TELECOMMUNICATIERECHT

AAK20137303

N.A.N.M. van Eijk

Wet- en regelgeving

De herziening van de regels over het plaatsen van *cookies* is in een volgende fase beland. De minister van Economische Zaken is een consultatie gestart over een voorontwerp van wet, dat de regels moet verruimen en de interpretatie van bestaande regels verheldert (*Kamerstukken II*, 2012/13, 24 095, nr. 344). Bij analytische cookies die alleen worden toegepast om het gebruik van de website in kaart te brengen en te analyseren, is volgens het voorontwerp niet nodig dat toestemming wordt verkregen van gebruikers. De privacyimplicaties van dit soort *cookies* zijn gering. Gaat het om meer dan geringe gevolgen voor de privacy, dan blijft toestemming vereist. Voor *tracking cookies*, die het individueel surfgedrag registeren ten behoeve van profileren, verandert er dus niets. Ten aanzien van het toestemmingsvereiste wordt aangegeven dat toestemming nimmer kan worden afgeleid uit het uitblijven van een handeling. Een actieve handeling blijft vereist. Van een dergelijke actieve handeling zou bijvoorbeeld sprake kunnen zijn wanneer een website duidelijk aangeeft dat het aanklikken van een bepaalde link of onderdeel van

de website wordt beschouwd als het instemmen met het plaatsen van *cookies*. Volgens de minister zou het CBP deze interpretatie onderschrijven.

Artikel 13a van de Telecommunicatiewet regelt een meldplicht voor aanbieders van openbare telecommunicatienetwerken- en diensten inzake datalekken. Het moet daarbij gaan lekken die nadelige gevolgen hebben voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst. Het gaat dus uitsluitend om lekken bij de betreffende aanbieders. Lekken bij aanbieders van bijvoorbeeld informatiediensten (denk aan persoonsgegevens bij webwinkels) of banken (creditcardgegevens en dergelijke) vallen buiten het bereik van deze bepaling. De lekken moeten worden gemeld aan de toezichthouder en aan eindgebruikers wanneer er sprake is van ongunstige gevolgen voor de persoonlijke levenssfeer. Wanneer er sprake is van afdoende technische beschermingsmaatregelen (bijvoorbeeld encryptie), dan hoeven eindgebruikers niet te worden geïnformeerd. Er bestaan veel onduidelijkheden over hoe nu precies de meldplicht moet worden uitgelegd. De Europese Commissie heeft daarom een voorstel gedaan voor een verordening (zie persbericht IP/13/591 d.d. 24 juni). Meldingen moeten in principe binnen 24 uur worden gedaan (de Nederlandse wetstekst spreekt van 'onverwijld'), zijn er effecten naar het buitenland dan moeten ook buitenlandse toezichthouders worden geïnformeerd. In een annex wordt exact aangegeven welke elementen deel moeten uitmaken van een melding. Verder gaat de ontwerpverordening dieper in op meldingen aan consumenten en wat onder afdoende technische beschermingsmaatregelen moet worden verstaan. De aankondiging van deze Europese verordening valt vrijwel samen met een nieuw wetsvoorstel om de melding van datalekken uit te breiden (*Kamerstukken II*, 2012/13, 33 662). Dit wetsvoorstel wil de Wet bescherming persoonsgegevens (Wbp) dusdanig aanpassen dat ook andere partijen (zoals webwinkels en andere informatiedienstenaanbieders) voortaan datalekken moeten melden bij het CBP. Bovendien krijgt het CBP het toezicht over artikel 13a Tw. Hiermee is overigens nog niet iedere vorm van datalekken voorzien van een wettelijk kader. Immers het gaat in artikel 13a Tw en de aanpassing van de Wbp alleen om lekken van persoonsgegevens. Het lekken van andere gegevens, zoals zakelijke/bedrijfsgegevens, wordt niet door deze bepalingen gedekt.

De diverse incidenten met de uitval van communicatienetwerken hebben ertoe geleid dat er een wettelijke regeling komt voor de compensatie van eindgebruikers/abonnees (*Kamerstukken II*, 2012/13, 24 095, nr. 342). Het zal om een minimumregeling gaan, die aan de aanbieders de ruimte laat extra compensatie te bieden. Bij een storing van langer dan 12 uur is een compensatie verplicht. De vergoeding is gekoppeld aan de maandelijkse abonnementskosten. Een storing van 12 tot 24 uur geeft zo recht op tenminste 1/30 van de maandelijkse abonnementskosten.

