UNIVERSITEIT VAN TILBURG

Juridische aspecten van geo-informatie

Een inventarisatie van juridische mogelijkheden, barrières en randvoorwaarden voor het gebruik van geo-informatie door de overheid, en meer in het bijzonder geo-locatiediensten.

Universiteit van Tilburg
TILT – Tilburg Institute for Law, Technology, and Society
Postbus 90153
5000 LE Tilburg
<J.Nouwt@uvt.nl>

Sjaak Nouwt
Leo van der Wees

Versie 1.0
November 2008

Centrum voor Recht, Technologie en Samenleving
Postbus 90153 • 5000 LE Tilburg • Bezoekadres > Warandelaan 2 • Tilburg • Telefoon 013 466 81 99 • www.uvt.nl/tilt/

Inhoudsopgave

1. Inleiding

Binnen verschillende beleidsterreinen en bestuurslagen van de overheid wordt steeds meer gebruik gemaakt van nieuwe technologieën voor de productie, de verwerking, het beheer en de ontsluiting van informatie. Deze informatie betreft vandaag de dag steeds vaker ook ruimtelijke informatie, veelal geo-informatie genoemd. Deze vorm van informatie gaat over het "waar" en "wanneer" van subjecten en objecten en wordt vaak gecombineerd met diverse andere gegevens. Bij dat laatste valt te denken aan demografische, economische of juridische kenmerken.[1]

Het gebruik van geo-informatie roept, al dan niet in combinatie met andere informatie, juridische vragen op. In dit onderzoek wordt getracht antwoorden te geven op een aantal van die juridische vragen. De centrale vraag luidt als volgt:

Wat zijn de juridische mogelijkheden, barrières en randvoorwaarden voor het gebruik van toepassingen (door de overheid) waarbij geo-informatie verwerkt wordt?

In eerdere studies - *Drempels weg!*[2] en *Open toegankelijkheid voor geo-informatie vergeleken: het gras leek groener dan het was*[3] - is reeds een aantal juridische belemmeringen aan de orde gekomen: leverings- en verstrekkingsvoorwaarden, openbaarheid, hergebruik, intellectuele eigendom en aansprakelijkheid. Deze belemmeringen zijn vooral onder de aandacht gebracht met het oog op het gebruik en de ontsluiting van geografische informatiesystemen (GIS). Systemen waaraan men veelal bijna vanzelfsprekend denkt indien geo-informatie aan de orde is.

Ook in deze studie wordt aandacht besteed aan geografische informatiesystemen, aan traditioneel gebruik van geo-informatie, en dus aan een aantal aspecten (intellectuele eigendom, openbaarheid / hergebruik) die in de eerdere studies ook aan de orde zijn gekomen. Daarbij is het onvermijdelijk dat een aantal zaken vermeld wordt dat ook in de eerdere studies aan de orde is gekomen. Er zijn evenwel ook nieuwe ontwikkelingen te melden.

Naast (traditionele) geografische informatiesystemen wordt in deze studie ook aandacht besteed aan mobiele locatiegebonden overheidsdiensten, ook wel location based services (LBS) genoemd.[4] Dit zijn diensten verleend door (overheids)instanties aan (veelal) burgers die mobiel zijn en die gebruik maken, of in het bezit zijn, van een mobiele telefoon, een chipkaart, een elektronische enkelband, of een andere locatiegebonden toepassing. Diensten waarbij net als bij geografische informatiesystemen, geo-informatie een rol kan spelen, maar waarbij andere juridische aspecten dan leveringsvoorwaarden, openbaarheid of aansprakelijkheid een rol spelen. Althans, diensten waarbij het juridisch zwaartepunt bij privacy-aspecten lijkt te liggen; bij het recht om rust gelaten te worden en bij het gegevensbeschermingsrecht, omdat daarbij gebruik wordt gemaakt van persoonsgegevens.

---

[1] Bastiaan van Loenen, Jaap Zevenbergen, Jitske de Jong, Geo-informatie: wat is het en wat is de juridische context?. In: Leo van der Wees, Sjaak Nouwt (red.), *Recht en locatie* Nederlandse Vereniging voor Informatietechnologie en Recht, Den Haag: Elsevier Juridisch, 2008.

[2] Drempels weg! Overzicht van belemmeringen in de ontsluiting van geo-informatie en mogelijke oplossingen., Geonovum, 26 november 2007 (Online beschikbaar op de website van Genovum (<www.google.nl> zoeken naar *drempels weg geo-informatie*)

[3] Open toegankelijkheid voor geo-informatie vergeleken: het gras leek groener dan het was, dr. ir. Bastiaan van Loenen, et al., ministerie van BZK, 4 april 2007. Online beschikbaar op de website van het ministerie van BZK, <www.google.nl> zoeken naar *open toegankelijkheidsbeleid geo-informatie*.

