Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

32 761 Verwerking en bescherming persoonsgegevens

Nr. 15 **BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 december 2011

Tijdens het voortgezet algemeen overleg over verwerking en bescherming van persoonsgegevens dat op 17 november 2011 plaatsvond (Handelingen II, 2011.12 nr. 25, behandeling verslag algemeen overleg over de notitie privacybeleid), is een aantal moties ingediend. Op enkele van die moties reageer ik in deze brief. Op de andere moties zal op andere wijze worden gereageerd.

Motie-Van Toorenburg e.a. (Kamerstukken II 2011/12, 32 761, nr. 12)

In deze motie verzoeken de indieners een wetsvoorstel voor te bereiden, inhoudende een plicht om burgers vooraf om toestemming te vragen bij voornemens tot verzameling van gegevens over hun wifirouters (een opt-in-regeling), dan wel de Kamer per brief te informeren welke onoverkomelijke nadelen daaraan verbonden kunnen zijn en die voor de regering reden zijn om van een dergelijk wetsvoorstel af te zien.
In het overleg heb ik aangegeven in een brief uiteen te zetten welke bezwaren ik zie tegen het opstellen van een dergelijke regeling. Ik herinner de Kamer eraan dat de reactie van Google van 15 november 2011 op de opgelegde last onder dwangsom, die de aanleiding tot deze motie vormde, wat mij betreft niet meer en niet minder is dan de reactie van een belanghebbende in een concrete handhavingszaak. Die handhavingszaak staat geheel op zichzelf en is blijkens een mededeling van het College bescherming persoonsgegevens (Cbp) bovendien nog niet afgerond. Ik treed niet in de inhoudelijke beoordeling van die zaak.
De ingediende motie is voor mij aanleiding geweest voor een korte inventarisatie te houden bij het ICT-bedrijfsleven en bij het College bescherming persoonsgegeven om met betrekking tot de verwerking van persoonsgegevens door middel van wifirouters de nodige feiten en achtergronden te verduidelijken. Op grond van die inventarisatie kom ik tot de volgende standpuntbepaling.

kst-32761-15
ISSN 0921 - 7371
's-Gravenhage 2011

Achtergrond

Door middel van wifirouters worden persoonsgegevens van de gebruikers van de router verwerkt. Doordat de elektronische communicatie tussen de router en de randapparatuur langs draadloze weg plaatsvindt, is het voor eenieder die beschikt over een geschikte ontvanger mogelijk de communicatie op te vangen. Ook van de inhoud van de communicatie kan kennis worden genomen, al is dat mede afhankelijk van de gebruikte apparatuur. Ik wijs erop dat dit algemeen bekend is. Gebruikers van wifirouters in openbaar toegankelijke gelegenheden moeten zich daarvan bewust zijn en zij zijn zelf ook medeverantwoordelijk voor het treffen van de juiste beveiligingsmaatregelen wanneer zij willen voorkomen dat anderen kennis kunnen krijgen van hun communicatie.

Een router moet zijn aangesloten op een vast elektronisch communicatienetwerk, omdat de afgewikkelde communicatie grotendeels over een dergelijk netwerk moet plaatsvinden. Dat aspect is uit oogpunt van de bescherming van persoonsgegevens van belang. De locatie van een router verandert doorgaans niet. Een router is bovendien niet persoonsgebonden in die zin dat gegevens van degene op wiens huisadres de router is aanbracht niet met behulp van het apparaat worden verwerkt, of dat die gegevens essentieel zijn voor het functioneren van het apparaat. Persoonsgegevens die via de router worden verwerkt, geven daardoor maar een beperkt beeld van iemands persoonlijke levenssfeer.
Daar komt bij dat veel routers juist zijn geïnstalleerd om kortdurend door een wisselende groep van betrokkenen te worden gebruikt. Het gaat daarbij om de routers waarbij op voor het publiek toegankelijke plaatsen als onderdeel van dienstverlening internettoegang wordt aangeboden, vaak op kosteloze wijze. Ten aanzien van die routers geldt dat de opvang en verwerking van de over de router afgewikkelde communicatie in de regel ook niet leidt tot de weergave van een indringend beeld van de persoonlijke levenssfeer van een of meer specifieke betrokkenen.

