Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

**Aanhangsel van de Handelingen**

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

## 575

Vragen van het lid **Verhoeven** (D66) aan de Minister van Economische Zaken over *het bericht dat het CBP pleit voor het inhoudelijk analyseren van dataverkeer* (ingezonden 17 september 2014).

Antwoord van Minister **Kamp** (Economische Zaken) (ontvangen 12 november 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2014–2015, nr. 241

Vraag 1
Bent u bekend met het bericht «CBP: providers mogen dataverkeer klanten inhoudelijk analyseren»?[1]

Antwoord 1
Ja.

Vraag 2, 3 en 5
Wat vindt u van de oproep van het College Bescherming Persoonsgegevens (CBP) om providers dataverkeer inhoudelijk te laten analyseren en opslaan?
Is het waar dat het CBP pleit voor Deep Packet Inspection (DPI) om inzicht in dataverbruik te verkrijgen?
Wat vindt u ervan dat een instantie die erop toeziet dat persoonsgegevens zorgvuldig worden gebruikt en beveiligd en dat privacy gewaarborgd blijft, voor een dergelijk privacygevoelig plan pleit? Vindt u dat een dergelijke oproep past bij de missie van het CBP? Heeft u contact gehad met CBP alvorens het de uitspraken deed?

Antwoord 2, 3 en 5
Tijdens de uitzending van het tv-programma Radar (d.d. 15 september jl.) heeft de voorzitter van het CBP gezegd dat de wet verplicht om klanten inzage te geven in persoonsgegevens die een telecomaanbieder over hen bewaart. Het CBP meldde nadien in een persverklaring dat aanbieders gegevens over het dataverkeer voor facturering en netwerkbeheer in een beperkt aantal gevallen zonder toestemming mogen bewaren, mits deze gegevens niet langer worden bewaard dan noodzakelijk. Daarna moeten de gegevens zo snel mogelijk worden geanonimiseerd of verwijderd. Voorts verklaarde het CBP dat aanbieders bepaalde gegevens zoals welke websites

[1] Tweakers, 15 September 2014, http://tweakers.net/nieuws/98464/cbp-providers-mogen-dataverkeer-klanten-inhoudelijk-analyseren.html

ah-tk-20142015-575
ISSN 0921 - 7398
's-Gravenhage 2014

of apps (op het niveau van domeinnamen) op welk moment hoeveel data hebben verbruikt, langer mogen bewaren als de klant daar vooraf uitdrukkelijke toestemming voor geeft. Tot slot meldde het CBP dat het zonder toestemming gebruiken van gegevens over bezochte websites en gebruikte apps voor eigen doeleinden van de telecomaanbieders, zoals voor marktanalyses, in strijd met de wet is. Het is mij niet bekend dat de voorzitter van het CBP zich tijdens het tv-programma zou hebben uitgelaten over of gepleit heeft voor een techniek (zoals DPI) om inzicht in dataverbruik te geven. Het CBP is een onafhankelijk bestuursorgaan dat toezicht houdt op de naleving van de wetten inzake het gebruik van persoonsgegevens. Het CBP heeft deze oproep in die context gedaan.

Vraag 4
Bent u van mening dat de opslag van data over gebruik van websites en apps door middel van DPI tot schendingen van privacy kan leiden?

