DE MOBIELE TELEFOON ALS PEILBAKEN

MAG DAT ?

uit
Ars Aequi
Jaargang 49-9, september 1999

Benno de Boer (UVA)

"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". (Fragment uit 1984 van George Orwell)

Enige tijd geleden stond in de Volkskrant van 26 mei 1999 het bericht dat de verdachten van de moord op de prefect van Corsica hadden bekend de moord te hebben gepleegd nadat zij waren geconfronteerd met gegevens waaruit bleek dat de mobiele telefoons van de verdachten zich allemaal op het tijdstip van de moord in de buurt van het theater hadden bevonden, waar de moord zich had voltrokken. Ook in Nederland heeft zich enige tijd geleden een zaak voorgedaan waarbij een verdachte werd verraden door zijn mobiele telefoon. In dit artikel wordt de vraag aan de orde gesteld of de wijze waarop dit is gebeurd wel gelegitimeerd is.

1 Inleiding

Op zaterdag 20 september 1997 vond in café De Plakhoek in Amsterdam een schietpartij plaats. Bij deze schietpartij werd een zogenaamde 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., bekend van de vele aan hem gewijde afleveringen van het populaire televisieprogramma Peter R. de Vries misdaadverslaggever, naar voren als deelnemer aan en aanstichter van de schietpartij. Na een geruchtmakend proces werd Okan O. veroordeeld tot een gevangenisstraf van vier jaar. Niet lang na die veroordeling overleed Okan O. aan kanker. Het is dan ook niet tot een hoger beroep in de zaak gekomen.

Na zijn aanhouding ontkende Okan O. 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. Ter terechtzitting

bleek echter dat het OM een aardige troef in handen had waarmee zij zei te kunnen bewijzen dat Okan O. wel op het tijdstip van de schietpartij in de omgeving van café De Plakhoek was. Vanaf zogenaamde GSM-palen wordt namelijk constant gepeild waar elke mobiele telefoon zich bevindt. De Officier van Justitie (verder: OvJ) liet ter terechtzitting een uitdraaitje van de zogenaamde locatiegegevens van de telefoon van Okan O. zien, waaruit volgens de OvJ bleek dat (de telefoon van) Okan O. zich op het tijdstip van de schietpartij wel degelijk in de buurt van De Plakhoek bevond.

Bovenstaand verhaal roept verschillende vragen op. De belangrijkste daarvan is de vraag of de huidige regeling van het onderzoek van telecommunicatie in het Wetboek van Strafvordering (verder: Sv) het eerdergenoemde gebruik van de mobiele telefoon als een soort peilbaken wel toestaat. Is het met behulp van de van een telecommunicatiebedrijf verkregen locatiegegevens van een mobiele telefoon met terugwerkende kracht traceren van een persoon op basis van de artikelen 125f en 125g Sv wel geoorloofd? Bij het beantwoorden van die vraag dient natuurlijk ook de nieuwe regeling van de Wet bijzondere opsporingsbevoegdheden (verder: Wet Bob) te worden betrokken. Indien de in de zaak van Okan O. gebruikte opsporingsmethode niet wettelijk geregeld is en de methode wel een substantiële inbreuk maakt op de persoonlijke levenssfeer, dan zal gebruik van dit middel ongeoorloofd 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 (§2). Daarna zal ik de huidige wettelijke regeling van het vorderen van inlichtingen over telecommunicatie (§3.1) en de regeling van het tappen (§3.2) onder de loep nemen en proberen te achterhalen of het gebruik van de mobiele telefoon als peilbaken in deze bepalingen geregeld is. Vervolgens zal ik aandacht besteden aan de inbreuk die de in de zaak Okan O. gebruikte methode maakt op het recht op privacy en onderzoeken of de door de Grondwet en het EVRM vereiste wettelijke regeling om deze inbreuk te rechtvaardigen aanwezig moet worden geacht (§4). Ik sluit af met enige conclusies naar aanleiding van de hiervoor genoemde paragrafen en zal tot slot mijn vizier op de toekomst van de opsporing richten (§5).

