TELECOMMUNICATIERECHT

AAK20137374

N.A.N.M. van Eijk

Wet- en regelgeving

Als er een telco-onderwerp is dat veel aandacht trekt, dan is het wel veiligheid. Veiligheid van netwerken, veiligheid van communicatie. De eventuele verkoop van KPN aan het Mexicaanse América Móvil – inmiddels verleden tijd – deed de nationale harten kloppen. Kon het wel dat een dergelijk bedrijf in buitenlandse handen komt en hoe zat het met de nationale veiligheid? Voor wat betreft de verkoop biedt de Nederlandse regelgeving weinig houvast. Er is niet zoiets als een wet die vereist dat bij bedrijven die een nationaal belang vertegenwoordigen er nog een separate toestemming is vereist. In ieder geval geeft de Telecommunicatiewet geen bijzondere aanknoopingspunten om een verkoop tegen te gaan. Wat bovendien vergeten wordt is dat de aandelen van KPN al in meerderheid worden gehouden door buitenlandse partijen (ofschoon een speciale beschermingsconstructie is ingeroepen, waardoor via een extra aandelenemissie een meerderheid van de aandelen in handen kwam van de stichting Preferente Aandelen KPN, die over de bedrijfsbelangen waakt). In een brief aan de Tweede Kamer gaat de minister van Economische Zaken verder in op de problematiek (*Kamerstukken II* 2012/13, 24 095, nr. 356). Ten aanzien van de nationale veiligheid stelt hij dat een overname van KPN door buitenlandse bedrijven die direct of indirect onder oneigenlijke invloed staan gevolgen kan hebben voor de nationale veiligheid (KPN verzorgt in opdracht van de overheid onder meer het C200-netwerk van de 'zwaailichtensector' en de zogenaamde 'Nood Communicatie Voorziening (NCV). Bezien wordt of bestaande maatregelen nog effectiever kunnen worden toegepast dan wel aanvullende maatregelen nodig zijn.

Andere veiligheidsvragen spelen rond de Snowden-onthullingen dat er op grote schaal door Amerikaanse (NSA) en Britse veiligheidsdiensten (GCHQ) gespioneerd zou worden via internet en andere vormen van communicatie. Over de onthullingen wordt op hoog niveau overleg gevoerd tussen Europa en de VS. Ook is een speciale expertgroep ingesteld (*Kamerstukken II* 2012/13, 30 977, nr. 61). De minister van Veiligheid en Justitie heeft toegezegd het parlement op de hoogte te zullen houden. De Tweede Kamer is bezorgd over het feit dat de NSA tot Europese financiële gegevens toegang zou hebben verkregen en wilde weten of telefoongegevens/gesprekken van kamerleden ook in vreemde handen konden raken (*Aanhangsel Handelingen II* 2013/14, nrs. 50 en 154). Dit laatste is door minister Plasterk van Binnenlandse Zaken ontkend.

Andere kamervragen hadden betrekking op het massaal afluisteren door NSA/GCHQ van internationale verkeer van de Belgische nationale telecomprovider Belgacom (brief d.d. 11 oktober 2013; *Aanhangsel Handelingen II*, 2013Z17658). Er zijn geen aanwijzingen dat dit ook in Nederland is gebeurd. Zorgwekkend is het antwoord op de vraag of Nederlandse telecomaanbieders verzoeken hebben gekregen van buitenlandse veiligheidsdiensten om toegang te geven tot hun internationaal telefoonverkeer: 'Het is de regering niet bekend of buitenlandse mogendheden Nederlandse aanbieders van telecommunicatie hebben benaderd'. De praktijken van de NSA worden mede mogelijk gemaakt door Amerikaanse regulering die weinig beperkingen oplegt voor wat betreft het toegang krijgen tot communicatieverkeer van niet-Amerikanen. Dit wordt ook wel eens samengevat onder het *Patriot Act*-probleem. Deze wetgeving verplicht bijvoorbeeld bedrijven met activiteiten in de Verenigde Staten tot medewerking bij het verkrijgen van toegang, ook wanneer de gegevens zich niet in de VS bevinden. Dit onderwerp kwam recentelijk weer op de tafel toen bleek dat een van de grootste internetknooppunten ter wereld, de in Amsterdam gevestigde AMS-IX, plannen had om activiteiten in de Verenigde Staten te ontplooien. De betreffende kamervragen waren nog niet beantwoord bij afronding van deze bijdrage (*Aanhangsel Handelingen II*, 2013Z18430 en 2013Z18033).

