Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

217

Vragen van de leden **Van den Berg** en **Van Dam** (beiden CDA) aan de Ministers van Justitie en Veiligheid, voor Rechtsbescherming en de Staatssecretaris van Economische Zaken en Klimaat over *het bericht «Apple deelde herleidbare, persoonlijke gegevens bij opnames Siri-gebruikers»* (ingezonden 15 augustus 2019).

Antwoord van Minister **Dekker** (Rechtsbescherming), mede namens de Minister van Justitie en Veiligheid en de Staatssecretaris van Economische Zaken en Klimaat (ontvangen 2 oktober 2019) Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3818

Vraag 1
Bent u bekend met het bericht «Apple deelde herleidbare, persoonlijke gegevens bij opnames Siri-gebruikers»?[1]

Antwoord 1
Ja, ik ben bekend met dit bericht.

Vraag 2
Waren de signalen uit het bericht, over vermeende schending van de privacy door Apple, al eerder bekend bij de Autoriteit Persoonsgegevens, die toezicht houdt op het gebruik van persoonsgegevens door organisaties?

Antwoord 2
Het fenomeen van afluisteren via smart speakers was bij de Autoriteit Persoonsgegevens (hierna: AP) bekend.

Vraag 3
Heeft de Autoriteit Persoonsgegevens actie(s) ondernomen richting Apple nadat vorige maand al naar buiten kwam dat Apple-medewerkers meeluisteren naar persoonlijke informatie van gebruikers, zoals medische gegevens?[2] Zo ja, welke actie(s)?

[1] NOS, 6 augustus 2019, https://nos.nl/artikel/2296594-apple-deelde-herleidbare-persoonlijke-gegevens-bij-opnames-siri-gebruikers.html.
[2] NOS, 29 juli 2019, https://nos.nl/artikel/2295635-apple-luistert-mee-naar-seks-drugsdeals-en-medische-informatie-via-siri.html.

ah-tk-20192020-217
ISSN 0921 - 7398
's-Gravenhage 2019

Antwoord 3
De Algemene Verordening Gegevensbescherming (hierna: AVG) kent het zogeheten één-loketmechanisme. Dit houdt in dat organisaties die grensoverschrijdende verwerkingen van persoonsgegevens uitvoeren nog maar met één privacytoezichthouder zaken hoeven te doen. Die wordt de «leidende toezichthouder» genoemd. De Ierse privacytoezichthouder is de leidende toezichthouder voor Apple. De AP is zogeheten «betrokken toezichthouder». Ik heb begrepen van de AP dat zij regulier contact heeft met de Ierse privacytoezichthouder, zowel bilateraal als binnen de (*European Data Protection Board* (EDPB) en dat de Ierse privacytoezichthouder op de hoogte is van deze kwestie (evenals vergelijkbare recente kwesties). De AP heeft overigens de mogelijkheid om kwesties onder de aandacht te brengen van de leidende toezichthouder als deze daarvan nog niet op de hoogte is.

Vraag 4
Deelt u de mening dat, indien de berichtgeving klopt, het zeer kwalijk is dat herleidbare, persoonlijke gegevens, afkomstig van gebruikers van in dit geval een spraakherkenningssysteem, worden gedeeld met derden?

Antwoord 4
Het delen van persoonsgegevens met derden is niet per definitie een kwalijke zaak. Het is van belang dat bedrijven binnen de geldende wet- en regelgeving persoonsgegevens kunnen delen met derde partijen, zodat zij deze gegevens kunnen analyseren om bepaalde producten of bedrijfsprocessen te optimaliseren.
Blijkens de berichtgeving en de reactie die Apple daarop heeft gegeven zijn er, naast de opnamen van de gesprekken, ook gegevens meegestuurd die maken dat de opnames herleidbaar werden tot een specifiek natuurlijk persoon, waardoor er sprake is van verwerking van persoonsgegevens. Indien deze verwerking zonder juiste rechtsgrondslag plaatsvindt -zoals de berichtgeving suggereert- dan is dat niet alleen kwalijk, maar ook onrechtmatig.