Dat ligt anders bij persoonsgegevens die worden verwerkt via een mobiele telefoon of een ander randapparaat met vergelijkbare functies (notebook of iPad). Die geven na ontvangst en verwerking doorgaans een veel indringender beeld vrij van de persoonlijke levenssfeer van de betrokkene, zoals de aanwezigheid van de gebruiker van het apparaat op bepaalde plaatsen, gekoppeld aan bepaalde tijden, het verplaatsingspatroon en de wijze van verplaatsing.

Verwerking van persoonsgegevens

Het Cbp heeft in de besluiten die jegens Google zijn genomen verduidelijkt dat er via de router twee combinaties van gegevens worden verwerkt die moeten worden aangemerkt als persoonsgegevens. De eerste combinatie is de Media Access Control (MAC)-adressen in combinatie met de berekende locatie van de router. De tweede combinatie is die van de Service Set Identifier (SSID), in combinatie met alle gegevens van de eerste combinatie.
Het MAC-adres is een uniek nummer dat de hardware identificeert. Het wordt door de fabrikant van de hardware toegekend. De gebruiker heeft daarop geen invloed. De SSID is de naam van het wifinetwerk. De SSID moet door de gebruiker worden ingesteld. De naam daarvan bepaalt de gebruiker zelf. Dit onderscheid acht het Cbp van groot belang voor de rechtvaardiging van de verwerking van persoonsgegevens.

Voor de eerstbedoelde combinatie geldt in de toepassingspraktijk van de Wet bescherming persoonsgegevens (Wbp) dat de verwerking van deze gegevenscombinatie niet van zodanige aard is, dat dit slechts met

uitdrukkelijke toestemming van de betrokkene gerechtvaardigd is. Het Cbp oordeelt dat voor de rechtvaardiging van de verwerking van de eerste combinatie van gegevens een beroep kan worden gedaan op het zogeheten gerechtvaardigd belang van de verantwoordelijke, bedoeld in artikel 8, onderdeel f, van de Wbp. De verantwoordelijk moet dan wel een afweging maken tussen zijn eigen belang en het belang of de fundamentele rechten en vrijheden van de betrokkene of derden, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer. De verantwoordelijke moet ook overigens voldoen aan de eisen die de Wbp stelt, zoals de welbepaaldheid van het doeleinde van de gegevensverwerking en de verplichting dat doeleinde uitdrukkelijk te omschrijven. Als die belangenafweging correct wordt verricht, zo volgt uit de beoordeling van het Cbp, is het aanbieden van geolocatiegebaseerde dienstverlening met behulp van de gegevenscombinatie rechtmatig.

Voor de tweede combinatie van gegevens heeft het Cbp vastgesteld dat er geen noodzaak bestaat om die gegevenscombinatie te verwerken voor het aanbieden van geolocatiegebaseerde diensten. Uit de besluitvorming door het Cbp vloeit voort dat de verwerking van de tweede combinatie niet gerechtvaardigd kan worden met een beroep op artikel 8, onderdeel f, van de Wbp. Er zal dan moeten worden teruggevallen op een van andere rechtvaardigingsgronden van artikel 8 van de Wbp. Toestemming van de betrokkene is dan een van de mogelijkheden. Het Cbp stelt zich daarnaast op het standpunt dat wanneer via geolocatiegebaseerde dienstverlening op een individuele gebruiker gerichte diensten worden aangeboden waarvan de verwerking van persoonsgegevens deel uitmaakt, eveneens toestemming van de betrokkene noodzakelijk is.