2 Plaatsbepaling en mobiele telefoons

In de zaak Okan O. is mede op grond van inlichtingen verstrekt door KPN Telecom aan politie en justitie de verblijfplaats van Okan O. op het tijdstip van de schietpartij wettig en overtuigend bewezen. Deze inlichtingen hadden 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 KPN (en de andere telecommunicatiebedrijven) geregistreerd waar elke telefoon zich bevindt. In de zaak van Okan O. werd duidelijk dat de plaatsbepaling geschiedt middels zend- en ontvangstbakens van KPN, de zogenaamde GSM-palen. Ongeveer een half jaar voor de uitspraak in de zaak Okan O. ontkenden de aanbieders van telecommunicatiediensten in Nederland nog het feit dat de gegevens met betrekking tot de locatie van de mobiele telefoons worden geregistreerd en bewaard in hun computers. Een Zwitserse krant onthulde destijds dat de gangen van een mobiele telefoon op de minuut en op enkele honderden meters nauwkeurig kunnen worden nagegaan. Dit heeft het Zwitserse telecommunicatiebedrijf Swisscom indertijd bevestigd. In de zaak Okan O. verklaarde een

medewerker van KPN dat in Nederland (in stedelijk gebied) ongeveer om de drie kilometer een GSM-paal staat. Dezelfde medewerker van KPN verklaarde ook dat de gangen van Okan O. alleen nagegaan hadden kunnen worden, doordat er gebruik was gemaakt van de voicemail van de telefoon. KPN registreert signalen die de mobiele telefoon uitzendt bij het doorschakelen van inkomende gesprekken naar de voicemail, zo stelde de medewerker van de KPN. Inmiddels is gebleken dat de computers van de KPN constant op de hoogte (moeten) worden gehouden van de locatie van de mobiele telefoon. In verband met de bestrijding van fraude (bellen op andermans kosten) worden deze call detail records vervolgens voor onbekende tijd bewaard. De tijd dat deze locatiegegevens bewaard worden is, overigens van belang in verband met de controleerbaarheid van die gegevens voor de zittingsrechter en voor de verdediging van de verdachte.

Uiteraard 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. Ook de Parlementaire Enquêtecommissie Opsporingsmethoden (verder: PEC) pleitte in haar rapport voor grote openheid met betrekking tot gebruikte opsporingsmethoden. Gebrek aan inzicht in en controle en toezicht op de gehanteerde opsporingsmethoden is volgens de commissie onverantwoord uit het oogpunt van de rechtsstaat en uit het oogpunt van behoorlijk bestuur. In reactie op het door de commissie Van Traa gestelde eist het nieuwe artikel 126ee Sv (Wet Bob) dan ook duidelijkheid over de nauwkeurigheid en controleerbaarheid van methoden waarbij gebruik wordt gemaakt van technische hulpmiddelen.

3 Onderzoek van telecommunicatie

3.1 Het verstrekken van inlichtingen

Artikel 125f Sv

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). Vanaf dat moment kon ook ander gegevensverkeer op rechtmatige wijze worden onderzocht. Deze regeling is nu nog te vinden in de artikelen 125f t/m 125h Sv.

Artikel 125f Sv biedt de OvJ (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 deze inlichtingen verschaffen met betrekking tot "alle verkeer dat over de telecommunicatie-infrastructuur of over een telecommunicatie-inrichting die wordt aangewend voor dienstverlening aan het publiek, heeft plaatsgevonden en ten aanzien 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 verplicht de bovengenoemde gegevens te verstrekken, behoudens de aanwezigheid van een verschoningsrecht. Het niet voldoen aan de vordering inlichtingen te verstrekken, is in artikel 184 Sr strafbaar gesteld.

Artikel 126n en artikel 126u Sv

Op 25 mei 1999 is het wetsvoorstel Wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden) (25 403) aangenomen door de Eerste Kamer. De wet zal per 1 februari 2000 in werking treden. Met de komst van de nieuwe wet blijven de genoemde bezwaren bestaan (3.1.1.). De artikelen 126n en 126u Sv zijn, voorzover van belang voor de hier aan de orde zijnde vraag, een kopie van het huidige 125f Sv.

3.2 Reikwijdte van de bepalingen

In de praktijk wordt de bevoegdheid van artikel 125f Sv onder meer gebruikt om te achterhalen met welke nummers, hoelang 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. In een recent arrest bevestigt de Hoge Raad dat de in artikel 125f Sv bedoelde vordering tevens betrekking kan hebben op verkeer dat nog moet plaatsvinden en waarvan het vermoeden bestaat dat de verdachte eraan zal gaan deelnemen.

