INLEIDING

Op zaterdag 20 september 1997 vond in café De Plakhoek in Amsterdam een schietpartij plaats. Bij deze schietpartij werd een zgn. stengun leeggeschoten op bezoekers en eigenaar van het café. Vreemd genoeg raakte alleen de eigenaar gewond. De politie ging direct op zoek naar de drie verdachten van de schietpartij. Bij deze zoektocht kwam Okan O., wel bekend van de vele aan hem gewijde afleveringen van het populaire, en journalistiek niet al te hoogstaande, televisieprogramma "Peter R. de Vries"naar voren als deelnemer en aanstichter van de schietpartij. Na een geruchtmakend proces werd Okan O. veroordeeld tot een gevangenisstraf van 4 jaar. Niet lang na die veroordeling overleed Okan O. aan kanker. Het is dan ook niet van een hoger beroep in de zaak gekomen.

Okan O. heeft altijd ontkent betrokken te zijn geweest bij de schietpartij. Okan O. ontkende zelfs op het bewuste tijdstip in Amsterdam te zijn geweest. Hij verklaarde dat hij in een discotheek in Alkmaar was op het moment van de schietpartij. Het is niet zijn verhaal wat zo opmerkelijk is. Wat wel opmerkelijk aan deze zaak is, is de wijze waarop het OM trachtte de bewijzen dat Okan O. wel op het tijdstip van de schietpartij in de omgeving van café De Plakhoek was. Het OM heeft in deze zaak handig gebruik gemaakt van het feit dat, ten tijde van de schietpartij, de mobiele telefoon van Okan O. werd getapt i.v.m. de verdwijning van zijn vriendin en kind. Het OM betoogde dat ondanks het feit dat er geen gesprekken waren gevoerd met die mobiele telefoon rond het tijdstip van de schietpartij, zij dankzij de tap toch kon bewijzen dat Okan O. op het bewuste tijdstip wel in Amsterdam was. Vanaf zgn. GSM-palen worden nl. regelmatig signalen verstuurd richting mobiele telefoons waarmee vervolgens de locatie van de telefoon kan worden bepaald. Het verhaal van het OM heeft de rechtbank, gezien de veroordeling, kunnen overtuigen.

Bovenstaand verhaal roept bij mij verschillende vragen op. De belangrijkste daarvan is de vraag of het bovenstaande gebruik van de opsporingsbevoegdheden geregeld in art 125f en 125g Sv wel wordt gedekt door de wettelijke regeling van bijzondere opsporingsmethoden. Bij het beantwoorden van die vraag dient natuurlijk ook de nieuwe regeling van het wetsvoorstel bijzondere opsporingsbevoegdheden (wetsvoorstel Bob) te worden betrokken. De vraag is dus of je mag plaatsbepalen m.b.v. de bevoegdheden die in het WvSv onder de noemer onderzoek van telecommunicatie staan. Indien deze opsporingsmethode niet wettelijk geregeld is en de methode wel een inbreuk maakt op de persoonlijke levenssfeer, dan zal gebruik van dit middel niet geoorloofd moeten worden geacht.

Bij het zoeken naar een antwoord op bovengenoemde vraag zal ik allereerst proberen te verduidelijken hoe de plaatsbepaling via mobiele telefoons in zijn werk gaat. Daarna zal ik de wettelijke regeling van het vorderen van inlichtingen over telecommunicatie en de regeling van het tappen onder de loep nemen. Daarbij zal ik ook aandacht besteden aan de regeling in het wetsvoorstel Bob en ook (in aparte paragrafen) aan de rechtsspraak m.b.t. deze artikelen en de opmerkingen m.b.t. observatie van de cie van Traa. Vervolgens zal ik aandacht besteden aan de inbreuk die de in de zaak Okan O. gebruikte methode maakt op het recht op privacy. Na nog enige aandacht te besteden aan andere methoden van plaatsbepaling, zal ik tenslotte in de conclusie mijn visie op de geoorloofdheid van de door politie en justitie, in de zaak Okan O., gebruikte methode geven.

Plaatsbepaling en mobiele telefoons

In de zaak Okan O. is mede o.g.v. inlichtingen verstrekt door KPN Telecom aan politie en justitie de verblijfplaats van Okan O. op het tijdstip van de schietpartij wettig en overtuigend bewezen.

De bovengenoemde inlichtingen hebben betrekking op de afgelegde route van de mobiele telefoon van Okan O. Ook als er geen gesprekken worden gevoerd met een mobiele telefoon, wordt er bij de KPN (en ook bij de andere telecommunicatiebedrijven) geregistreerd waar de telefoon zich bevindt.

In de zaak van Okan O. werd duidelijk dat de plaatsbepaling geschiedt middels zend- en ontvangstbakens van de KPN, de zgn. GSM-palen. Ongeveer een half jaar voor de uitspraak in de zaak Okan O.[1] ontkenden de aanbieders van telecommunicatiediensten in Nederland nog het feit dat de gegevens m.b.t. de locatie van de mobiele telefoons werden geregistreerd en bewaard in computers. Dit naar aanleiding van onthullingen in een Zwitserse krant m.b.t. dit onderwerp. Daar zouden de gangen van de drager van de mobiele telefoon op de minuut en op enkele honderden meters nauwkeurig kunnen worden nagegaan. Iets wat het Zwitserse telecommunicatiebedrijf Swisscom heeft bevestigd. In de zaak Okan O. verklaarde een medewerker van KPN dat dat in Nederland (in stedelijk gebied) ongeveer om de drie kilometer GSM-palen staan. Dezelfde medewerker van KPN verklaarde ook dat de gangen van Okan O. alleen nagegaan hadden kunnen worden, omdat er gebruik was gemaakt van de voice-mail van de telefoon. De KPN registreert signalen die de mobiele telefoon uitzendt bij het doorschakelen van inkomende gesprekken naar de voicemail. In Zwitserland wordt echter min of meer constant de locatie van de mobiele telefoon geregistreerd. Deze gegevens zouden vervolgens minstens een half jaar worden bewaard. Permanente lokalisatie van de telefoon zou noodzakelijk zijn om er voor te zorgen dat de gebruiker bereikbaar blijft. Het is dan ook waarschijnlijk dat zo'n permanente registratie ook in Nederland plaatsvindt. Dit te meer omdat bekend is geworden dat de KPN locatiegegevens zou gebruiken in hun strijd tegen fraude met telefoons. De zgn. "call detail records" zouden moeten helpen bij het voorkomen en bestrijden van het "op andermans kosten telefoneren".