Het Cbp is op grond van artikel 52, tweede lid, van de Wbp een onafhankelijk bestuursorgaan, belast met het toezicht op de naleving van de Wbp. Ik onthoud mij daarom van een beoordeling van de besluiten van het Cbp. Wel acht ik het in deze context van betekenis dat het Cbp zich bij zijn besluitvorming mede heeft gebaseerd op het Advies 13/2001 over geolocatiediensten op slimme mobiele apparaten van 16 mei 2011 (WP 185), afkomstig van de Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens (de Artikel 29 Werkgroep), een onafhankelijk samenwerkingsverband van de privacytoezichthouders uit de EU. (Zie http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.)

Uit de uitleg van het Cbp volgt dat, het aanbieden van geolocatiegebaseerde diensten, mits gebaseerd op de verwerking van de MAC-adressen en de berekende locatie van router, als een rechtmatige vorm van dienstverlening moet worden aangemerkt. Het vaststellen van wettelijke voorschriften die het aanbieden van deze diensten bindt aan de voorwaarde van toestemming van de betrokkene, leidt daarom tot een beperking van de vrijheid die diensten aan te bieden.

Juridische beoordeling

Gegeven de omstandigheid dat de rechtsgrondslag voor verwerking van de gegevens gezocht moet worden in artikel 8, onder f, van de Wbp, zou vaststelling van een wettelijke regeling mede betrekking moeten hebben op een beperking – voor één specifiek doeleinde – van de werking van deze regeling. Dan moet worden beoordeeld of dat in overeenstemming is met artikel 7, onder f, van richtlijn 95/46/EG (de EU-privacyrichtlijn), waarop artikel 8, onder f, van de Wbp is gebaseerd. Artikel 7, onder f, van de EU-privacyrichtlijn geldt als een van de algemene beginselen van die richtlijn. Het Hof van Justitie van de Europese Unie legt deze bepaling zodanig uit «dat de lidstaten aan artikel 7 van richtlijn 95/46 geen nieuwe

beginselen betreffende de toelaatbaarheid van de verwerking van persoonsgegevens mogen toevoegen, noch bijkomende vereisten mogen vaststellen die de reikwijdte van een van de zes in dat artikel vervatte beginselen zouden wijzigen» (HvJEU 24 november 2011, C-468/10 en C-469/10, ASNEF en FECEMID/Spanje, r.o. 32). Het Hof legt in hetzelfde arrest uit dat de beoordelingsmarge die de lidstaten op grond van artikel 5 van de EU-privacyrichtlijn hebben niet mag worden gebruikt om die beginselen te wijzigen, maar alleen om deze nader te bepalen (r.o. 35). Het arrest betrof de uitleg van de Spaanse wettelijke voorschriften tot implementatie van de richtlijn. In die voorschriften was de eis gesteld dat op het gerechtvaardigd belang van de verantwoordelijke, bij gebreke aan toestemming van de betrokkene, slechts een beroep kan worden gedaan wanneer de gegevens zijn opgenomen in voor het publiek toegankelijke bronnen. De richtlijn stelt deze laatste eis niet.
Ik ben met enige uitgebreidheid op dit arrest ingegaan, omdat het stellen van de dwingende eis van toestemming van de betrokkene bij elke verwerking van diens gegevens over voor het publiek beschikbare wifirouters, naar mijn oordeel neerkomt op vrijwel dezelfde schending van de beginselen van de EU-privacyrichtlijn als waarvan in het arrest sprake is. Het komt er dan ook op neer dat het vaststellen van een wettelijke regeling met die inhoud hoogstwaarschijnlijk in strijd met het Europees recht is.

