst-26643-430
ISSN 0921 - 7371
's-Gravenhage 2016

Tevens willen wij u hierbij informeren over (de werkwijze bij) eventuele meldingen van datalekken bij de desbetreffende Nederlandse toezichthouders.

Sinds 1 januari 2016 geldt in Nederland de meldplicht datalekken op grond van de Wet bescherming persoonsgegevens (Wbp). Deze meldplicht houdt in dat verwerkingsverantwoordelijken (zowel bedrijven als overheden) onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra zij een ernstig datalek hebben dat mogelijk ernstige nadelige gevolgen kan hebben voor de bescherming van persoonsgegevens. Het datalek moet ook gemeld worden aan de mensen van wie de persoonsgegevens zijn gelekt, indien het datalek waarschijnlijk ongunstige gevolgen zal hebben voor hun persoonlijke levenssfeer. Ten tijde van de situatie zoals in het artikel wordt beschreven, was de meldplicht op grond van de Wbp in Nederland nog niet van kracht. Wel is in Nederland sinds 5 juni 2012 op grond van de Telecommunicatiewet, ter implementatie van Richtlijn 2009/136/EG van het Europees Parlement en de Raad van de Europese Unie van 25 november 2009 (PbEG L 337), een meldplicht voor datalekken van kracht die geldt voor aanbieders van elektronische openbare communicatienetwerken, zoals telecomproviders. Tot 1 januari 2016 was de Autoriteit Consument en Markt (ACM) de daarvoor bevoegde instantie en sinds die datum de AP. De ACM doet overigens geen uitspraken over specifieke meldingen die bij haar zijn gedaan.

Inlichtingen- en veiligheidsdiensten

Bij de mondelinge vragen is gesuggereerd dat er een mogelijke link zou zijn met inlichtingen- en/of veiligheidsdiensten. De AIVD werkt op grond van de Wet op de Inlichtingen- en veiligheidsdiensten 2002 (Wiv2002). De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) houdt toezicht op de rechtmatigheid van de uitvoering van de werkzaamheden van de AIVD. De rapporten van de CTIVD zijn openbaar en worden de door de betrokken Ministers aan uw Kamer aangeboden.

In het algemeen geldt dat de AIVD continu alert is op signalen van mogelijke activiteiten van buitenlandse diensten in Nederland of gericht tegen Nederlandse belangen. Waar nodig doet de AIVD onderzoek naar deze inlichtingenactiviteiten. Indien wordt geconstateerd dat een buitenlandse mogendheid zonder toestemming inlichtingenactiviteiten verricht op Nederlands grondgebied treft de Nederlandse regering passende en van de situatie afhangende maatregelen.

Tenslotte dient vermeld te worden dat de CTIVD in toezichtrapport 38 uit 2014 vaststelt dat zij geen aanwijzingen heeft gevonden dat de AIVD en de MIVD buitenlandse diensten, bij wijze van U-bochtconstructie, zouden verzoeken gegevens te verzamelen op een manier die henzelf niet is toegestaan.

Wetgeving

Het lid Verhoeven (D66) heeft de Staatssecretaris van Veiligheid en Justitie verzocht kritisch te kijken naar enkele wetsvoorstellen of wetsvoornemens in relatie tot het voorkomen van soortgelijke incidenten waarbij grote hoeveelheden persoonsgegevens terechtkomen bij buitenlandse instanties. Het lid Verhoeven heeft in dit kader de volgende wetsvoorstellen of voorgenomen wetsvoorstellen genoemd: Computercriminaliteit III (Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit), ANPR passagege-

gevens (Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie), aanpassing bewaarplicht telecommunicatiegegevens (Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken) en de implementatie van de PNR-richtlijn. In de genoemde wetsvoorstellen zijn strikte voorschriften opgenomen over welke gegevens mogen worden verzameld en hoe lang deze mogen worden bewaard, strenge regels over de beveiliging van gegevens en ook zijn strikte voorwaarden beschreven waaronder deze gegevens verstrekt mogen worden en voor welke doeleinden. De EU-richtlijn 2016/681 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) schrijft eveneens deze strenge regels voor en deze worden in Nederlandse wet- en regelgeving geïmplementeerd.

Terughalen van gegevens

Het lid Oosenbrug (PvdA) stelde vervolgens in dat verband de vraag hoe het voor Nederlanders mogelijk is om de gegevens terug te halen en *the right to be forgotten* op deze manier werkelijk in te zetten.

