Noot bij de zaak Liberty / UK (EHRM 1 juli 2008, appl. 58243/00), *NJ*, 2010-26, nr. 324, p. 3120-3121.

Inleiding en de zaak Liberty

1. In onze samenleving wordt de burger met behulp van elektronische communicatiemiddelen op steeds grotere schaal intensief in de gaten gehouden. Het EHRM heeft zich daarover al dikwijls uitgesproken. In deze noot recapituleer ik de jurisprudentie van het EHRM. Ik onderscheid drie situaties: het individueel actief monitoren (bijvoorbeeld het afluisteren van een verdachte), het collectief actief (strategisch) monitoren (het controleren op bepaalde kenmerken, bijvoorbeeld vliegtuigpassagiers bij controlepoortjes) en het collectief passief monitoren (het verzamelen van grote hoeveelheden gegevens zonder dat er nog iets mee wordt gedaan, bijvoorbeeld het gedurende een bepaalde periode opslaan van telecommunicatiegegevens). De situaties kunnen overigens in elkaar overgaan. Deze zaak, waarin het Hof de term 'strategisch monitoren' introduceert, gaat over de tweede categorie. Eerst iets over de onderhavige zaak.
2. Deze zaak begon in de jaren negentig in het VK toen het Engelse ministerie van Defensie alle telecommunicatie tussen Dublin en Londen begon af te vangen met een zogenaamde Electronic Test Facility (ETF). De eisers in deze procedure zijn Britse en Ierse civil right organisaties, die zich bij diverse Engelse instanties (zie de samenvatting) beklaagden dat zij in de betrokken periode zijn afgeluisterd, zonder dat er voor die praktijk een deugdelijke wettelijke basis was. Hun klacht was in het bijzonder dat de telefoongesprekken waren 'gefilterd' volgens geheime filtercriteria en zonder dat er een behoorlijk afluisterbevel bestond. Deze klacht wordt door het Hof gehonoreerd (zie hierna onder collectief actief monitoren). Het afluisterproces ging in de volgende fasen in zijn werk:
    a. Er werd eerst een afluisterbevel uitgevaardigd waarin de te onderscheppen verbindingen werden aangewezen. Dat kon heel breed zijn: bijvoorbeeld alle zeekabels die in het VK aan land komen.
    b. De uitvaardiging van een certificaat door de minister van Binnenlandse Zaken waarin de informatie categorieën, die in de aangewezen communicatiemiddelen mochten worden onderschept, werden omschreven.
    c. De installering van het filtersysteem, zoekmachines die op vooraf ingestelde trefwoorden of combinaties daarvan de communicaties onderschepten.
    d. Het opschonen van de op trefwoorden gefilterde communicaties, zoals het verwijderen van namen of het verwijderen van details die buiten het opsporingsdoel vielen.
    e. De verspreiding van deze informatie voor onderzoeksdoeleinden.

Algemene regels

3. Zoals meestal in dit soort zaken, staat het Hof lang stil bij de vraag of de wettelijke regels en de praktijk wel voldoen aan het criterium dat de wet 'accessible' en 'forseeable' is, d.w.z. of de praktijk 'in accordance with the law' is. De zaak spitst zich toe op de voorzienbaarheid van de wettelijke beperking ('in accordance with the law'). De criteria

a. Bestaat er een definitie van de categorieën van personen die mogen worden afgeluisterd?
b. Is de duur van het afluisteren beperkt?
c. Is er een vastgelegde procedure hoe gegevens mogen worden opgeslagen, gebruikt en onderzocht?
d. Liggen de voorzorgsmaatregelen vast die bij communicatie van de gegevens aan derden in acht moeten worden genomen?
e. Onder welke omstandigheden mogen of moeten de gegevens worden vernietigd?

4. Dit zijn algemene regels die het Hof heeft geformuleerd naar aanleiding van afluisteren, zodat zij niet onverkort op elke situatie kunnen worden toegepast. De situaties kunnen variëren van waarneming en opslag met elektronische middelen van de beeltenis van een persoon (bewakingscamera's in de cel, zie de zaak Perry, EHRM 17 juli 2003, *NJ* 2006, 40, met annotatie EJD), opslaan van gegevens over iemands levenspatroon en sociale uitingen (de registers van de veiligheidsdiensten, zie de zaak Segerstedt, EHRM 6 juni 2006, *NJ* 2009, 449, m.nt. E.J. Dommering), waarneming en opslag van iemands (elektronische) communicatiehandelingen (zowel de inhoud als waar en met wie, de zaak Copland, EHRM 3 april 2007, *NJ* 2007, 617, met annotatie E.J. Dommering).