Tijdens de behandeling van het wetsvoorstel Bob stelde de GPV-fractie expliciet de vraag of het "onder de vigeur van dit artikel (artikel 126n Sv, BdB) is toegestaan om achteraf de plaats te bepalen van waaruit een verdachte heeft gebeld (cursief: BdB)". De toenmalige Minister van Justitie antwoordde toen: "de onderhavige bevoegdheid is al sinds lang in onze wetgeving opgenomen. () Voor zover verkeersgegevens, in aanvulling op reeds bij de politie aanwezige informatie, uitsluitsel zouden kunnen geven over de plaats van waaruit gebeld is, staat de wettekst er niet aan in de weg op deze wijze de plaats te bepalen". Spijtig genoeg is niet duidelijk of de minister hier ook mobiele telefonie voor ogen stond. Duidelijk is wel dat het hier om de situatie gaat waar wel is gebeld (cursief: BdB). Het betreft hier dus gegevens met betrekking tot de totstandgekomen communicatie tussen mensen. Ik denk dan ook dat uit de woorden van de minister niet ondubbelzinnig kan worden afgeleid dat alle locatiegegevens mogen worden opgevraagd op grond van het nieuwe artikel 126n Sv (om zo een compleet beeld te krijgen van de door de mobiele telefoon in een bepaalde periode afgelegde route). Dit zou immers betekenen dat de mobiele telefoon gaat functioneren als een peilbaken. Een peilbaken is een technisch hulpmiddel ter observatie van een verdachte. Het gebruik hiervan is geregeld in het centrale observatieartikel 126g lid 3 Sv (Wet Bob). Daar is echter ondubbelzinnig te lezen dat een dergelijk technisch hulpmiddel niet op een persoon bevestigd mag worden, tenzij de persoon in kwestie toestemming daarvoor heeft gegeven. Een ruime interpretatie van de woorden van de minister (inhoudende dat zij het oog had op alle locatiegegevens van mobiele telefoons) lijkt mij dan ook in strijd met het bepaalde in artikel 126g Sv.

Mevis noemt als mogelijke gegevens die onder het bereik van artikel 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 van de verbinding is dan kennelijk voldoende, daadwerkelijke communicatie tussen personen lijkt niet te hoeven plaatsvinden. De rechtbank gaat echter een stap verder in de zaak Okan O.:

"Uit de parlementaire geschiedenis van artikel 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 artikel 125f Sv in de daar genoemde gevallen inlichtingen gevorderd kunnen worden door het openbaar ministerie."

Blijkens de bewoordingen van artikel 125f Sv betreffen de inlichtingen alle verkeer waarvan wordt vermoed dat de verdachte daaraan heeft deelgenomen. Het komt mij voor dat, wil er sprake zijn van het in artikel 125f Sv bedoelde verkeer, er sprake moet zijn van enige handeling van de zijde van minstens één van de deelnemers aan het verkeer. De rechtbank, zo blijkt hierboven, rekent echter ook alle tussen de mobiele telefoon en de computers/GSM-palen van de netwerkbeheerder verzonden signalen tot de inlichtingen betreffende alle verkeer met behulp van telecommunicatie.

Ten aanzien van de grond voor het vorderen van de inlichtingen staat niets in artikel 125f. Dat is jammer, want zou dat wel het geval geweest zijn, dan zou daarin wellicht een aanwijzing te vinden zijn geweest omtrent de toelaatbaarheid van plaatsbepaling op grond van dit artikel.

Het heeft er mijns inziens alle schijn van dat de plaatsbepaling middels mobiele telefonie niet is geregeld in artikel 125f Sv. In het Vademecum Strafzaken wordt ten aanzien van de reikwijdte van dit artikel gesteld "Artikel 125f Sv (.) is beperkt tot het onderzoek naar de vraag vanaf welke aansluitpunten is gecommuniceerd en voor hoelang." Buruma en Vegter stellen met betrekking tot artikel 125f: " Artikel 125f Sv is geen observatiebevoegdheid."