Jurisprudentie

Een interessante uitspraak van het CBb in een langlopende *spam / spyware*-zaak (ECLI:NL:CBB:2013:CA3716). In 2007 werden een drietal ondernemingen en twee privépersonen door OPTA (nu opgegaan in de ACM) beboet wegens het overtreden van artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen (Bude). Dit artikel is de voorloper van de huidige *spam / spyware*- en *cookie*-regeling (art. 11.7a Tw) en verplicht tot afdoende informatie over het plaatsen/uitlezen van gegevens op randapparatuur en tot het bieden van de mogelijkheid tot het weigeren ervan. In deze *DollarRevenue*-zaak werd op meer dan 22 miljoen computers software geplaatst. Met de spyware van DollarRevenue konden gegevens worden verzameld en de computers konden worden gespamd met allerlei commerciële informatie. OPTA legde een recordboete op van in het totaal € 1 miljoen. De rechtbank Rotterdam liet de boetes van OPTA grotendeels in stand (ECLI:NL:RBROT:2010:BL2092 d.d. 02/02/2010). Dat DollarRevenue gebruikmaakte van zogenaamde *affiliates*, tussenpartijen waarmee gecontracteerd werd, om de software te plaatsen en dat niet zelf deed, werd niet relevant geacht aangezien naar de opvatting van de rechtbank dat de overtreden norm zich ook richt tot DollarRevenue. Het CBb is echter een andere mening toegedaan en ziet de *affiliates* als degenen die onder de bepaling vallen. De *affiliates* zijn verantwoordelijk voor het plaatsen van de spyware. Daarmee zijn de *DollarRevenue*-betrokkenen niet als daders aan te merken en vernietigt het CBb de sanctie van OPTA. De grote vraag is wat de ACM nu zal doen. Gaat men alsnog achter de *affiliates* aan? Zal er bij de regelgever op worden aangedrongen dat in dezen geen gat in het toezicht moet zitten en zeker dient te worden gesteld dat partijen als DollarRevenue zelfstandig kunnen worden aangepakt?

DollarRevenue is een grote zaak, maar er is ook veel klein leed. In september 2012 werden er Kamervragen gesteld over het bedrijf ZakelijkeTelefonie.nl (*Aanhangsel Handelingen II*, 2012/13, nr. 424. De onderneming zou zich schuldig maken aan bedenkelijke acquisitiepraktijken en OPTA zou al 148 klachten hebben ontvangen. In een zaak bij de Rechtbank Amsterdam (ECLI:NL:RBAMS:2013:CA3503 d.d. 8 mei 2013) claimt een ondernemer uit Sint Agatha (Noord-Brabant) dat zonder zijn toestemming ZakelijkeTelefonie.nl het telefooncontract heeft overgenomen. Het al niet erg duidelijke antwoordkaartje (waardoor men zich misleidt voelt, zo blijkt uit veel van de klachten) is niet door een bevoegde ondertekend. De rechter is van oordeel dat ZakelijkeTelefonie.nl in het register van de Kamer van Koophandel had moeten nagaan wie bevoegd was. Nu er geen bevoegdelijke ondertekening is, is er geen overeenkomst. Over de vraag of er sprake is van bedenkelijke acquisitie laat de rechter zich niet uit. Evenmin kan de ondernemer rekenen op enige vorm van schadevergoeding ter compensatie voor de tijd die hij in de zaak heeft gestopt. Het is maar goed dat de minister voornemens is om dit soort acquisitiepraktijken via de Telecommunicatiewet te gaan aanpakken.

Literatuur

– F. Simons, 'Flexibele frequenties: een nieuw hoofdstuk 3 Tw', in: *Mediaforum* 2013-06, p. 154-158.
– P.C. Knol & G.J. Zwenne (red.), Telecommunicatie- en privacyrecht (4e druk), Deventer: Kluwer 2013, 1667 p., ISBN 978 90 13 06877 1;
– Voor wie een redelijk recente Engelse vertaling van de Telecommunicatiewet zoekt: *www.government.nl/documents-and-publications/notes/2012/06/07/dutch-telecommunications-act.html*.
– ine niet verantwoordelijk voor persoonsgegevens op