Economische effecten

Verder ben ik van mening dat het aanbod van geolocatiegebaseerde dienstverlening voor de innovatie van grote betekenis is. Ondernemers kunnen deze vorm van dienstverlening uitbouwen met functionaliteiten die gebruikers in staat stellen om op innovatieve wijze in contact te komen met de aanbieders van diensten. Nederland wil graag voorop lopen met het aanbod van innovatieve diensten. Deze dienstverlening moet daarom niet onnodig worden beperkt door het stellen van wettelijke voorschriften. Dat er van het hanteren van de eis van voorafgaande toestemming een beperking uitgaat, lijkt waarschijnlijk. Wanneer het verwerken van persoonsgegevens via wifirouters afhankelijk zou worden gemaakt van de eis van uitdrukkelijke toestemming, betekent dit dat elke eigenaar of exploitant van een router actief een aantal handelingen moet verrichten om de toestemming te verlenen. Afgaande op ervaringen met vrijwillige opt-in-regelingen in andere sectoren, moet dan rekening worden gehouden met een positieve respons van ongeveer 10%. Wanneer 10% van het thans in gebruik zijnde aantal routers gebruikt mag worden voor de verwerking van persoonsgegevens van gebruikers, is het niet mogelijk in Nederland op een zinvolle wijze geolocatiegebaseerde diensten aan te bieden. De innovatie die deze vorm van dienstverlening kan opleveren, gaat daarmee aan Nederland voorbij.
Bovendien wordt in geen enkel ander land in de EU vaststelling van een wettelijke toestemmingseis overwogen. Nederland zou zich met dergelijke voorschriften onnodig van de rest van Europese Unie isoleren.

Samenvattend ben ik van oordeel dat het vaststellen van een wettelijke regeling die de verwerking van persoonsgegevens over publiek toegankelijke wifirouters belemmert juridisch gezien geen begaanbare weg is, en uit economisch oogpunt onverstandig lijkt. Ik zal de totstandkoming van dergelijke wetgeving daarom niet bevorderen.

Motie-Schouw c.s. (Kamerstukken II 2011/12, 32 761, nr. 8)

In deze motie wordt gevraagd om alle elementen van de door de Eerste Kamer aangenomen motie-Franken (Kamerstukken I 2010/11, 31 051, D) waarvoor geen nadere studie nodig is direct uit te voeren.

Voor zover nog nodig herbevestig ik dat de motie-Franken in zijn geheel ten uitvoer wordt gelegd. In het Integraal Afwegingskader voor beleid en regelgeving (IAK) is informatie opgenomen over de motie Franken. Daarnaast is in de negende wijziging van de Aanwijzingen voor de regelgeving die op 11 mei 2011 in werking is getreden de nieuwe aanwijzing 162a opgenomen ter nadere uitwerking van artikel 7 en 8 van de Wet bescherming persoonsgegevens. Deze aanwijzing bepaalt dat in een regeling met bepalingen over de verwerking van persoonsgegevens een welbepaalde en uitdrukkelijke omschrijving van de doeleinden van de gegevensverwerking moet zijn opgenomen. Daarnaast moet de toelichting op de regeling een expliciete afweging bevatten van belangen van verantwoordelijken en betrokkenen in relatie tot die doeleinden Mijn ministerie waakt daarover bij de wetgevingskwaliteitstoetsing van wetsvoorstellen en voorstellen voor algemene maatregelen van bestuur.

Motie-Van der Steur c.s. (Kamerstukken II 2011/12, 32 761, nr. 7)

In deze motie dringt de Kamer in Europees verband aan op een gezamenlijke regeling voor de bescherming van gegevens.

Ik zie deze motie als een aansporing dit belang met nadruk te betrekken bij de komende herziening van het Europees gegevensbeschermingsrecht. Eind januari 2012 verwacht ik daarvoor de voorstellen van de Europese Commissie. U zult van die voorstellen op de gebruikelijke wijze op de hoogte worden gebracht door de Commissie. Ook zult u zo spoedig mogelijk daarna het gebruikelijke BNC-fiche ontvangen met een eerste beoordeling van mijn kant.

De staatssecretaris van Veiligheid en Justitie,
F. Teeven