Vraag 5
Is bij het op deze wijze delen van persoonsgegevens volgens u sprake van inbreuk op de privacy?

Antwoord 5
De privacy van personen kan worden geraakt wanneer er op onrechtmatige wijze persoonsgegevens worden gedeeld. Het is echter aan de AP om te bepalen of de verwerking van persoonsgegevens in kwestie onrechtmatig was.

Vraag 6
Kunt u – in het kader van de juridische bescherming van burgers – uitleggen welke regelgeving hier primair van toepassing is? Is dat de Algemene verordening gegevensbescherming (inclusief alle daarbij behorende wet- en regelgeving) of is dat het Wetboek van Strafrecht, in het bijzonder de artikelen 139a en volgende? Tot welke instantie zouden burgers en/of bedrijven zich primair moeten richten bij (vermeende) situaties van stiekem afluisteren zoals bedoeld in deze Kamervragen, de Autoriteit Persoonsgegevens dan wel de politie en/of het openbaar ministerie?

Antwoord 6
De AVG betreft de relevante regelgeving om het gedrag van Apple aan te toetsen. De kernvraag daarbij is of Apple zich kan beroepen op een geldige verwerkingsgrondslag als bedoeld in artikel 6, eerste lid van de AVG. De uiteindelijke beoordeling van deze vraag in een feitelijke situatie is aan de bevoegde toezichthoudende autoriteit.
Nederlandse ingezetenen kunnen bij de AP een klacht indienen over de wijze waarop een verwerkingsverantwoordelijke omgaat met jouw persoonsgegevens. De AP is vervolgens op grond van de AVG verplicht om ofwel zelf deze klacht in behandeling te nemen of deze door te sturen naar de leidende toezichthouder in Ierland. De Ierse toezichthouder treedt in overleg met de andere betrokken toezichthouders. Als zij van mening zijn dat er sprake is van onrechtmatige verwerking van persoonsgegevens, dan kunnen er verschil-

lende maatregelen worden getroffen, waaronder het opleggen van een bestuurlijke boete (waarbij deze boete kan oplopen tot 20.000 euro of voor een onderneming tot 4% van de totale wereldwijde jaaromzet in het voorafgaande boekjaar). De Ierse toezichthouder stuurt vervolgens zijn besluit naar de AP en de AP zorgt voor doorgeleiding aan de Nederlandse klager. Als deze niet tevreden is over de klachtafhandeling of het besluit van de Ierse toezichthouder, dan kan de betrokkene in Nederland in bezwaar gaan en uiteindelijk beroep instellen bij de Nederlandse bestuursrechter.
Het heimelijk afluisteren van gesprekken is in het Nederlandse Wetboek van Strafrecht strafbaar gesteld in de artikelen 139a en verder. Bij de vraag of sprake is van strafbare handelingen is onder meer van belang waar de desbetreffende handelingen hebben plaatsgevonden en of aan alle bestanddelen van de strafbaar gestelde handeling is voldaan. Het is aan het Openbaar Ministerie en in voorkomend geval de strafrechter om hierover te oordelen.

Vraag 7
Bent u bereid Apple om een reactie op de berichtgeving te vragen, daar het bedrijf dat afgaande op het artikel van de NOS tot dusver niet heeft willen doen?

Antwoord 7
Apple heeft inmiddels een reactie op de berichtgeving op zijn eigen website geplaatst. Die houdt, kort gezegd, in dat het bedrijf voorlopig geen audio opnames meer beluistert, maar alleen computer gegenereerde transcripties van gesprekken verwerkt. Na een software-update zal Apple het beluisteren van audiofragmenten voortzetten, maar alleen van betrokkenen die zich hier vrijwillig voor hebben aangemeld. Het beluisteren van de fragmenten zal alleen worden gedaan door medewerkers van Apple. Deze medewerkers zullen onbedoelde Siri-aanvragen direct verwijderen.

Vraag 8
Bent u bereid van Apple te eisen dat het bedrijf per direct maatregelen neemt om de privacy van gebruikers van zijn producten/diensten, waaronder spraakherkenning, te waarborgen? Welke (juridische) mogelijkheden hebt u daartoe?

