TELECOMMUNICATIERECHT

AAK20147593

N.A.N.M. van Eijk

Wet- en regelgeving

Geruime tijd geleden, in 2008, werd door het kabinet gestart met een traject dat zou moeten leiden tot een modernisering van de Grondwet (*Kamerstukken II* 2011/12, 31570). Zoals zoveel eerdere pogingen strandde ook dit initiatief grotendeels. Bepalingen zoals artikel 7 Grondwet (uitingsvrijheid) en artikel 13 (communicatievrijheid) zijn zwaar achterhaald en sluiten niet aan bij de jurisprudentie die inmiddels door het Europese Hof voor de Rechten van de Mens in Straatsburg is ontwikkeld. Alleen

ten aanzien van artikel 13 Grondwet stelde het kabinet voor om tot concrete actie over te gaan (*Kamerstukken II* 2011/12, 31570, nr. 21). Een voorontwerp werd opgesteld en tot eind 2013 ter consultatie aangeboden (*www.internetconsultatie.nl/briefentelecommunicatiegeheim*). Het Kabinet heeft nu een definitief voorstel toegestuurd aan de Tweede Kamer (*Kamerstukken II* 2013/14, 33989). Het voorstel regelt een uitbreiding van het communicatiegeheim dat zich nu nog alleen uitstrekt tot klassieke communicatievormen als de brief, telegraaf en telefoon. Voortaan worden alle vormen van communicatie – 'content' wordt het genoemd in het voorstel – grondwettelijk beschermd doordat er een algemeen brief- en telecommunicatiegeheim komt. E-mail, telefoonverkeer via internet en besloten communicatie via sociale media vallen allen onder het nieuwe grondrecht. Dit betekent dat het primair gaat om een uitbreiding van grondrecht in de transportfase. Dit sluit redelijk aan bij klassieke ideeën dat in het bijzonder dit onderdeel van het proces bescherming verdient. Geopende brieven en op een pc opgeslagen e-mailberichten vallen buiten artikel 13 Grondwet. Meer en meer is de vraag aan de orde of daarmee een afdoende niveau van communicatievrijheid/-geheim wordt verkregen. Doordat het communicatieverkeer (o.a. dankzij de Snowden-affaire) steeds meer van encryptie wordt voorzien, is het achterhalen van informatie in de transportfase moeilijker geworden (in tegenstelling tot verkeers- en locatiegegevens, die niet van encryptie zijn te voorzien en in de handhaving een steeds belangrijkere rol spelen). Opsporing schuift mede daarom door naar de 'randen van de communicatienetwerken'. Via het plaatsen van malware op randapparaten kan toch toegang tot de communicatie worden verkregen (zie de discussie over het omstreden voorstel 'Computercriminaliteit III'. Het is de vraag of er niet voor een meer functionele benadering moet worden gekozen, waarbij bijvoorbeeld ook toegang tot communicatie-apparaten afdoende wordt beschermd. In dit verband is er door het Amerikaanse Supreme Court een interessante uitspraak gedaan in de recente Riley-zaak (*www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf*). Daarin oordeelt het Supreme Court dat voor het doorzoeken van een mobiele telefoon een afzonderlijke last is vereist. In het zeer lezenswaardige arrest wordt onder meer gesteld:

'Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.'

Via het *fourth amendment* (dat zich ook uitstrekt tot privacy) wordt aldus een belangrijke uitbreiding aan de bescherming van de communicatie toegevoegd. Een interessante invalshoek die ook bij de aanpassing van het grondwetsartikel aan de orde kan komen. Het omstreden tweede lid van het voorontwerp is grotendeels ongewijzigd gebleven. Hierin wordt bepaald dat voor beperkingen een rechterlijke last nodig is, behalve wanneer het gaat om nationale veiligheid. Dan kan worden volstaan met een 'door of met machtiging van hen die daartoe bij de wet zijn'. Dit is in feite een verslechtering ten opzichte van het voorontwerp dat nog sprak van een ministeriële toestemming. De tekst van het voorstel laat delegatie toe. Waarborgen ten aanzien van een juiste toepassing van het tweede lid zouden moeten voortvloeien uit Europese jurisprudentie, zo valt in de memorie van toelichting te lezen. In de nationale veiligheidsdiscussie is meermalen geopperd om ook ten aanzien van het inzetten van bevoegdheden een rechterlijke last (of daarmee vergelijkbaar beschermingsniveau) te introduceren en dat constitutioneel te borgen. Ervaringen in andere landen – inclusief de Verenigde Staten – geven aan dat een dergelijke bescherming mogelijk is.