Individueel monitoren

5. Het individueel afluisteren en aftappen heeft in Nederland een grote vlucht genomen (voor een overzicht zie Dorien Verhulst, 'Kroniek aftappen en gegevensvergaring', in: *Mediaforum* 2010-1, p. 2-11). De aanvullende eis die daarbij wordt gesteld is dat de getapte binnen redelijke tijd wordt in kennisgesteld dat hij is afgetapt (de zaak Malone, EHRM 2 augustus 1984, *NJ* 1988, 534, m.nt. PvD). Met die eis wordt in Nederland nogal eens de hand gelicht, zie R. Chavannes, 'Veel taps, weinig verantwoording', in: *Mediaforum* 2008-6, p. 246. Bij individueel cameratoezicht is zelfs notificatie vooraf vereist (de zaak Perry). Individueel monitoren is de meest belastende vorm van iemand in het geheim bespieden. Hij wordt immers ieder moment gevolgd, 'op de huid gezeten' (aftappen, schaduwen).
6. In Nederland is in het kader van bestrijding van (vooralsnog alleen) kinderpornografie (http://www.justitie.nl/onderwerpen/criminaliteit/cybercrime/kinderporno/neb/) een discussie ontstaan over het filteren van websites waarop die porno wordt aangeboden. Op dit moment zijn het de Internet Service Providers (ISP) die feitelijk de filterverplichting op hun bord krijgen. De politie spoort onder meer op basis van strategische monitoring met trefwoorden of trefbeelden sites op. De vangst wordt geïndividualiseerd in zwarte lijsten op grond waarvan de ISP's de doorgifte van websites

op de lijst blokkeren. Websites onderscheiden zich van telefoon – en emailverkeer, omdat het gaat om openbare informatie, zodat daarop de normen van artikel 7 Gw en 10 EVRM van toepassing zijn. Ik heb betoogd dat filteren door of vanwege de overheid in strijd is met het censuurverbod van artikel 7 Gw ('Filteren is gewoon censuur, en daarmee basta', in: *Tijdschrift voor Internetrecht* 2008, [1], nr 5, p. 124-125). Als het gaat om de proportionaliteit en de transparantie van deze praktijk, zijn daarop naar analogie beginselen uit de vijf stappen test toe te passen. De websites die geweerd worden, worden immers eerst heimelijk door de politie op basis van strategische monitoring bekeken, een handeling die grote gelijkenis vertoont met 'afluisteren' op basis van (een combinatie van) trefwoorden. Met toepassing van de vijf stappen test, moet de conclusie zijn dat de huidige informele praktijk op basis van onderhandse afspraken tussen de politie en de ISP's, deze test niet kan doorstaan.

Collectief actief monitoren

7. Collectief actief monitoren op bepaalde kenmerken is minder belastend dan individueel monitoren, omdat het in eerste aanleg niet herleidbaar is tot personen. Het is in zoverre wel belastend dat er actieve waarneming plaatsvindt naar potentieel tot personen herleidbare communicaties of gedragingen, zodat daarop direct individuele actie kan volgen.
8. Het Hof beslist dat de vijf stappentoets ook van toepassing is op 'strategic monitoring': 'The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other.' Toepassing van de vijf stappen toets valt voor het VK negatief uit. De eerste, hiervoor onder 2 a beschreven fase, passeert al niet toets 3 a: immers alle personen die over de zeekabels communiceren vallen er onder. Ook de omschrijving van de communicaties die voor onderschepping in aanmerking kwamen was te ruim om in stap 3 a door de beugel te kunnen. De omschrijving van de filtercriteria en de werking van de filtermachine (fase 2 b en c) komt niet door stap 3 c heen, terwijl de fasen 2 d en e het niet halen omdat de 'arrangements' die daarvoor bestonden niet publiek toegankelijk waren.
9. Het Hof heeft zich kennelijk in dit soort zaken laten inspireren door de Duitse G10 wet (de Duitse Wet Inlichtingen en Veiligheid), die in de zaak Weber en Saravis de Straatsburgse toets der kritiek kon doorstaan. Strategische monitoring mag volgens deze wet met zoektermen die geschikt zijn om de veiligheidsrisico's die de dienst beoogt te onderzoeken/bestrijden bloot te leggen. Ook zijn de procedureregels nauwkeurig in de wet geregeld. Zo moeten de autoriteiten iedere zes maanden controleren of de vastgelegd data nog nodig zijn voor het onderzoek. Zo neen, dan moeten ze worden vernietigd. Ook vindt het Hof dat het best mogelijk is de gehanteerde criteria en procedures openbaar te maken zonder dat dit het functioneren van een veiligheidsdienst behoeft te schaden.
10. Het is mij niet bekend of de AIVD of een andere instantie in Nederland aan strategische monitoring doet. Strategische monitoring vindt op grote schaal plaats bij het wereld telefoon-, fax- en emailverkeer via satellieten (het ECHELON project, waarin de geheime diensten van de VS, het VK, Canada, Australië en Nieuw Zeeland samenwerken, op basis