Het is vooralsnog een raadsel hoe lang de KPN de locatiegegevens bewaart. Er worden perioden genoemd van 3 maanden tot 1 jaar. De tijd dat de gegevens bewaard worden is m.n. van belang i.v.m. de controleerbaarheid van die gegevens voor de zittingsrechter en de verdediging van de verdachte. Naast deze informatie is het voor de rechter en de verdediging eveneens zeer belangrijk dat de exacte technische details over de locatiebepaling aan het licht komen. Hoe kan de rechter anders de betrouwbaarheid van de methode beoordelen. Hoe zeker is het bijvoorbeeld dat het altijd de dichtstbijzijnde GSM-paal is die het signaal van de mobiele telefoon ontvangt?

Volledige openheid over de precieze werking van de locatiebepaling van de mobiele telefoon lijkt mij een absoluut vereiste voor het gebruik van deze methode voor strafrechtelijke doeleinden. Alleen indien volledige duidelijkheid bestaat over hoe een en ander in zijn werk gaat, kan een oordeel over de betrouwbaarheid en de nauwkeurigheid van het middel worden vervormd. M.i. kan in het strafproces geen genoegen worden genomen met de geheimzinnigheid die de aanbieders van telecommunicatiediensten op dit moment m.b.t. de methode van plaatsbepaling van mobiele telefoons betrachten. Ook het voorgestelde art 126ee (wetsvoorstel Bob) eist duidelijkheid over de nauwkeurigheid en controleerbaarheid van methoden waarbij gebruik wordt gemaakt van technische hulpmiddelen. Voorafgaand aan een eventuele belangenafweging om de geoorloofdheid van deze opsporingsmethode te bepalen, zal dan ook het belang van deze methode voor de strafrechtspleging en het belang van de telecommunicatiebedrijven (die gediend zijn met de geheimhouding van de precieze werking van deze methode) tegen elkaar moeten worden afgewogen.

Het argument dat de opsporing in andere (toekomstige) zaken zal kunnen worden belemmerd door de onthulling van de werking van het middel, is m.i. niet overtuigend genoeg om de exacte werking verborgen te houden. Een vergelijking met b.v. de "Mercedes-zaak" gaat m.i. scheef. Het ging in die zaak weliswaar om het aan criminelen inzicht verschaffen in bepaalde opsporingstechnieken, maar in die zaak stond het recht op bescherming van de persoonlijke levenssfeer van de verdachte op het spel. Daarbij was er in die zaak ook weinig aanleiding om te twijfelen aan de betrouwbaarheid van de daar gebruikte methode, mede door het vermoedelijke gebrek aan complexiteit van de methode.

[1] Rechtbank Amsterdam, 4 mei 1998

Artikel 125f

In 1971 werd het onderzoek van telefoongesprekken in ons land geïntroduceerd in het Wetboek van strafvordering. Twintig jaar later werd, met de komst van de Wet computercriminaliteit, de wettelijke regeling van het onderzoek van telefoongesprekken aangevuld met (wettelijke) mogelijkheden tot onderzoek van andere vormen van telecommunicatie (bijvoorbeeld de fax en de e-mail)[2]. Vanaf dat moment kon ook ander gegevensverkeer op rechtmatige wijze worden onderzocht. De regeling is nu nog te vinden in de artikelen 125f t/m 125h Sv.

Artikel 125f Sv biedt de officier van justitie (of tijdens het gerechtelijk vooronderzoek de rechter-commissaris) de mogelijkheid om, onder de in dat artikel gestelde voorwaarden, van alle medewerkers van een bedrijf dat telecommunicatievoorzieningen aanbiedt, te vorderen dat hij of zij inlichtingen verschaft m.b.t. “alle verkeer dat over de telecommunicatie-infrastructuur of over een telecommunicatie-inrichting die wordt aangewend voor het publiek, heeft plaatsgevonden en waarvan het vermoeden bestaat dat de verdachte eraan heeft deelgenomen”. Voor de uitvoering van die vordering zijn politie en justitie aangewezen op technische bijstand van de medewerkers van de bedrijven die de telecommunicatiediensten aanbieden. De persoon aan wie de vordering is gericht is dan ook, behoudens de aanwezigheid van een verschoningsrecht, verplicht de bovengenoemde gegevens te verstrekken. Het niet voldoen aan de vordering inlichtingen te verstrekken, is in art 184 Sr strafbaar gesteld.

In de praktijk wordt de bevoegdheid onder meer gebruikt om te achterhalen met welke nummers, hoe lang en en passant ook waarvandaan is gebeld. De praktijk laat ook zien dat gegevens al worden gevorderd voorafgaand aan de telefoongesprekken waarover de inlichtingen worden gevraagd. Corstens lijkt de mening toegedaan dat dit voorafgaand aan de gesprekken waarover informatie vorderen met het oog op de wetsgeschiedenis gelegitimeerd moet worden geacht. Ogenblikkelijk dringen zich beelden bij mij op waarin ik rechercheurs bij de KPN op een beeldscherm de verplaatsing van de telefoon van de verdachte volgen en dit (mobiel) doorbellen naar de observerende agenten. Gelukkig zegt Mevis in Tekst en Commentaar dat de vordering als bedoeld in art 125f alleen betrekking mag hebben op verkeer dat reeds heeft plaatsgevonden. Volgens Mevis verzetten niet alleen de bewoordingen van het artikel zich daartegen, ook zou dit teveel lijken op de figuur van het “tappen” dat geregeld is in art 125g[3]. De meningen zijn verdeeld.