Tot slot: de *Diginotar*-zaak, een onderwerp dat meerdere malen in deze rubriek aan bod is gekomen. Het bedrijf Diginotar dat certificaten uitgaf die gebruikt worden om o.a. internetcommunicatie en -transacties veilig te stellen, werd gehackt en daardoor kon de betrouwbaarheid van die certificaten niet meer worden gegarandeerd. Diginotar wist al zo'n maand of twee dat er wat mis was, maar zei daar niets over. Mede daarom is nu het Besluit elektronische handtekeningen aangepast dat bedrijven die certificaten uitgeven verplicht om onverwijld veiligheidsinbreuken te melden (*Stb.* 2013, 362). Of het veel gaat helpen is maar de vraag. Zo heeft het besluit alleen betrekking op zogenaamde gekwalificeerde certificaten. De veelgebruikte SSL-certificaten (het slotje in het browserscherm) vallen er bijvoorbeeld buiten. Overigens heeft de Tweede Kamer haar verslag uitgebracht over het wetsvoorstel over een algemene meldplicht voor datalekken (*Kamerstukken II* 2012/13, 33 662). Er wordt onder meer gesignaleerd dat de meldplichten voor datalekken inmiddels een lappendeken zijn geworden.

De Europese Commissie heeft voorstellen gepubliceerd om de bestaande Europese regels voor de Telecommunicatiesector deels te herzien dan wel de uitvoering ervan nader in te kaderen. Dit zou moeten gebeuren via een nieuwe verordening (Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, COM(2013) 627 final, Brussel, 11/9/2013; Zie tevens IP/13/828 en IP/13/779). Er is nogal wat kritiek op de voorstellen. Zo noemde het Europese samenwerkingsverband van telco-toezichthouders BEREC, het een onsamenhangende lappendeken van maatregelen. Een aantal van de voorstellen: De invoering van een 'Europees paspoort', waardoor registratie in een lidstaat de toegang tot de rest van interne markt moet waarborgen; verlaagde roamingtarieven (maar niet zo laag als eerder aangekondigd) en een materiële regeling van netneutraliteit. Op dit laatste

is veel kritiek omdat tegelijkertijd nadrukkelijk ruimte wordt geboden om capaciteit op het internet te reserveren voor bepaalde diensten (*managed services*). Daarmee dreigt de ruimte voor het 'open internet' in de knel te komen, aldus de tegenstanders.

Jurisprudentie

Een nieuw hoofdstuk is toegevoegd aan wat zo ongeveer de langstlopende zaak in telecomland is. Al vele jaren probeert OPTA, nu de ACM, de zogenaamde *terminating*-tarieven te regelen. Het gaat om de tarieven die betaald moeten worden voor het afhandelen van gesprekken (bv. KPN biedt een gesprek afkomstig van haar netwerk aan bij UPC om dat te laten afleveren bij de abonnee waarvoor het bestemd is). In beginsel gaat de zaak erom dat de toezichthouder voor deze afhandeling een tarief wil hanteren dat voldoet aan een kostenberekeningsmethode die ook door de Europese Commissie wordt aanbevolen. Dit wordt bepaald in een zogenaamd marktanalysebesluit. Het CBb lag tot op heden telkens dwars omdat het meende dat de noodzaak tot de methode onvoldoende onderbouwd was en een lichtere kostenberekeningsmethode derhalve de voorkeur had. De ACM dacht met een laatste marktanalysebesluit (*Stcrt.* 2013, 22592) aan alle bezwaren tegemoet te komen en kreeg ook de zegen van de Europese Commissie (IP/13/760). Echter, in voorlopige voorziening constateert het CBb opnieuw dat de onderbouwing onvoldoende is en schroeft de tarieven opnieuw terug (ECLI:NL:CBB:2013:99). Er zit voor de ACM niets anders op dan wederom op zoek te gaan naar een motivering die wel door het CBb geaccepteerd zal worden.

Literatuur

– A. Arnbak & J. van Hoboken, 'De wind van Snowden in de Amerikaanse informatieparaplu', *Mediaforum* 2013-7/8, p. 173;
– M. Bolhuis, 'Toenemende aandacht voor meldplicht datalekken ter bescherming van persoongegevens, Quo Vadis?', *Mediaforum* 2013-7/8, p. 174-186;
– N.A.N.M. van Eijk, 'Over KPN en het algemeen belang', *Mediaforum* 2013-9, p. 209;
– J. Kohlen, 'Project 15: samenvoegen NMa, OPTA en CA en de stroomlijning der bevoegdheden', *Mediaforum* 2013-9, p. 210-216.