Voor de opvatting dat de huidige regeling van artikel 125f Sv en de toekomstige regeling van artikel 126n en 126u Sv niet de onderhavige methode regelt, zijn volgens mij ook aanwijzingen te vinden in het bovengenoemde arrest van de Hoge Raad. Hierin somt de Hoge Raad de inlichtingen op die op grond van artikel 125f verkregen kunnen worden. Volgens de Hoge Raad vallen onder die inlichtingen: "inlichtingen omtrent de wijze van totstandkoming en afwikkeling van het telecommunicatieverkeer, zoals 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." De Hoge Raad geeft geen voorbeeld dat dusdanig geïnterpreteerd kan worden dat daaronder redelijkerwijs ook de locatiegegevens van een mobiele telefoon vallen. Dat zou alleen dan mogelijk zijn indien duidelijk zou zijn dat de Hoge Raad onder telecommunicatieverkeer ook van de menselijke communicatie onafhankelijke gegevensuitwisseling tussen mobiele telefoon en computer (van bijvoorbeeld KPN) rekent.

Wat dat betreft is het natuurlijk (ook) voor de duidelijkheid met betrekking tot deze opsporingsmethode spijtig dat Okan O. is overleden. Gezien de (terechte) verbazing en verontwaardiging van de raadsman van Okan O. over de door justitie gebruikte methode in deze zaak, vermoed ik dat deze kwestie, mocht Okan O. niet zijn overleden, wel aan de Hoge Raad 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 Hoge Raad nu politie en justitie deze zo op het eerste gezicht zeer handige methode ontdekt hebben. Als ik raadsman zou zijn van een verdachte waartegen deze opsporingsmethode was ingezet, dan zou ik het in ieder geval wel weten.

3.3 Afluisteren of opnemen van telefoongesprekken

Artikel 125g Sv 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 artikel 125f Sv.

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

Waarom is artikel 125g Sv in dit kader van belang? Bij de plaatsbepaling met behulp van de locatiegegevens van de mobiele telefoon is de tapbevoegdheid nodig om te kunnen bepalen of de verdachte daadwerkelijk de telefoon bij zich had. Alleen als de verdachte met de mobiele telefoon een afgeluisterd gesprek heeft gevoerd, kan dat aangetoond worden. Als inlichtingen met betrekking tot de plaats waar de mobiele telefoon zich heeft bevonden vallen onder "alle verkeer" van artikel 125f Sv en er op grond van dat artikel gegevens opvraagd worden, dan is zonder het gebruik van de bevoegdheid uit artikel 125g Sv alleen de plaats van de telefoon te bepalen, zonder dat te achterhalen valt wie die telefoon bij zich droeg. Was het de verdachte, zijn vriendin of toch die zakenpartner van hem?

4 **Het recht op bescherming van de persoonlijke levenssfeer**

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

De gedaante van de inbreuk bij het opvragen van locatiegegevens is echter 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 het door de telefoon afgelegde traject in belangrijke

mate gelijk te stellen met het soort inbreuk dat gemaakt wordt bij het gebruik van een peilbaken.

Gelet op artikel 10 lid 2 en 3 en artikel 13 lid 2 van de Grondwet en artikel 8 EVRM is het noodzakelijk dat daar waar opsporingsmethoden een substantiële inbreuk maken op het recht op privacy van de burger een wettelijke regeling bestaat die het gebruik van deze opsporingsmethoden legitimeert. Artikel 8 EVRM eist dat er sprake is van 'forseeability' met betrekking tot de wettelijke regeling. Het moet voor de gemiddelde rechtsgenoot duidelijk zijn wat hem op grond van 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 daardoor wellicht ook aan het oog van de overheid in de gedaante van politie en justitie. Hetgeen ik in §3 ten aanzien van de reikwijdte van de huidige regeling van het onderzoek van telecommunicatie heb gesteld lijkt hiervoor een duidelijke aanwijzing te zijn.

Als we concluderen dat de regeling in art 125f Sv niet toegesneden is op de hier aan de orde zijnde opsporingsmethode, moet, voordat geconcludeerd kan worden dat niet is voldaan aan de eisen van artikel 10 Grondwet en artikel 8 EVRM, onderzocht worden of het gebruik van de mobiele telefoon als peilbaken wellicht door een andere wettelijke regeling gelegitimeerd kan worden.