van het UKUSA verdrag uit 1947). Voorzover dit monitoringsysteem onder de rechtsmacht van enig lid van de Raad van Europa valt, is het zonder twijfel in strijd met artikel 8 van het EVRM, zoals door het EHRM uitgelegd. Hoe de betrokkenheid van Nederland en de EU bij dit project is, blijft overigens onduidelijk. Er is rond ECHELON in 2001 enige parlementaire activiteit van het Nederlandse parlement (brief van minister de Grave aan de Tweede Kamer van 19 januari 2001) geweest, maar daarna is het stil geworden.

11. Een andere vorm van strategische monitoring die hand over hand toeneemt is het onderzoek aan vliegtuigpassagiers op metalen en vloeistoffen. In het arrest van Gillian & Quinton/UK, EHRM 10 januari 2010 (appl.4158/05) veroordeelde het Hof het *at random* aanhouden van voorbijgangers op straat om te onderzoeken of zij wapens of verdachte materialen bij zich dragen, dit alles in het kader van de Terrorism Act 2000, die de politie op dit gebied onbeperkte bevoegdheden geeft. Het meende dat dit een verschil zou zijn ten opzichte van het collectief strategisch monitoren van vliegtuigpassagiers, omdat die zich door de keuze van het reizen per vliegtuig daaraan vrijwillig zouden hebben onderworpen, een argument waar ik niet erg van onder de indruk kan raken, maar dat ik nu maar daar laat.
12. Een vraag die bij de praktijk van het strategisch monitoren kan worden gesteld (en die niet in het onderhavige arrest wordt behandeld) is of er niet een algemene notificatie vooraf vereist is, bijvoorbeeld 'dit communicatiekanaal wordt op geweld/porno gemonitord' (zoals bij voorbeeld wel gebeurd bij collectief passief moniotoren bij cameratoezicht, zie hierna).

Collectief passief monitoren

13. Cameratoezicht op openbare plaatsen is thans in heel Europa gangbaar. In Nederland heeft het een regeling gekregen in artikel 151c Gemeentewet, waarin de vijstappen toets is te herkennen. Daarbij valt het op dat er een notificatieplicht vooraf geldt. Cameratoezicht ligt dicht tegen strategisch monitoren aan, omdat achter het bewakingspanel waarnemers zitten die de beelden screenen op het gedragskenmerk geweld of andere verstoring van de openbare orde door de zich in beeld bevindende voorbijgangers. Dat is niet het geval met het opslaan van telecommunicatiegegevens, hetgeen een in beginsel passieve bezigheid is. Over de wet die dit regelt (Wet van 19 juli 2009, *Stb.* 2009, 360) is het nodige te doen geweest over de *duur* van de opslag (zie Verhulst t.a.p. p. 7). Een andere soortgelijke discussie is die van de centrale opslag van biometrische persoonsgegevens in het kader van de paspoortverstrekking (*Stb.* 2009, 252). Collectief passief monitoren rukt ook op in het wegverkeer. In de brief aan de Tweede Kamer met het kabinetsstandpunt over het advies Commissie Brouwer-Korf en de evaluatie van de Wet bescherming persoonsgegevens van 3 november 2009 (TK 2009-2010, 31051, nr. 5, par. 3.5.2.), wordt er op aangedrongen de kentekenherkenning van auto's (ANPR: Automatic Number Plate Recognition) nu maar snel in te voeren. Ik citeer uit de brief: 'Met een totaal van 10 miljoen kentekens in Nederland is duidelijk dat ANPR kan uitgroeien tot een belangrijk handhavingsinstrument van de overheid en bij kan dragen aan een veiliger samenleving in het bijzonder.'

14. Het Hof toetste in de zaak Marper de opslag van DNA profielen van verdachten (in zoverre dus een vorm van strategisch monitoren, omdat de bron al is geselecteerd op een bepaald kenmerk, namelijk het zijn van 'verdachte') op proportionaliteit (EHRM 4 december 2009, *NJ* 2009, 410). Ook ongebreidelde verzameling van (nog) niet waargenomen individuele of kenmerkende gegevens kan dus in strijd komen met artikel 8 lid 2 EVRM.

E.J. Dommering