TELECOMMUNICATIERECHT

AAK20178297
N.A.N.M. van Eijk

Wet- en regelgeving

Opnieuw is een hoofdstuk toegevoegd aan de herziening van de bestaande regels voor de telecommunicatiesector: de herziening van de e-Privacyrichtlijn (IP/17/5, 10 januari). Eerder is in deze rubriek gesproken over de nieuwe verordening met betrekking tot roaming en netneutraliteit. Ook het magnum opus, de opstelling van een Electronic Communications Code is besproken. Juist deze laatste herziening geeft aan hoe de problemen van de hedendaagse informatiesamenleving niet meer in een traditioneel kader te vangen zijn. Diensten die voorheen 'klassieke' telecom waren, zoals telefoneren, krijgen steeds meer alternatieven – WhatsApp – waarvan de vraag is of die wel passen in hetzelfde raamwerk. Vergelijkbare vragen doen zich voor in het mediadomein, waar de herziening van de Audiovisuele mediadienstenrichtlijn wordt aangegrepen om internetdiensten zoals YouTube te gaan reguleren. De herziening van de e-Privacyrichtlijn vertoont gelijke trekken. Allereerst is er de voor de hand liggende vraag waarom er een herziening nodig is, nadat nog maar kortgeleden een nieuwe privacyverordening is vastgesteld die in 2018 in werking treedt. Was het niet juist de bedoeling dat deze alomvattend zou zijn? Dan is er toch geen sectorspecifieke regeling meer nodig, laat staan het omzetten van een richtlijn in een verordening, zo lijkt de logische conclusie. Een deel van het antwoord is dat marktpartijen en andere stakeholders voorstander zouden zijn van een sectorspecifieke regulering. Wat treffen we aan in het voorstel voor een regulering (COM(2017)10 final – 2017/003 (COD)? In de eerste plaats wordt het vereiste van toestemming versterkt. Toestemming is nadrukkelijk vereist en de toestemmingverlening dient op een effectieve wijze te worden ingericht. De teugel wordt aangetrokken bij de beruchte cookies, maar ook wanneer het gaat om spam en direct marketing. De cookievoorstellen, die veel lijken op de Nederlandse wetgeving, zullen veel van de aandacht opeisen, ook al omdat de Europese Commissie meent dat bijvoorbeeld via een browserinstelling een meer effectieve toestemmingverlening mogelijk is. In de tweede plaats zien we meer focus op de vertrouwelijkheid van de communicatie, dat past natuurlijk mooi bij een 'post-Snowden-tijdperk'. Het doorzoeken van de inhoud van de communicatie kan alleen maar in zeer bijzondere omstandigheden. De impact op de gebruikelijke praktijk dat veel apps en internetdiensten dat al doen – al dan niet met expliciete toestemming van gebruikers – zal in het verdere debat zeker aan de orde komen.

De betekenis van nieuwe Europese regels staat of valt met goede implementatie, toezicht en handhaving. In *KwartaalSignaal* 138 en 139 werd gewezen op het feit dat de Nederlandse regering een eigen interpretatie heeft gegeven aan de betreffende Europese verordening door het bestaande absolute verbod op prijsdiscriminatie in stand te houden. T-Mobile daagde de wetgever en toezichthouder uit door een dienst aan te bieden waarbij muziekgebruik niet ten laste kwam van de reguliere data-bundel. Volgens T-Mobile was dit een redelijke interpretatie van de verordening, die ook gesteund zou worden door het overlegorgaan van telecomtoezichthouders, BEREC. De ACM startte onmiddellijk een onderzoek, oordeelde dat T-Mobile zich niet aan de Telecommunicatiewet hield en legde een last onder dwangsom op. Wel was de ACM bereid mee te werken aan een snelle gang naar de rechter. Die zal moeten uitmaken of de nationale regels wel voldoende in lijn zijn met de Europese verordening.

Jurisprudentie

De rechters van het Europese Hof in Luxemburg, die al eerder wetgeving waarin telecomaanbieders verplicht werden tot grootschalige dataopslag ('dataretentie') naar de prullenbak verwezen (ECLI:EU:C:2014:238) en daarmee de Europese en nationale regelgever in hun hemd zetten, moesten oordelen over nieuwe reparatiewetten in Zweden en in het Verenigd Koninkrijk. Deze wetten bieden opnieuw uitgebreide mogelijkheden tot het verzamelen van telecomgegevens waarvan de vraag is of dit niet zou leiden tot het permanent volgen van grotendeels onschuldige burgers. Burgerrechtenorganisaties kwamen in het verweer en vroegen de rechters om vast te houden aan hun eerdere oordeel dat grootschalige gegevensverzameling met waarborgen moet zijn omkleed. Regeringen van veel lidstaten van de Europese Unie – inclusief Nederland – namen aan het proces deel met min of meer het tegenovergestelde standpunt. De boodschap van het Europese Hof in zijn oordeel van 21 december 2016 (ECLI:EU:C:2016:970) is duidelijk. Ja, gegevens verzamelen voor de bestrijding van ernstige misdrijven en terrorisme is toegestaan. Maar de mitsen zijn ook helder: verzamelen is alleen gerechtvaardigd als het ook daadwerkelijk bijdraagt aan de bestrijding van deze ernstige misdrijven en terrorisme. Dit betekent dat wetgeving over het grootschalig volgen van burgers moet voorzien in een systeem dat verantwoording aflegt over de effectiviteit ervan. In de tweede plaats stelt het Hof dat alleen wanneer het gaat om echt ernstige misdrijven het massaal verzamelen en gebruiken van gegevens geoorloofd is. Ten derde laat het Hof er geen misverstand over bestaan dat het massaal verzamelen en gebruiken van deze gegevens alleen kan wanneer daarover vooraf onafhankelijk toezicht wordt uitgeoefend, bij voorkeur door de rechter.

Literatuur

– HvJ EU 8 april 2014, *NJ* 2016/446, m.nt. E.J. Dommering (*Digital Rights Ireland*) en HvJ EU 6 oktober 2015, *NJ* 2016/447, m.nt E.J. Dommering (*Schrems*).
– C. Hijzen, *Vijandbeelden, de veiligheidsdiensten en de democratie, 1912-1992* (diss. Leiden), Amsterdam: Boom uitgevers 2016 (*https://openaccess.leidenuniv.nl/handle/1887/44272*, helaas onder embargo tot 2019).
– J.J. Oerlemans, *Investigating cybercrime* (diss. Leiden), Amsterdam: Amsterdam University Press 2017 (*https://openaccess.leidenuniv.nl/handle/1887/44879)*.
– B.F.E. Bosch & N.A.N.M. van Eijk, 'Wifi-tracking in de winkel(straat): inbreuk op de privacy?', *P&I* 2016, afl. 6, p. 238-246.