Mevis stelt in Tekst en Commentaar het volgende: "inlichtingen die uitsluitend betrekking hebben op één der participanten (bijv. omtrent de tenaamstelling van een bepaald abonneenummer van telefoon of fax) zijn geen onderdeel van het verkeer en kunnen dus via andere wegen worden opgevraagd; de beperkte regeling (beslissing OvJ of r-c) van artikel 125f Sv hoeft niet te worden gevolgd: HR 11 februari 1986, NJ 1986, 661." En verder stelt hij nog: "Voor zover sprake is van een persoonsgegeven voorziet artikel 11 Wet Persoonsregistraties in de wettelijke basis om, in geval van dringende en gewichtige reden, desgevraagd gegevens te verstrekken voor zover de persoonlijke levenssfeer van de geregistreerden daardoor niet onevenredig wordt geschaadt". Ik ben van mening dat de Wet Persoonsregistraties in geen geval voldoende wettelijke basis biedt voor de hier in het geding zijnde opsporingsmethode. Mijns inziens verdient de inbreuk op het recht op privacy die door het gebruik van deze methode wordt gemaakt een expliciete wettelijke basis in het Wetboek van Strafvordering. Gezien het louter strafrechtelijke karakter dienen de specifieke problematische kanten van de in ernstige mate privacybedreigende combinatie van onderzoek van telecommunicatie en plaatsbepaling in de vorm van een soort peilbaken door de wetgever te worden afgewogen tegen de specifieke strafrechtelijke achtergrond.

Ook een verwijzing naar de in het verleden veelvuldig als bevoegdheidstoekennende bepalingen misbruikte artikelen 2 Politiewet 1993 en artikel 141 Sv is mijns inziens niet afdoende om te stellen dat de methode in kwestie een wettelijke basis heeft. Deze bepalingen zijn te algemeen geformuleerd. In het bekende Zwolsman-arrest stelde de Hoge Raad expliciet dat daar waar door opsporingsmethoden inbreuk wordt gemaakt op fundamentele rechten van de burger, dit alleen dan is toegestaan als zon bevoegdheid voldoende kenbaar en voorzienbaar in de wet is omschreven. Het algemeen geformuleerde artikel 2 Politiewet voldoet dan ook niet aan die eisen, aldus de Hoge Raad. De voortschrijdende ontwikkeling van het recht op privacy en de toenemende technische verfijning en intensivering van onderzoeksmethoden en technieken verlangen een meer precieze legitimatie voor inbreuken op het recht op privacy dan artikel 2 Politiewet biedt.

Met de bovenstaande overwegingen in gedachte kan mijns inziens slechts geconcludeerd worden dat het aan de wetgever is om het gebruik van de hier besproken opsporingsmethode als rechtmatig te bestempelen. Het is niet aan de rechter, justitie of politie om te bepalen dat het gebruik van deze methode verantwoord is. Dit valt ook op te maken uit de woorden van de voormalige Minister van Justitie Sorgdrager. In reactie op vragen uit de Tweede Kamer stelde zij (ongetwijfeld mede naar aanleiding van het door de PEC gestelde) dat daar waar opsporingsmethoden een ernstige inbreuk op de privacy opleveren, deze methoden niet toegepast kunnen worden zolang zij niet wettelijk geregeld zijn. Een rechterlijke inkadering levert volgens haar geen begaanbare weg op. Onze Grondwet, zo betoogt zij, eist in deze een expliciete, voldoende specifieke basis in de wet in formele zin. Zij stelt dan ook dat daar waar dergelijke methoden worden gebruikt, voorafgaand aan een expliciete regeling, het gebruik van deze methoden in het algemeen niet tot bewijsmateriaal zal leiden dat de rechter zal willen toelaten. Als voorbeeld hiervan kan een recente uitspraak van de rechtbank Assen dienen. De rechtbank overwoog ten aanzien van de gebezigde opsporingsmethoden (stelselmatige observatie) onder andere "dat niet gezegd kan worden dat voor deze vergaande inbreuk op de in artikel 8 EVRM en artikel 10 Grondwet gewaarborgde rechten van de verdachte een voldoende wettelijke grondslag gevonden kan worden in artikel 2 Politiewet 1993 en artikel 141 Sv. Derhalve dient de gehanteerde opsporingsmethode als onrechtmatig te worden aangemerkt." Dit had in casu bewijsuitsluiting tot gevolg.

De wetgever dient dus de afweging te maken tussen het belang van de strafrechtspleging enerzijds en het belang van de bescherming van de persoonlijke levenssfeer anderzijds. Bij deze belangenafweging zal de wetgever in ieder geval moeten letten op de proportionaliteit en de subsidiariteit, zoals het ook is gebeurd bij artikel 125g Sv (indien het onderzoek dit dringend vordert). En dan natuurlijk bij voorkeur iets duidelijker geformuleerd. De wetgever zal dan ook 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 laatste 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.