Om bij dit laatste onderwerp te blijven: de minister van Economische zaken komt met een wetsvoorstel dat regels gaat stellen inzake de overname van telecombedrijven in het belang van nationale veiligheid (*Kamerstukken II* 2013/14, 24095, nr. 368). Een en ander is een vervolg op het eerdere voornemen van het Mexicaanse América Móvil om KPN over te nemen (*Kamerstukken II* 2012/13, 24095, nr. 356). Het is de bedoeling dat er voortaan kan worden ingegrepen wanneer een overname van een Nederlands telecombedrijf schade kan toebrengen aan het netwerk en daardoor de nationale veiligheid in gevaar kan komen. Daarbij wordt onderscheid gemaakt tussen geopolitieke risico's en veiligheidsrisico's. Bij geopolitieke risico's gaat het om een beoogde overname die ingegeven is door overwegingen als het onder druk kunnen zetten van de nationale overheid. Bij veiligheidsrisico's gaat het om de toegang tot kennis en informatie. Binnen bedrijven wordt vertrouwelijke informatie verwerkt, onder meer in het kader van het werk van veiligheids- en opsporingsdiensten. De voorgestelde maatregelen komen erop neer dat een verklaring van geen bezwaar is vereist bij de overname of doorverkoop van een telecomonderneming waar het gaat om vitale telecommunicatie-infrastructuur. Ook een verklaring van geen bezwaar ten aanzien van benoemingen in de raad van bestuur of raad van commissarissen kan vereist zijn. In de brief wordt aangegeven dat de beoogde regels waarschijnlijk alleen relevant zullen zijn voor KPN, dat diverse taken verzorgt die gelinkt zijn aan nationale veiligheid. Het wetsvoorstel moet begin 2015 gereed zijn.

Jurisprudentie

De Hoge Raad heeft zich uitgesproken over de inzet van zogenaamde IMSI-catchers (onder meer arrest dd. 1 juli 2014, ECLI:NL:HR:2014:1562, zie ook: ECLI:NL:PHR:2013:2782). Het gaat om een technologie om mobiele verkeers- en locatiegegevens te vergaren zonder dat gebruikers dit doorhebben. De Hoge Raad stelt vast dat artikel 126nb Sv – dat wordt aangevoerd als grondslag voor het verzamelen van de informatie – slechts een wettelijke basis biedt voor het identificeren van een gebruiker, niet voor het vergaren van locatie- en locatiegegevens. Alleen beperkte verzameling van verkeersgegevens is verenigbaar met artikel 3 Politiewet (algemene handhaving van de rechtsorde). De Hoge Raad bevestigt hiermee haar

eerdere opvatting dat dit artikel slechts inzetbaar is ‘op een wijze die een beperkte inbreuk maakt op grondrechten van burgers en die niet zeer risicovol is voor de integriteit en beheersbaarheid van de opsporing. In het bijzonder kan de toepassing van deze opsporingsmethode jegens de gebruiker van de gsm-telefoon onrechtmatig zijn indien zij in verband met de duur, intensiteit en frequentie ervan geschikt is om een min of meer compleet beeld te verkrijgen van bepaalde aspecten van het persoonlijk leven van de betrokkene. *Great minds think alike*: mijns inziens sluit de opvatting van de Hoge Raad goed aan bij het oordeel van het Supreme Court in de *Riley*-zaak.

Literatuur

– O. Troja, ‘VMC-studiemiddag 13 juni 2014, Nationale veiligheid en afluisterstaat’, in: *Mediaforum* 2014-6, p. 167-170;
– O. van Daalen, ‘Consternatie bij de afdeling vermiste en gevonden telefoons’, in: *Mediaforum* 2014-5, p. 133;
– C. Prins, ‘Geheime handel in digitale lekken’, in *NJB* 2014, 17, p. 1171;
– B. van der Sloot, ‘Privacy in het post NSA-tijdperk, tijd voor een fundamentele herziening?’, in *NJB* 2014-17, p. 1172-1179.