Openbaar

Kenmerk: OPTA/ACNB/2011/201469
Datum: 30 juni 2011

Voorlopige bevindingen OPTA over gebruik van Deep Packet Inspection door aanbieders van mobiele telefonienetwerken

Aanleiding

Medio mei 2011 kwam in het nieuws dat enkele aanbieders van mobiele telecommunicatienetwerken gebruik maken van technieken waarmee deze aanbieders op diepgaand niveau datapakketten analyseren die over hun mobiele netwerk getransporteerd worden. Deze technieken, die doorgaans aangeduid worden met de term Deep Packet Inspection (hierna: DPI), zouden inbreuk kunnen maken op de persoonlijke levenssfeer van gebruikers van die netwerken. Sommige berichten in de media spreken van het afluisteren van abonnees door hun netwerkaanbieder.

Het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna: het college) heeft daarop besloten een onderzoek te doen naar de gedragingen van aanbieders van mobiele telecommunicatienetwerken op grond van zijn bevoegdheden die volgen uit de Telecommunicatiewet (hierna: Tw).

Het onderwerp is ook in de Tweede Kamer aan de orde geweest en Minister Verhagen heeft over het gebruik van DPI op 1 juni 2011 Kamervragen beantwoord.[1]

Onderzoeksvraag

Het college is met de minister[2] van oordeel dat het gebruik van DPI-technieken wettelijke beperkingen kent. Het betreft hier met name wet- en regelgeving ter bescherming van persoonsgegevens en ter bescherming van de persoonlijke levenssfeer. Het analyseren van een deel van de inhoud van datapakketten kan noodzakelijk zijn voor netwerkaanbieders in het kader van bijvoorbeeld internetveiligheid.[3] De inzet van DPI-technieken om bijvoorbeeld spyware tegen te gaan draagt dan bij aan de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees. Daarentegen kunnen bepaalde vormen van DPI of bepaalde doelstellingen van het gebruik van DPI juist strijdig zijn met de genoemde wet- en regelgeving.

Het college richt zijn onderzoek op de vraag of de manier waarop mobiele netwerkaanbieders datapakketten analyseren strijdig is met bepalingen uit de Tw waarop het college bevoegd is toe te zien. Het college heeft daarbij de volgende onderzoeksvragen gehanteerd:

1. Gebruiken de netwerkaanbieders technieken om datapakketten die over hun mobiele netwerken getransporteerd worden te analyseren of te laten analyseren naar gegevensstromen dan wel applicaties? Zo ja:
2. Waarom doen deze netwerkaanbieders dat?
3. Op welke wijze worden de datapakketten geanalyseerd?
4. Is dat strijdig met de bepalingen uit de Telecommunicatiewet waarop OPTA toezicht houdt?

---

[1] http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/06/01/brief-aan-de-tweede-kamer-over-deep-packet-inspection.html.

[2] Idem.

[3] Dit wil niet zeggen dat in alle gevallen per definitie ook van de boodchap van de communicatie kennis hoeft te worden genomen.

Wettelijke bepalingen waarop OPTA toezicht houdt

Het college houdt op grond van artikel 15.1, derde lid van de Telecommunicatiewet (hierna: Tw) toezicht op de naleving van een aantal bepalingen die tot doel hebben persoonsgegevens en de persoonlijke levenssfeer te beschermen. Dat zijn artikel 18.13, artikel 11.2 en artikel 11.3 Tw, die verplichtingen opleggen aan aanbieders van openbare elektronische communicatiediensten en –netwerken, waaronder dus de mobiele netwerkaanbieders.

Privacy en communicatiegeheim:
Artikel 18.13, eerste en tweede lid Tw verplichten (kort gezegd) aanbieders om bij hun bedrijfsvoering in acht te nemen het belang van de bescherming van persoonsgegevens, de bescherming van de persoonlijke levenssfeer, de bescherming van het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken.

Zorgplicht:
Artikel 11.2 Tw verplicht (kort gezegd) aanbieders om zorg te dragen voor de bescherming van persoonsgegevens en de bescherming van persoonlijke levenssfeer van abonnees en gebruikers van hun netwerk, onderscheidenlijk hun dienst.

Beveiligingsplicht:
Artikel 11.3, eerste lid, Tw verplicht (kort gezegd) aanbieders om passende technische en organisatorische beveiligingsmaatregelen te nemen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers.

Andere relevante wettelijke bepalingen

Ook de Wet bescherming persoonsgegevens (hierna: Wbp) bevat relevante bepalingen voor de onderzoeksvraag van het college, maar voor die bepalingen is het College Bescherming Persoonsgegevens (hierna: het CBP) de toezichthoudende instantie. Met het CBP is een samenwerkingsprotocol van kracht om, wanneer beide toezichthouders op basis van hun eigen bevoegdheid bevoegd zijn toezicht te houden, in concrete gevallen het toezicht af te stemmen.

In artikel 139c van het Wetboek van Strafrecht is bepaald dat het afluisteren, aftappen of opnemen van elektronische communicatie op enkele uitzonderingen na verboden is.[4]

Onderzoeksaanpak

Het college heeft zich in het kader van dit onderzoek (quick scan) beperkt tot het stellen van schriftelijke vragen aan de aanbieders van mobiele telecommunicatienetwerken. De antwoorden zijn in afzonderlijke gesprekken met de aanbieders doorgesproken. Bij elk van die gesprekken is om nadere schriftelijke toelichting gevraagd en die hebben de aanbieders elk verstrekt.