Overigens zal in geval van plaatsbepaling met behulp van “het vorderen van inlichtingen” ook gebruik moeten worden gemaakt van art 125g, omdat art 125f niet betrekking heeft op een bepaalde persoon maar op een bepaald telefoonnummer (in het geval van een mobiele telefoon op een bepaalde telefoon). De inlichtingen met betrekking tot de plaats van de telefoon zeggen nog niets over wie gebruik maakte van de telefoon. Zie hierover de paragraaf over art 125g.

Blijkens de bewoordingen van het artikel betreffen de inlichtingen *alle verkeer*. D.w.z. alle gegevensverkeer via telecommunicatie waarvan wordt vermoed dat de verdachte daaraan heeft deelgenomen. Hoewel het mij voorkomt dat de zinsnede “dat de verdachte daaraan heeft deelgenomen” nog wel te lezen is als “het vermoeden dat de verdachte in het bezit was van de in het geding zijnde telefoon”, betwijfel ik toch dat gegevens die nodig zijn voor plaatsbepaling vallen onder de bewoordingen “inlichtingen betreffende alle verkeer met behulp van telecommunicatie”.

[2] Wet van 23 december 1992 (Stb. 1993, 33).
[3] T&C Strafvordering, 2e druk, p. 286.

Mevis noemt als mogelijke gegevens die onder het bereik van art 125f vallen, de gegevens die betrekking hebben op de vragen “Wie telefoneerde op welk moment vanaf welk toestel hoelang en met wie?”. De MvA noemt ook de overdracht via de telecommunicatie-infrastructuur van signalen waarmee een ander wordt opgeroepen. Het totstandkomen is dan kennelijk voldoende, daadwerkelijke communicatie lijkt niet plaats te hoeven vinden. Dit laatste wordt ook benadrukt door de rechtbank in de zaak Okan O.;

“Uit de parlementaire geschiedenis van art 125f (…) blijkt dat niet alleen van verkeer kan worden gesproken als er daadwerkelijke communicatie plaatsvindt. Op grond daarvan moet het ervoor worden gehouden dat in casu in het kader van de normale bedrijfsvoering van de netwerkbeheerder naar de GSM uitgezonden en geregistreerde signaal, behoort tot het in dat artikel bedoelde verkeer ter zake waarvan op de voet van art 125f Sv in de daar genoemde gevallen inlichtingen gevorderd kunnen worden door het openbaar ministerie.”

Ten aanzien van de grond van het vorderen van de gegevens waar het mij om gaat staat niets in artikel 125f. Dat is jammer, want zou dat wel het geval geweest zijn, dan zou daar wellicht een aanwijzing omtrent de toelaatbaarheid van plaatsbepaling op grond van dit artikel uit zijn af te leiden geweest.

In tegenstelling tot art 125f spreekt art 125g over “het onderzoek dat het “tappen” dringend vordert”. Uit deze bewoordingen van artikel 125g leidt Corstens af dat hier wel plaatsbepaling onder kan vallen[4].

Overigens bevatten de gevallen waarin de bevoegdheid van artikel 125f mag worden gebruikt, “in geval van heterdaad, van een misdrijf waarvoor voorlopige hechtenis is toegelaten of van een misdrijf, bedoeld in art 138a Sr (…)”, ook geen aanwijzing omtrent de bovengenoemde vraag. Hieruit wordt slechts duidelijk dat toepassing van dit middel alleen gelegitimeerd is als er sprake is van ernstige misdrijven.

Ondanks het feit dat strikt genomen de gegevens m.b.t. de locatie van de telefoon wel tot “telecommunicatie” te rekenen zijn, betwijfel ik toch of de plaatsbepaling middels mobiele telefoon geregeld is in art 125f. Ik word in die opvatting gesterkt bij het lezen van opmerkingen als:

“Art 125f Sv (….) is beperkt tot het onderzoek naar de vraag vanaf welke aansluitpunten is gecommuniceerd en voor hoe lang”5; en

“ Art 125f Sv is geen observatiebevoegdheid”6

Met de komst van de nieuwe regeling uit het wetsvoorstel Bob verandert m.i. bijzonder weinig m.b.t. de bovengenoemde bezwaren. Ook het feit dat art 125f in de nieuwe regeling in twee artikelen staat doet hier niets aan af. De artikelen 126n en 126u lijken een kopie te zijn van het huidige 125f Sv. Dat onderzoek van telecommunicatie o.g.v. art 126u mogelijk is in de zgn. poractieve fase is niets nieuws. Dit is ook op basis van de huidige wettige regeling mogelijk gelet op de art 129 Sv en art 46 lid 1 Sr .

Artikel 125g

Art 125g heeft betrekking op het tappen of opnemen van telecommunicatie terwijl die plaatsvindt. Het gaat dus om gegevens die normaliter niet worden vastgelegd, en dus niet kunnen worden gevorderd op grond van art 125f.

[4] Corstens, Het Nederlandse strafprocesrecht (Handboek), 2e druk, p.418.
[5] Vademecum Strafzaken/Suppl. 72 [22]-98-100.
[6] Buruma/Vegter, Buitengewone opsporingsmethoden, Studiepocket strafrecht nr 34, 1998.