Antwoord 4
Ja, het analyseren van verkeersgegevens (bijvoorbeeld via DPI) kan leiden tot schending van privacy, namelijk in het geval er geen voorafgaande toestemming is verkregen voor het analyseren. Het is de abonnee zelf die de afweging kan maken tussen zijn privacy en het inzetten van een dergelijk instrument voor beter inzicht in zijn dataverbruik. Inmiddels zijn er alternatieven om dataverbruik te analyseren (zie antwoord op vraag 6).
Ik hecht er sterk aan dat de persoonlijke levenssfeer, het gebruik en opslag van persoonsgegevens en de vertrouwelijkheid van elektronische communicatie beschermd en gerespecteerd worden. De telecomaanbieders zijn gebonden aan wettelijke kaders zoals de Telecommunicatiewet (Tw), de Wet bescherming persoonsgegevens (Wbp) en het Wetboek van Strafrecht. Ongeacht de techniek moet de telecomaanbieder zich houden aan vigerende wet- en regelgeving.
Zo moeten organisaties op grond van de Wbp persoonsgegevens op behoorlijke en zorgvuldige wijze verwerken en opslaan. Bovendien mogen persoonsgegevens alleen worden verzameld voor welbepaalde, duidelijk omschreven en gerechtvaardigde doeleinden en mogen ze niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
Voor wat betreft de verkeersgegevens, dat wil zeggen de door de aanbieders voor het overbrengen van communicatie over elektronische communicatienetwerken verzamelde en verwerkte gegevens, geldt als hoofdregel dat deze verwijderd dan wel geanonimiseerd moeten worden zodra de verkeersgegevens niet langer nodig zijn ten behoeve van de overbrenging van communicatie (artikel 11.5 Tw). Wel mogen de aanbieders conform het tweede lid zonder toestemming verkeersgegevens verwerken die noodzakelijk zijn voor facturering tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden afgedwongen. Voor het opmaken van een factuur aangaande de mobiele internettoegang is in beginsel de hoeveelheid gebruikte data van belang en niet hoe deze data is verbruikt. Gezien het feit dat de aanbieder voor het opmaken van een factuur geen aanvullende gegevens nodig heeft, mogen aanbieders op basis van artikel 11.5, tweede lid Tw geen aanvullende gegevens verwerken. Verkeersgegevens, zoals bezochte websites, moeten derhalve in beginsel verwijderd of geanonimiseerd worden nadat de verbinding met het internet is verbroken. De aanbieders zijn wel verplicht hun abonnees of gebruikers in kennis te stellen over verkeersgegevens die worden verwerkt en de duur van de verwerking (artikel 11.5 lid 4 Tw). De maximale opslagtermijn die geldt voor de opslag van gegevens voor facturering is vijf jaar (artikel 3:307 BW). Verder is de zogenoemde «bewaarplicht gegevens telecommunicatie» van toepassing (artikel 13.2a Tw). Dit houdt in dat een set verkeers- en locatiegegevens (zoals bepaald in de bij hoofdstuk 13 van de Tw opgenomen bijlage) ten behoeve van de opsporing en vervolging van strafbare feiten zes maanden (internet) of twaalf maanden (telefonie) bewaard dienen te worden. Na verloop van die termijn moeten deze gegevens worden vernietigd.
Voorts voorziet het via een amendement van uw Kamer opgenomen artikel 11.2a (Kamerstukken 2010–2011, 32 549, nr. 16) in aanvullende waarborgen met betrekking tot het vertrouwelijke karakter van de communicatie en de daarmee verband houdende gegevens die via openbare communicatienetwer-

ken en diensten worden doorgegeven. Het tweede lid van deze bepaling bevat een algemeen verbod op onder meer het analyseren met of zonder opslag van de communicatie, behalve in het geval dat specifiek omschreven uitzonderingen van toepassing zijn. In dat kader is het tweede lid onder a van belang. Op grond van deze uitzonderingsgrond heeft de abonnee de vrijheid er voor te kiezen dat diens communicatie (zoals data over gebruik van websites en apps) wordt geanalyseerd, bijvoorbeeld via DPI. Voor deze handelingen is in elk geval uitdrukkelijke toestemming van de betrokken abonnee vereist krachtens dat onderdeel. Verder dient de aanbieder voorafgaand aan het verkrijgen van toestemming de abonnee te voorzien van informatie over de gegevens die worden verwerkt, de doeleinden waarvoor de gegevens worden verwerkt en de duur van de verwerking. Dit betekent dus dat een aanbieder na het ontvangen van een klacht van een abonnee die een hoge rekening heeft gekregen als gevolg van onverklaarbaar hoog dataverbruik, dit datagebruik niet achteraf kan analyseren. Immers indien de abonnee hiervoor geen toestemming heeft verleend voorafgaand aan de betrokken periode, is de betreffende data niet beschikbaar. Slechts toekomstig datagebruik kan, na uitdrukkelijke toestemming van de abonnee, worden geanalyseerd. Hierbij moet worden aangetekend dat de abonnee diens toestemming op elk moment kan intrekken.

Vraag 6
Bent u bereid alternatieven voor DPI te onderzoeken om datagebruik bij te houden?

Antwoord 6
De markt speelt actief in op een groeiende vraag naar manieren om dataverbruik lokaal op het mobiele apparaat bij te kunnen houden. Los van het feit dat de hedendaagse smartphones via instellingen het datagebruik per app kunnen tonen, zijn er diverse datateller-apps in online stores te vinden die op een gemakkelijke manier het datagebruik in de gaten kunnen houden en waarmee bovendien alarmlimieten ingesteld kunnen worden. Daarom zie ik geen reden om onderzoek te verrichten naar alternatieven voor DPI.