Op basis van de op deze manier verkregen informatie bepaalt het college of er op bepaalde gebieden nader onderzoek noodzakelijk is of handhavend opgetreden dient te worden.

[4] Artikel 139d van het WvSr bepaalt verder dat het treffen van voorbereidingen om wederrechtelijk af te kunnen tappen eveneens strafbaar is.

Bevindingen

Het college stelt vast dat alle onderzochte mobiele netwerkaanbieders in meer of mindere mate technieken gebruiken om datapakketten te monitoren en te analyseren die over hun mobiele netwerken getransporteerd worden. Daarbij worden gegevensstromen en applicaties geïdentificeerd en daarvoor vindt de analyse soms op diep niveau plaats. Een analyse op diep niveau houdt in dit verband in dat meer dan alleen de header van een datapakket bekeken wordt door de aanbieder.

Elke aanbieder heeft daarbij op eigen wijze toegelicht dat dit gebeurt met het oog op het zo goed mogelijk afwikkelen van het verkeer en het optimaliseren van de dienstverlening.

Privacy en communicatiegeheim (artikel 18.13 Tw)
Het college heeft in zijn onderzoek geen aanwijzingen gevonden dat de onderzochte aanbieders de mails van hun abonnees lezen, verstuurde foto's bekijken, of bijdragen op sociale netwerken lezen. De aanbieders hebben ook verklaard dit niet te doen. Maar het college stelt tegelijkertijd vast dat aanbieders kennis nemen van meer informatie dan alleen de informatie die is bestemd voor de afhandeling van het berichtenverkeer. Het is vooralsnog de vraag of het kennisnemen van deze informatie een inbreuk op artikel 18.13 Tw oplevert.

Om deze vraag te beantwoorden, dient niet alleen beoordeeld te worden of het communicatiegeheim wordt geschonden, maar dienen ook de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer beoordeeld te worden. Het zwaartepunt van die beoordeling ligt bij het CBP. Het CBP en het college hebben hierover overlegd. Op grond van het samenwerkingsprotocol is besloten dat het college zijn bevindingen en de onderzoeksgegevens over de naleving van artikel 18.13 Tw ter beschikking stelt aan het CBP. Het CBP zal deze bevindingen en de onderzoeksgegevens betrekken bij zijn onderzoek naar de naleving van de Wbp en de verwerking van persoonsgegevens bij de inzet van DPI-technieken.

Mede in het licht van de onderzoeksresultaten van het CBP houdt het college de mogelijkheid open om nader onderzoek te doen in verband met het bepaalde in 18.13 Tw.

Beveiligingsplicht (artikel 11.3 Tw)
Bij alle vormen van communicatie over elektronische communicatienetwerken bestaat altijd het risico dat kennis wordt genomen van de inhoud ervan, hetzij bedrijfsmatig, hetzij incidenteel door een gebrekkige beveiliging. Dat is een risico dat niet uitsluitend geldt voor communicatie die overgebracht wordt via mobiele datanetwerken. Bij zijn onderzoek heeft het college kennis genomen van de verklaringen van de mobiele netwerkaanbieders over de organisatorische en technische maatregelen die zij hebben getroffen ter bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in algemene zin. Er is op basis daarvan voor het college geen aanleiding om specifiek de aanbieders die over mobiele netwerken beschikken aan zwaarder toezicht te onderwerpen dan andere aanbieders van elektronische communicatiediensten. Het college voert hierbij met name toezicht uit indien hij signalen ontvangt dat een aanbieder tekort zou schieten in het nemen van organisatorische en technische maatregelen.

Zorgplicht (artikel 11.2 Tw)
Het is voor het college nog niet duidelijk of de inzet van de door de aanbieders gebruikte analysemiddelen en de daarbij verwerkte gegevens in alle gevallen gerechtvaardigd en proportioneel is in het licht van de zorgplicht van artikel 11.2 Tw. Met andere woorden, het college vraagt zich af hoe de hoeveelheid en de soort gegevens die de aanbieders verwerken en analyseren zich verhouden tot de plicht die de aanbieders hebben om zorg te dragen voor de bescherming van de persoonsgegevens en de persoonlijke levenssfeer van de abonnees. Daarvoor is nader onderzoek nodig.

Het is daarbij van belang dat artikel 11.2 Tw nauw samenhangt met het bepaalde in de Wet bescherming persoonsgegevens, waarop het CBP toeziet. Het CBP en het college hebben hierover overlegd. Op grond van het samenwerkingsprotocol is besloten dat het college zijn bevindingen en de onderzoeksgegevens naar de naleving van artikel 11.2 van de Tw ter beschikking stelt aan het CBP. Het CBP zal deze bevindingen en de onderzoeksgegevens betrekken bij zijn onderzoek naar de naleving van de Wbp en de verwerking van persoonsgegevens bij de inzet van DPI-technieken.

Conclusies

1. Op basis van het bovenstaande is er in het kader van de Tw voor het college in dit stadium van het onderzoek geen aanleiding voor handhavend optreden tegen de onderzochte aanbieders van mobiele netwerken.
2. Het college zal de bevindingen en de onderzoeksgegevens ter beschikking stellen aan het CBP, die deze betrekt bij zijn onderzoek naar de naleving van de Wbp.
3. Het college zal in het vervolg van zijn onderzoek ook de onderzoeksresultaten van het CBP betrekken en indien nodig handhavend optreden.