De rechter-commissaris kan, tijdens een gerechtelijk vooronderzoek, bepalen dat gegevensverkeer via de telecommunicatie-infrastructuur die voor dienstverlening aan het publiek wordt gebruikt, wordt afgetapt of opgenomen. De uitvoering van het tapbevel ligt in handen van opsporingsambtenaren, die evenals bij art 125f aangewezen zullen zijn op de medewerking van medewerkers van de verschillende in Nederland opererende telecommunicatiebedrijven. Opvallend verschil met art 125f is dat deze bevoegdheid alleen mag worden toegepast tijdens het GVO. In de praktijk worden dan ook veelvuldig een GVO gevorderd met als achterliggend doel gebruik te kunnen gaan maken van deze bevoegdheid.

Waarom is art 125g in dit kader van belang? Allereerst heb je de tapbevoegdheid nodig om te kunnen bepalen of de verdachte daadwerkelijk de telefoon bij zich had op het moment waarop de inlichtingen uit art 125f betrekking hebben. Als je de inlichtingen met betrekking tot de plaats waar de mobiele telefoon zich heeft bevonden laat vallen onder “alle verkeer” van art 125f en je op grond van dat artikel die gegevens opvraagt, dan heb je zonder art 125g alleen de plaats van de telefoon, zonder dat je weet wie die telefoon bij zich droeg. Was het de verdachte, z’n vriendin of toch die zakenpartner van ‘m ?

Artikel 125h

De rechter-commissaris moet beslissen wat er met de inlichtingen die op grond van art 125f zijn verkregen, moet gebeuren. Gegevens die van geen betekenis zijn voor het onderzoek moeten blijkens het eerste lid van art 125h zo spoedig mogelijk worden vernietigd. Datgene wat na vernietiging overblijft (en dan heb ik het niet over papiersnippers of as) dient bij de processtukken gevoegd te worden. Als niet binnen een maand na het verkrijgen van de inlichtingen, bedoeld in art 125f, door de officier van justitie een gerechtelijk vooronderzoek wordt gevorderd dan dienen de gegevens vernietigd te worden.

Corstens wijst er in zijn handboek op dat de regeling van art 125h lacuneus is. Allereerst loopt de verdachte het risico dat hij niet kan aantonen dat vernietigd materiaal wel relevant is. Zo kan het voorkomen dat bij die vernietigde gegevens ontlastend materiaal zat. Daarnaast is niet geregeld in hoeverre hij toegang heeft tot het oorspronkelijke materiaal. Zijn de gegevens/gesprekken wel juist weergegeven in de processen-verbaal?[7]. De formulering van het eerste lid van art 125h laat m.i., gezien de woorden “zo spoedig mogelijk”, ook geen ruimte voor redeneringen in de trant van: “Ach, laten we die printgegevens m.b.t. de locaties waar X zich al die tijd bevond nog maar een tijdje bewaren, je weet maar nooit of het ooit nog eens van pas komt”.

In het nieuwe wetsvoorstel bijzondere opsporingsbevoegdheden (wetsvoorstel Bob) is deze materie geregeld in de derde afdeling van titel Vb getiteld “de bewaring en de vernietiging van processen-verbaal en andere voorwerpen en het gebruik van gegevens voor een ander doel”.

In art 126cc is geregeld dat, zolang de zaak niet is geëindigd, de OvJ de processen-verbaal en andere voorwerpen met betrekking tot o.a. gegevens verkregen door “onderzoek van telecommunicatie” bewaart. Deze bepaling is met name van belang omdat in art 126aa wordt bepaald dat het al of niet voegen van processen-verbaal (en andere voorwerpen) bij de processtukken afhankelijk is van het oordeel van de officier van justitie omtrent de betekenis daarvan voor het onderzoek. Nu zijn ook de gegevens die niet bij de processtukken zijn gevoegd, omdat de OvJ ze kennelijk niet relevant vond, toch beschikbaar voor bijvoorbeeld verdachte en rechter, voor het geval zij van mening zijn dat die gegevens wel relevant zijn. Op grond van het 5e lid van art 126aa kan de verdachte vervolgens verzoeken de stukken alsnog bij het procesdossier te voegen. Hiermee lijkt een van de lacunes in de wetgeving die Corstens constateerde, namelijk de ontoegankelijkheid van de niet bij de processtukken gevoegde gegevens, verholpen te zijn. Daarbij moet ik echter aantekenen dat ik vermoed dat de bevoegdheid van art 126aa lid 5 in de praktijk zelden gebruikt zal kunnen worden. Het lijkt mij namelijk

[7] Corstens, p. 419.

een hele opgave voor de verdachte en diens verdediging om op de hoogte te raken van het bestaan van stukken die niet in het procesdossier zitten. Dit vergt een dusdanig intensief onderzoek van de kant van de verdediging dat lid 5 m.i. alleen van betekenis is voor verdachten die zo vermogend zijn dat zij zichzelf kunnen voorzien van een eigen “onderzoeksapparaat”. De vraag is echter of er een wetsbepaling valt te formuleren die het bovengenoemde probleem kan voorkomen.

Uiteraard is de stap van dit artikel naar het nieuwe wetsvoorstel bijzonder opsporingsbevoegdheden en daarvandaan weer naar het wetsvoorstel wijziging Wet politieregisters snel gemaakt. Art 126dd maakt die stap dan ook. Art 126dd bepaalt dat de officier van justitie gegevens die verkregen zijn middels onderzoek/opnemen van telecommunicatie kunnen worden gebruikt voor een ander strafrechtelijk onderzoek (een andere zaak) dan wel kunnen worden opgeslagen in het register zware criminaliteit (als bedoeld in de Wet politieregisters). Dit betekent dat die gegevens dus niet conform art 126cc vernietigd hoeven te worden. Dit is niet mogelijk op grond van de huidige regeling. Art 125h opent niet de mogelijkheid tot het bewaren van gegevens die relevant zouden kunnen zijn voor toekomstige onderzoeken. Zonder wettelijke regelingen moet dat ook uitgesloten worden geacht gezien de inbreuk die het opslaan van dergelijke gegevens maakt op de persoonlijke levenssfeer van de betrokkenen.