Antwoord 8
Het is aan de bevoegde privacytoezichthouders in de EU om een onderzoek te starten naar het handelen van Apple. Indien er onderzoek wordt gedaan, is het wederom aan de desbetreffende toezichthouder om op basis van dat onderzoek te bepalen of Apple al dan niet maatregelen dient te nemen. Het is dan ook niet aan het kabinet om een dergelijk verzoek aan Apple te richten, noch om eisen te stellen aan het handelen van Apple.
Overigens heeft Apple in zijn reactie wel aangegeven dat het een aantal maatregelen heeft genomen en nog zal nemen, zie daarvoor het antwoord op vraag 7.

Vraag 9
Wijzen incidenten als die bij Apple, maar ook bij andere techbedrijven, volgens u op het bestaan van een «privacyprobleem» in deze sector?

Antwoord 9
Het feit dat zich een aantal incidenten bij verschillende bedrijven heeft voorgedaan, wijst niet direct op een «privacyprobleem» in de gehele sector. Specifieke incidenten met het analyseren van spraakgegevens voor productverbetering wijzen er wel op dat er meerdere bedrijven lijken te zijn die hierbij niet binnen de wettelijke kaders zijn gebleven. Gelet op hun onafhankelijkheid, is het aan de verschillende Europese toezichthouders zelf om te bepalen of zij ambtshalve optreden tegen bedrijven die de fout in gaan en hoe zij met eventuele klachten van betrokkenen omgaan.

Vraag 10
Bent u van mening dat wet- en regelgeving op dit moment voldoende toereikend zijn om de privacy van consumenten van techproducten en -diensten te beschermen? Waar schiet deze wet- en regelgeving mogelijk nog tekort?

Antwoord 10
De wet- en regelgeving acht ik op dit moment in het algemeen inderdaad toereikend om de privacy van consumenten van techproducten en -diensten te beschermen.
In lijn met de kabinetsvisie op horizontale privacy ziet het kabinet in dit verband evenwel twee onderwerpen waar het juridisch kader mogelijk nog tekortschiet en die het kabinet aan de orde wil stellen bij de evaluatie van de AVG, die uiterlijk mei 2020 moet zijn afgerond.[3]
Ten eerste is het kabinet van mening dat grote techbedrijven, ook als zij rechtmatig handelen, enorme hoeveelheden gegevens kunnen verzamelen en gebruiken. Het kabinet wil kijken of de hoeveelheid gegevens die deze bedrijven verzamelen, kan worden beteugeld. Ten tweede wil het kabinet dat wordt geëvalueerd of de normen uit de AVG wel voldoen om de risico's van profilering tegen te gaan, specifiek wanneer profilering leidt tot prijsdiscriminatie of zelfs tot uitsluiting van bepaalde groepen voor sommige producten of diensten.

Vraag 11
Wat kunt u doen om consumenten van techproducten en -diensten beter bewust te maken van de risico's die zij lopen bij het gebruik ervan ten aanzien van privacy, maar bijvoorbeeld ook spionage (via zogeheten «spyware»)?

Antwoord 11
Het kabinet vindt het belangrijk om het privacybewustzijn van burgers te vergroten en zal daarom in het voorjaar van 2020 een publiekscampagne starten over de privacyrisico's bij het gebruik van digitale applicaties. In deze campagne wordt aandacht besteed aan de risico's die burgers lopen als ze persoonlijke data delen.
Verder werkt Tilburg University aan een rapport over eventuele verdere regulering van «spyware» en de vermindering van de privacyrisico's die aan deze producten kleven. Dit rapport wordt in het voorjaar van 2020 verwacht en zal hopelijk inzichtelijk maken in hoeverre er verdere maatregelen genomen moeten worden om de privacyrisico's bij deze producten verder in te dammen.[4]

[3] Kamerstuk 34 926, nr. 8, p. 10.
[4] Kamerstuk 34 926, nr. 8, p. 11.