5 **Conclusie**

Op grond van het voorgaande moet geconcludeerd worden dat - daar waar het gaat om de mobiele telefonie het combineren van de bestaande methoden van onderzoek van telecommunicatie, om vervolgens aan de hand van de verkregen locatiegegevens de gangen van de verdachte te achterhalen, niet geregeld is. De huidige regeling omvat dus niet het met behulp van het onderzoek van telecommunicatie (vooraf of achteraf) permanent kunnen lokaliseren van verdachten. Het strekt dan ook tot aanbeveling om deze materie expliciet te regelen in het Wetboek van Strafvordering, indien de wetgever deze methode geoorloofd vindt. De zaak kan niet worden afgedaan door te stellen dat de wetgever nu eenmaal niet alle technische ontwikkelingen kan voorzien. De inbreuk die door deze opsporingsmethode op de privacy gemaakt wordt, is daarvoor simpelweg te ernstig en wijkt te veel af van de wijze waarop de methoden van artikel 125f en 125g Sv inbreuk maken op de privacy. Ook kan de ernst van de inbreuk niet worden afgedaan met opmerkingen als "wie niet wil dat hij gevolgd wordt via zijn GSM, moet zn mobiele telefoon

(inclusief voicemail) dan maar uitzetten". Dit is veel te simpel gedacht. Mevis en de Hoge Raad kunnen zich ook niet vinden in dergelijke gedachten.

Indien de wetgever besluit dat deze methode wettelijk geregeld moet worden, 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 kunt 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? Ten slotte 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. Bij dit alles is het raadzaam om de regeling van de stelselmatige observatie in artikel 126g Sv van de Wet Bob voor ogen te houden. Betoogd kan immers worden dat deze combinatie van methoden van onderzoek van telecommunicatie verdacht veel lijkt op de in dat artikel geregelde observatie. De bepaling dat een technisch hulpmiddel ter ondersteuning van de observatie niet op een persoon bevestigd mag worden, dient daarbij niet over het hoofd gezien te worden.

Natuurlijk is het voor de wetgever verleidelijk om deze zo op het eerste gezicht voor politie en justitie zeer handige opsporingsmethode te legaliseren. De vraag is echter wat in dezen wijsheid is. Moderne technieken brengen 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 ervan durfden dromen). Deze voortschrijding der techniek, met name op het gebied van het verzamelen, opslaan en verplaatsen van allerhande gegevens, heeft echter ook tot gevolg dat het schrikbeeld van Big Brother is watching you, dat zo indringend werd beschreven in George Orwells 1984, steeds dichterbij lijkt te komen. Maar zover zijn we natuurlijk nog niet, ook niet als de plaatsbepaling met behulp van de locatiegegevens van de mobiele telefoon een regel- en rechtmatig gebruikt opsporingsmiddel wordt. De methode is minder ingrijpend dan de in 1984 beschreven situatie, omdat hier de methode slechts ruwweg de locatie van de verdachte (althans van zijn telefoon) vastlegt. Daar staat echter wel tegenover dat deze methode echt overal en altijd werkt, dit in tegenstelling tot het nog fictieve telescreen.

Maar het gevaar van een wereld waarin privacy voor sommigen (bijv. voor de door de overheid als verdachte aangemerkte personen) een wel heel erg schaars goed wordt is reëel. Een verdachte kan (als politie en justitie het de moeite waard en bovendien geoorloofd achten) in de gaten gehouden worden door middel van cameras, 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!

Voorzover 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, medische en biologische wetenschappen, nog lang niet in zicht is. Ik denk dat we ervoor moeten waken niet alleen elke opsporingsmethode afzonderlijk te beoordelen met betrekking tot de mogelijke inbreuk op de persoonlijke levenssfeer, maar dat we vooral ook moeten letten op de gevolgen van het combineren van de methoden die op de steeds langer wordende lijst van bijzondere opsporingsbevoegdheden staan. Deze extra zorgvuldigheid moet zowel door de wetgever als door diegenen die de methoden gebruiken in acht worden genomen, zeker daar waar een gelijktijdige combinatie van methoden mogelijk is. Zoals dat het geval is bij plaatsbepaling via iemands mobiele telefoon. 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, met het oog op de ingrijpende gevolgen voor de privacy, grote behoedzaamheid vereist.

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