Rechtspraak

Voor de opvatting dat de huidige regeling van art 125f en de toekomstige regeling van art 126n en art 126u niet afdoende is om aan te nemen dat de onderhavige methode geregeld is (een vereiste voor de rechtmatigheid van het gebruik van deze opsporingsmethode gezien de inbreuk die door dit middel op privacy wordt gemaakt[8]) zijn volgens mij ook aanwijzingen te vinden in een recent arrest van de Hoge Raad[9]. Hierin somt de HR de inlichtingen op die op grond van art 125f verkregen kunnen worden. Volgens de HR vallen onder die inlichtingen: “de bij het verkeer betrokken aansluitnummers, de bij het verkeer gebruikte apparatuur, het tijdstip van de aanvang en de duur van het verkeer en de vraag of daadwerkelijke communicatie heeft plaatsgevonden”. Hoewel het arrest dat niet met zoveel woorden zegt, denk ik dat de gegevens die betrekking hebben op de locatie van de mobiele telefoon niet in de door de HR gegeven invulling van het begrip “inlichtingen” in de zin van art 125f zullen vallen. Wat dat betreft is het natuurlijk (ook) voor de duidelijkheid met betrekking tot deze opsporingsmethode spijtig dat Okan O. is overleden. Gezien de verbazing en verontwaardiging van de raadsman van Okan O., vermoed ik dat deze kwestie, mocht Okan O. niet zijn overleden, wel aan de HR zou zijn voorgelegd. Overigens kan ik mij niet voorstellen dat dit middel niet in de nabije toekomst aan de kaak zal worden gesteld bij de HR nu politie en justitie deze zo op het eerste gezicht zeer handige methode ontdekt hebben. Als ik raadsman van een verdachte waartegen deze opsporingsmethode was ingezet dan zou ik het in ieder geval wel weten.

De op handen zijnde wetswijzigingen zoals voorgesteld in het wetsvoorstel Bob veranderen niets aan deze opvattingen. De artt 126n en 126u lijken nl. een kopie te zijn van het huidige art 125f. Ik denk dan ook niet dat de inzichten van de HR zich zullen wijzigen met de komst van deze twee artikelen.

Het recht op bescherming van de persoonlijke levenssfeer

Dat het onderzoek van telecommunicatie (het afluisteren en opnemen van vertrouwelijke communicatie en het vorderen van inlichtingen daarover) inbreuk maakt op de persoonlijke levenssfeer zal voor de vrijwel iedereen vanzelfsprekend zijn. Een goede aanwijzing hiervoor is art 13 lid 2 van de Grondwet waarin wordt bepaald dat het telefoongeheim onschendbaar is (behalve in de gevallen bij de wet bepaald). Een dergelijk onderzoek zal zonder wettelijke legitimatie niet alleen een inbreuk opleveren op art 13 lid 2 van de Grondwet, maar ook op art 8 EVRM.

[8] Zie ook de opmerkingen van de minister van justitie in de MvT bij het wetsvoorstel Bob.
[9] HR 7 april 1998, NJB no. 18 1998, nr. 69.

Communicatie met behulp van technische hulpmiddelen zoals telefoon, fax en computer maakt een dusdanig essentieel deel uit van ons dagelijks leven dat niet van mensen verwacht mag worden dat, indien men iets vertrouwelijks wil bespreken, men dit dan maar fluisterend en in elkaars directe bijzijn moet doen. Een andere aanwijzing voor het feit dat de inbreuk op de privacy, die bij het gebruik van de onderhavige opsporingsmethoden wordt gemaakt, substantieel is, is het vereiste van de toestemming van de rechter-commissaris voor het aftappen.

Dat met het verschaffen van informatie aan politie en justitie waaruit, met redelijk grote nauwkeurigheid, kan worden nagegaan waar iemand wanneer was ook het recht op privacy in het gedrang komt, lijkt mij eveneens voor de hand te liggen.

De privacy komt bij de toepassing van opsporingsmethoden in het kader van het onderzoek van telecommunicatie met name in de knel door twee factoren. Allereerst is er de hoge mate van heimelijkheid, die immers een voorwaarde is voor het succes van de opsporingsmethoden. Daarnaast is niet alleen de privacy van de verdachte in het geding, maar zijn er ook niet-verdachten in het spel. Met name de eerste factor is bij plaatsbepaling met behulp van mobiele telefoons van belang. Het is toch een vrij beangstigend idee om zonder dat je het weet, constant een spoor achter te laten van waar je bent geweest en dat dit spoor bovendien vele maanden blijft liggen.

De gedaante van de inbreuk bij de nieuwe methode is echter wel een andere dan bij het “conventionele” onderzoek van telecommunicatie. Mijns inziens is het tappen van een mobiele telefoon in combinatie met het vorderen van inlichtingen bij de aanbieders van telecommunicatiediensten omtrent die telefoon in belangrijke mate gelijk te stellen met het soort inbreuk dat gemaakt wordt bij het gebruik van een peilbaken. Deze combinatie van opsporingsbevoegdheden leidt nl. tot niets anders dan een registratie van de gangen van de mobiele telefoon en zijn baasje.