Het antwoord op deze vraag hangt af van de wetgeving die op het concrete geval van toepassing is. Op basis van de huidig bekende informatie, kan het antwoord op de gestelde vraag niet anders dan algemeen van aard zijn.

Indien een buitenlands bedrijf een vestiging in Nederland heeft die persoonsgegevens verwerkt, of bij de verwerking van persoonsgegevens gebruik maakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, valt deze verwerking van persoonsgegevens onder de Wet bescherming persoonsgegevens (Wbp, zie artikel 4). In het bericht in de Volkskrant wordt gesuggereerd dat het om een transitie van spraak naar tekst gaat door een bedrijf dat geen vestiging in Nederland heeft – Appen heeft vestigingen in Australië, de Verenigde Staten en de Filipijnen – en bovendien geen middelen heeft gebruikt die zich in Nederland bevinden: de transitieactiviteit zou in Groot-Brittannië hebben plaatsgevonden. Een en ander betekent dat de Wbp op de verwerking van persoonsgegevens bij deze activiteit niet van toepassing zou zijn en in dat geval de Autoriteit Persoonsgegevens ook niet bevoegd zou zijn om op te treden.

Als het bij de transitieactiviteit om een gegevensverwerking zou gaan die wel onder de Wbp zou vallen, dan heeft de betrokken burger een recht op inzage in de verwerkte gegevens (artikel 35) en kan hij deze laten corrigeren (artikel 36). Een recht om de gegevens terug te halen of een *right to be forgotten* heeft betrokkene op grond van de Wbp niet, al is er op grond van jurisprudentie van het Europese Hof van Justitie wel sprake van erkenning van het bestaan van een dergelijk recht.[2] Een *right to be forgotten* heeft de burger in de toekomst ook op grond van de Algemene Verordening Gegevensbescherming. Artikel 17 lid 2 van deze verordening geeft een burger in bepaalde gevallen een recht op gegevenswissing. Verder geeft de verordening een burger in artikel 20 het recht de hem betreffende persoonsgegevens in een gestructureerde, gangbare en door machine leesbare vorm te verkrijgen, maar dit recht geldt alleen als het gegevens betreft die hij zelf aan de verantwoordelijke voor de gegevensverwerking heeft verstrekt en het bovendien om een verwerking gaat waarvoor betrokkene toestemming heeft gegeven of die noodzakelijk is

[2] Arrest van Hof EU van 13 mei 2014 in zaak Google Spain vs AEPD e.a., (ECLI:EU:C:2014:317).

ter uitvoering van een overeenkomst tussen betrokkene en de verantwoordelijke. Als het bij de transitieactiviteit om een gegevensverwerking zou gaan die onder de Wbp zou vallen, kan een burger bij een vermeende inbreuk op die wet op grond van artikel 60 de Autoriteit Persoonsgegevens verzoeken daarnaar een onderzoek in te stellen.

Omdat de beschreven transitieactiviteit in Groot-Brittannië zou zijn verricht is ook de Privacy Act 1998 van het Verenigd Koninkrijk in ogenschouw genomen. Omdat die wet evenals de Wbp op de huidige Europese privacyrichtlijn is gebaseerd, geldt daarvoor in grote lijnen hetzelfde als wat hierboven met betrekking tot de Wbp is vermeld. Dit impliceert dat, als deze transitieactiviteit heeft plaatsgevonden met middelen in het Verenigd Koninkrijk, de Privacy Act daarop van toepassing is. Bij een vermeende inbreuk op die wet kan men zich daar wenden tot de Britse toezichthouder, de Information Commissioner. Van een specifiek recht om gegevens terug te halen of een *right to be forgotten* is echter in deze wet geen sprake, al geldt de erkenning van laatstbedoeld recht door het Europese Hof van Justitie uiteraard ook voor het Verenigd Koninkrijk.

Nu het in de media om een Australisch bedrijf gaat, is tot slot ook gekeken naar de Australische wetgeving. Op basis van de Australische Privacy Act 1988 kan een burger onder bepaalde voorwaarden een klacht indienen bij de Australian Information Commissioner, de Australische toezichthouder op het gebied van privacy, met betrekking tot een vermeende inbreuk op één van de in die wet genoemde *Australian Privacy Principles* door een in Australië gevestigde rechtspersoon. Van een specifiek recht om gegevens terug te halen of een *right to be forgotten* is echter ook in deze wetgeving geen sprake.

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

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