Als het inderdaad zo is dat de aard van de inbreuk niet alleen groter is, maar ook van een geheel andere aard als de inbreuk waar art 125f op ziet, dan moet m.i. geconcludeerd worden dat het in het geding zijnde gebruik van de opsporingsmethoden niet wettelijk geregeld is. Gelet op art 10 lid 2 en 3 en art 13 lid 2 van de Grondwet lijkt het mij verantwoord om te stellen dat een wettelijke regeling van deze opsporingsmethoden zeer zeker nodig is om het gebruik daarvan de legitimeren. Ook art 8 EVRM eist dat inbreuken op het in dat artikel beschermde privé-leven slechts gelegitimeerd kunnen zijn indien deze worden toegestaan in een nationale wettelijke regeling en de inbreuken gerechtvaardigd kunnen worden met een beroep op een van de in art 8 lid 2 genoemde gronden. Art 8 EVRM eist ook dat er sprake is van “forseeability” m.b.t. de wettelijke regeling. Het moet voor de gemiddelde rechtsgenoot duidelijk wat hem o.g.v. de wettelijke regelingen staat te wachten. Ik zou willen stellen dat onze huidige wettelijke regeling niet doet verwachten dat het mogelijk is dat je door een mobiele telefoon bij je te dragen, je jezelf bloot stelt aan het niets ontgaande oog van de GSM-palen en daarmee aan het oog van de overheid in de gedaante van politie en justitie. Hiertegen kan wellicht ingebracht worden dat het voor de wetgever ondoenlijk is om zelf alles te voorzien wat zich afspeelt op dit enorm in ontwikkeling zijnde gebied. Ik ben echter van mening dat die vlieger slechts opgaat als er een grote gelijkenis bestaat tussen de oude en nieuwe methoden (bijvoorbeeld bij het aftappen van de gewone telefoon en het aftappen van de autotelefoon). Deze gelijkenis ontbreekt hier.

Ik denk dat de Wet Persoonsregistraties geen voldoende wettelijke basis biedt voor de hier in het geding zijnde opsporingsmethode. Hoewel Mevis op grond van een uitspraak van de Hoge Raad[10], van mening lijkt te zijn dat art 11 van deze wet, indien de benodigde inlichtingen uitsluitend betrekking hebben op een van de deelnemers aan de communicatie, voldoende wettelijke basis is voor het verstrekken van deze gegevens[11], ben ik een andere mening toegedaan. M.i. kan de bepaling in de Wet Persoonsregistraties niet worden gebruikt in deze strafrechtelijke context, ook niet, zoals Mevis stelt, "in geval van dringende en gewichtige redenen en het verstrekken van de gegevens de persoonlijke levenssfeer van de geregistreerde daardoor niet onevenredig wordt geschaad". M.i. verdient de inbreuk op het recht op bescherming van de persoonlijke levenssfeer door het gebruik van deze methode een expliciete wettelijke basis in het Wetboek van Strafvordering. De specifieke problematische kanten van de in ernstige mate privacybedreigende combinatie van onderzoek van telecommunicatie en plaatsbepaling in de vorm van een soort peilbaken, gezien het louter strafrechtelijke karakter dienen door de wetgever te worden afgewogen tegen de specifieke strafrechtelijke achtergrond.

Het bovenstaande betekent dat het m.i. slechts aan de wetgever is om het gebruik van deze opsporingsmethode als rechtmatig te bestempelen. Het is naar mijn mening niet aan de rechter, justitie of politie om te bepalen dat het gebruik van deze methode verantwoord is. De wetgever dient de afweging te maken tussen het belang van de strafrechtspleging enerzijds en het belang van de bescherming van de persoonlijke levenssfeer anderzijds. Daarbij zal zij moeten aangeven in welke gevallen, op welke gronden en onder welke voorwaarden plaatsbepaling met behulp van tappen en het vorderen van inlichtingen over telecommunicatieverkeer geoorloofd is. Dit is natuurlijk allemaal niet nodig als de wetgever mocht concluderen dat deze opsporingsmethode sowieso geen deel mag uitmaken van het opsporingsbevoegdhedenpakket van politie en justitie.

Bij de bovengenoemde belangenafweging zal de wetgever overigens in ieder geval moeten letten op de proportionaliteit en de subsidiariteit, zoals het ook is gebeurd in art 125g ("indien het onderzoek dit dringend vordert"). En dan natuurlijk liefst ietsje duidelijker.

Van Traa

Het in het geding zijnde gebruik van de bevoegdheden tot onderzoek van telecommunicatie waren hoogstwaarschijnlijk niet bekend bij de parlementaire commissie opsporingsmethoden (PEC). Ik heb in ieder geval niets daarover kunnen terugvinden in het verslag van haar onderzoek[12].

Van belang is wel dat de PEC constateert dat verschillende in de praktijk gebruikte observatiemethoden geen uitdrukkelijke wettelijke basis hebben. De PEC heeft het over een "wildgroei aan opsporingsmethoden"[13]. De PEC stelt vast dat er te veel discussie mogelijk is over de vraag of de inzet van bepaalde observatiemethoden al dan niet rechtmatig is[14]. Daar waar inbreuk gemaakt wordt op de fundamentele rechten van de burger, en dat is bij langdurige observatie het geval, dient er een wettelijke basis te zijn voor de gebruikte methoden (tenzij er sprake is van een noodtoestand). Zowel inhoud als procedure van de gebruikte observatiemethoden was veelal niet of te summier geregeld. Ook op het gebied van de observatiemethoden deed de normeringscrisis zich dus voor. De controle op het gebruik van observatiemethoden moet volgens de PEC zowel voorafgaand aan de toepassing als achteraf (door de rechter) meer invulling krijgen. De PEC pleit dan ook voor grote openheid m.b.t. de gebruikte methoden.

[10] HR 8 november 1994, DD 95.085
[11] T&C, art 125f, aant. 6b.
[12] Inzake opsporing, Enquetecommissie opsporingsmethoden, SDU 1996
[13] Idem, p.432
[14] Idem, p.205ev

Gebrek aan inzicht in en controle en toezicht op de gehanteerde opsporingsmethoden is onverantwoord uit het oogpunt van de rechtsstaat en onverantwoord uit het oogpunt van behoorlijk bestuur. De overheid als geheel is hier tekortgeschoten, zo stelt de PEC[15].

Gezien de bevindingen en aanbevelingen van de PEC kan ik het mij niet voorstellen dat de PEC de plaatsbepaling via mobiele telefoons, als deze methode niet expliciet wettelijk geregeld is, geoorloofd zou hebben geacht.

Andere "vergelijkbare" vormen van plaatsbepaling

Begin jaren '90 maakt de politie gebruik van een apparaatje genaamd de Kolibrie, waarmee vrij eenvoudig de gesprekken die worden gevoerd met een autotelefoon kunnen worden afgeluisterd. De politie verklaarde destijds dat er geen sprake was van afluisteren van telecommunicatie omdat er slechts gebruik werd gemaakt van de kolibries om te achterhalen waar iemand naar toe ging. Dit om de observatie te vergemakkelijken. Later is men tot het inzicht gekomen dat het hier natuurlijk gewoon "aftappen" van telecommunicatie betrof.

Een andere opsporingsmethode waar plaatsbepaling en onderzoek van telecommunicatie elkaar raken, is de mogelijkheid om iemands locatie te bepalen door op grond van art 125g te tappen en vervolgens o.g.v. art 125f de gegevens m.b.t. de gevoerde gesprekken te vorderen. Luisterend naar de opnames van de gesprekken bepaal je wie er heeft gebeld op een bepaald tijdstip. De inlichtingen van het telecommunicatiebedrijf wijzen vervolgens uit vanaf welke aansluiting diegene belde en zodoende ook waar diegene zich bevond.

Hoewel de methode zo op het eerste gezicht lijkt op de plaatsbepaling met behulp van de locatiegegevens van de mobiele telefoon, is deze combinatie van de bevoegdheden uit de artikelen 125f en 125g toch minder ingrijpend te noemen met het oog op de aantasting van de privacy. De belangrijkste reden hiervoor zijn m.i. dat van diegene die "gevolgd" wordt, niet constant de plaats waar hij zich bevindt kan worden bepaald, maar slechts op de momenten dat hij telefoneerde via het getapte toestel. Het Big-Brother-is-watching-you-element is dus minder sterk aanwezig. Dat is dan ook de reden waarom ik van mening ben dat de huidige regeling voor deze vorm van handig combineren van bevoegdheden voldoende is.

Tenslotte nog een blik op de toekomst. Moderne technieken brengen steeds nieuwe mogelijkheden om iemand te traceren. Niet alleen door de apparatuur die politie en justitie gebruiken, maar ook door de wonderen der techniek waar de verdachte over beschikt. Zo is op dit moment wel te voorzien dat er ooit (zeg over een jaar of tien) de meeste (nieuwe) auto's voorzien zullen zijn van een boordcomputer, die allerlei informatie heeft over de situatie op de weg van A naar B. Deze actuele informatie zal steeds worden aangevuld en ververst. De boordcomputer zal deze informatie ontvangen. Het komt mij heel waarschijnlijk voor dat elke auto/boordcomputer (net zoals dat overigens ook bij gewone computers het geval is) zijn eigen identificatienummer heeft en als zodanig dan ook herkend kan worden. Het zal dan net als bij de mobiele telefoon mogelijk zijn om te traceren waar de auto zich bevindt. En zo is er dan weer een nieuwe manier van plaatsbepaling geboren. En Big Brother vaart er wel bij.

[15] Idem, p 433

Conclusie

Op grond van het voorgaande moet geconcludeerd worden dat de combinatie van de methoden van onderzoek van telecommunicatie, om daar vervolgens iemands locatie te bepalen, als het gaat om mobiele telefonie, niet geregeld is. De huidige regeling omvat niet het m.b.v. onderzoek van telecommunicatie lokaliseren van verdachten. Het strekt dan ook tot de aanbeveling om deze materie expliciet te regelen in het Wetboek van Strafvordering, indien de wetgever deze methode als geoorloofd ziet. De inbreuk die door deze opsporingsmethode op de privacy gemaakt wordt is simpelweg te ernstig en wijkt teveel af van de wijze waarop de methode van art 125f en 125g inbreuk maakt op de privacy om af te zien van expliciete regeling van deze materie. Ook kan de ernst van de inbreuk niet worden afgedaan met opmerkingen als “wie niet wil dat hij gevolgd wordt via zijn GSM, moet hem dan maar uitzetten”. Dit is veel te simpel gedacht. Mevis[16] en de Hoge Raad[17] zijn ook deze mening toegedaan.

Indien de wetgever besluit deze methode wettelijk te gaan regelen is het wellicht raadzaam daarbij te kijken naar de regeling van de observatie in art 126g van het wetsvoorstel Bob. Betoogd kan immers worden dat deze combinatie van methoden van onderzoek van telecommunicatie verdacht veel lijkt op een observatiemethode. Wellicht dat de criteria van stelselmatigheid die de wetgever in dat kader hanteert dan ook, voor zover in deze en überhaupt bruikbaar, van dienst kunnen zijn. De algemene criteria voor observatie spelen ook nu een rol in de jurisprudentie die betrekking heeft op observatie[18].

De vraag is echter wat in deze wijsheid is. Moderne technieken brengen niet alleen met zich mee dat wij steeds mobieler worden, steeds meer werk kunnen laten verrichten door technische hulpmiddelen, en tot dingen in staat zijn waarover we een eeuw geleden nog niet *konden* dromen (ik zal maar even in het midden laten of we er van durfden dromen). Deze voortschrijding der techniek, met name op het gebied van het verzamelen, opslaan en verplaatsen van allerhande “gegevens”, heeft ook tot gevolg dat het schrikbeeld van “Big Brother is watching you”, dat zo indringend werd beschreven in George Orwell’s 1984, steeds dichterbij lijkt te komen.

“The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any given individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live - did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinised”.

Zover zijn we natuurlijk nog niet, ook niet als de plaatsbepaling m.b.v. gegevens over de locaties van de mobiele telefoon een regelmatig en rechtmatig gebruikt opsporingsmiddel wordt. Minder erg dan de in “1984” beschreven situatie, omdat hier de methode slechts ruwweg de locatie van de verdachte (althans van zijn telefoon) vastlegt. Daar staat tegenover dat deze methode ook in het donker werkt in tegenstelling tot het “telescreen”.

Maar het gevaar van een wereld waarin privacy voor sommigen (bijv. de door de overheid als verdachte (van een misdrijf) aangemerkte personen) een wel heel erg schaars goed wordt is reëel.

[16] T&C Sv, art 125g, aant. 15b.
[17] HR 19 december 1995, NJ 1996, 249 en HR 23 januari 1996, DD 96.178.
[18] Inzake opsporing, p. 178.

Een verdachte kan (als politie en justitie het de moeite waard en bovendien geoorloofd achten) in de gaten gehouden worden met camera's, afluisterapparatuur in vele verschijningsvormen, peilbakens, vingerafdrukken, DNA-materiaal, infiltranten, schaduwende agenten, vuilnissnuffels en natuurlijk niet te vergeten door het opvragen van allerlei gegevens bij banken, computers en telecommunicatiebedrijven! En dat allemaal zonder dat de verdachte er erg in heeft, voor zover het natuurlijk prettig is om wel te weten dat al je bewegingen worden waargenomen. Je moet er niet aan denken.

Wat ik nu met dit verhaal over de Staat der Nederlanden in de rol van Big Brother wil zeggen is het volgende: ik ben van mening dat ondanks het feit dat elke in Nederland in de wet bestaande opsporingsmethode op zichzelf best te rechtvaardigen is door een beroep te doen op het belang van de strafrechtspleging, we niet uit het oog mogen verliezen dat de lijst van opsporingsbevoegdheden al maar langer en langer wordt en dat het einde, gezien de ontwikkelingen in de technische en medische/biologische wetenschappen nog lang niet in zicht is. Ik denk dat we er voor moeten waken elke opsporingsmethode afzonderlijk te beoordelen m.b.t. de mogelijke inbreuk op de persoonlijke levenssfeer, maar vooral ook op de combinatie van de methoden die op de steeds langer wordende lijst van bijzondere opsporingsbevoegdheden staan. Dit zal m.i. zowel bij het accepteren van opsporingsmethoden in de wet, als bij de afweging van belangen die in de praktijk vooraf zal moeten gaan aan toepassing moeten gebeuren. De bovenbedoelde extra zorgvuldigheid moet met name in acht worden genomen daar waar gelijktijdige combinatie van methoden mogelijk is. Iets waar, bij plaatsbepaling via iemands mobiele telefoon, sprake van is. Je tapt de mobiele telefoon, om vervolgens na te gaan waar die telefoon zich gedurende (een deel van) de tapperiode bevond. Bij een dergelijke combinatie is grote behoedzaamheid vereist.

Indien de wetgever besluit dat deze methode wettelijke regeling behoeft, en deze ook krijgt, dan dient vervolgens zo expliciet mogelijk geregeld te worden wanneer en hoe deze methode mag worden ingezet, om zo te voorkomen dat de mensen die in de praktijk deze methode (gaan) gebruiken zelf op zoek moeten gaan naar de grenzen van dit opsporingsinstrument. Op duidelijke wijze dienen de gronden waarop, de gevallen waarin en de voorwaarden waaronder de opsporingsmethode mag worden toegepast te worden omschreven.

Zo zal de vraag aan de orde moeten komen of de methode alleen gebruikt mag worden om bij te dragen tot het bewijs van reeds gepleegde feiten of dat deze methode bijvoorbeeld ook reeds mag worden gebruikt om de georganiseerde criminaliteit in kaart te brengen? Overigens denk ik dat het raadzaam is te bepalen dat indien er geen gesprekken zijn gevoerd door de verdachte op of omstreeks het tijdstip van locatiebepaling, de plaatsbepaling van de mobiele telefoon slechts als ondersteunend bewijs mag dienen. Je kan immers niet zeker weten dat de eigenaar van de telefoon ook daadwerkelijk de telefoon altijd bij zich draagt.

Ook zal bepaald moeten worden wanneer de situatie noopt tot inzet van dit middel. Wat moet er gebeuren wil dit middel ingezet mogen worden?

Tenslotte moet worden bepaald in welke fase van het onderzoek dit middel gebruikt mag worden en of er wellicht een rechter-commissaris aan te pas moet komen om de inzet van deze methode geoorloofd te maken.

Dit alles brengt mij tot de slotsom: bezint eer ge met weer een nieuwe opsporingsmethode begint!

Gebruikte bronnen

- Procesdossier Okan O.
- Enkele naar aanleiding van de zaak Okan O. verschenen krantenartikelen
- Het NJB, de NJ en de DD.
- Corstens, Het Nederlandse Strafprocesrecht, 2e druk 1995
- Tekst en Commentaar Strafvordering, 2e druk 1997
- Reader “Actualiteiten strafvordering” 1998
- Inzake opsporing, eindrapport van de parlementaire commissie opsporingsmethoden
- P.J.P. Tak (red.) Bespiegelingen omtrent de Wet Bijzondere Opsporingsbevoegdheden, Politiestudies nr. 21, 1998
- Y. Buruma/P.C. Vegter, Buitengewone opsporingsmethoden, studiepocket strafrecht nr 34, 1998
- George Orwell, Nineteen Eighty-Four, voor het eerst gepubliceerd in 1949
- Vademecum Strafzaken
- Wetsvoorstel bijzondere opsporingsbevoegdheden en de Memorie van Toelichting daarop