[4] Location-based service, Wikipedia, <en.wikipedia.org/wiki/Location_Based_Services>.

Aandacht voor locatiegebonden diensten is niet alleen gepast omdat dit soort diensten in opkomst is. Ook lijkt *location awareness*, het weten waar we zijn, het in zich te hebben om misschien wel net zo belangrijk te worden als dat we ons bewust zijn van datum en tijd. [5]

In het navolgende treft u een beschrijving aan van regels die betrekking hebben op privacy, arbeidsrecht (in het licht van privacy), openbaarheid / hergebruik, en intellectuele eigendom. De eerste twee rechtsgebieden staan in nauw verband met de genoemde mobiele locatiegebonden diensten, terwijl de laatste twee net als in eerdere studies (meer) betrekking hebben op de traditionele geografische informatiesystemen.

In de studies *Drempels weg!* en *Open toegankelijkheid voor geo-informatie vergeleken: het gras leek groener dan het was* is nog verwezen naar respectievelijk het wetsvoorstel Markt en Overheid en het voorstel voor een Algemene Wet Overheidsinformatie die uiteindelijk de Wet Openbaarheid van bestuur zou moeten gaan vervangen. Deze voorstellen worden in deze studie niet nader toegelicht. Simpelweg omdat over deze wetsvoorstellen amper nog iets is vernomen. Het laatste kamerstuk inzake de Wet Markt en Overheid dateert alweer van mei 2007[6], terwijl het laatste steekhoudende nieuws over de Algemene Wet Overheidsinformatie dateert van 2006.[7]

Bij de beschrijving van de verschillende juridische onderdelen zullen (overheids)diensten worden beschreven en tegen het juridische licht worden gehouden. Elk juridisch onderdeel sluit af met een conclusie.

Tot slot eindigt het rapport met de beschrijving van een case study waarin het gebruik van geo-informatie in de praktijk onder de loep genomen. Gekozen is voor het gebruik van SMS door de overheid in het kader van de opsporing van strafbare feiten. In deze case study worden in het bijzonder het gebruik van SMS-Alert,en de Groeps-SMS besproken in het licht van het recht om met rust gelaten te worden (privacy) en het gegevensbeschermingsrecht Deze case study heeft ook geleid tot de publicatie van een artikel in het tijdschrift Computerrecht (2008, nr. 4). De tekst van dit artikel is aan dit rapport toegevoegd als Bijlage 3.

[5] Jan Smits, Hotze de Jong, Leo van der Wees, Het recht en locatiegebonden diensten. In: Leo van der Wees, Sjaak Nouwt (red.), Recht en locatie. Nederlandse Vereniging voor Informatietechnologie en Recht, Elsevier Juridisch, Den Haag, 2008.
[6] *Kamerstukken II* 2006-2007, 28050, nr. 12, Wet markt en overheid; Brief minister over stand van zaken wetsvoorstel. Toegevoegd aan Overheid.nl op 8-5-2007.
[7] Algemene wet overheidsinformatie (voorontwerp), Recht.nl, 10/05/06, <recht.nl/24339>.

2. Privacy

Het spreekt voor zich dat het privacyrecht een belangrijke plaats inneemt in dit rapport. Althans, gezien het feit dat aandacht wordt besteed aan mobiele (overheids)diensten die betrekking hebben op, of gebruikt worden door subjecten is de kans aannemelijk dat privacy aan orde komt. Dit wordt vooral duidelijk na de bespreking hieronder van diensten die reeds in gebruik zijn of die ontwikkeld gaan worden. Sterker, dan bekruipt de lezer bijna het gevoel dat het nu dan toch eindelijk "1984" is. Ook de studie *Van privacyparadijs tot controlestaat*[8] van het Rathenau Instituut en een recent themanummer van de Groene Amsterdammer getiteld *De Gluurstaat*[9] wijzen in die richting.

Betrof de Rathenau-studie overigens de uitdijende bevoegdheden van politie en justitie in relatie tot privacy. In het themanummer van de Groene Amsterdammer blijkt net als in deze studie naar geo-diensten (locatiegebonden diensten en geografische informatiesystemen) dat de publieke privacy in het geding is. Het lijkt erop alsof we ons steeds minder vrij kunnen bewegen in de publieke ruimte. Locatiegebonden mobiele diensten spelen daarbij een rol, maar ook geo-informatiesystemen als Street View, waardoor het mogelijk is online zichtbaar te worden als iemand zich toevallig in een bepaalde straat begeeft als een Street View-camera daar opnamen maakt.[10]

Allereerst volgt hierna een juridische uiteenzetting over privacy. Daarin wordt de privacyregulering op globaal, Europees en nationaal niveau beschreven. Daarna worden de verschillende gedaanten van privacy nader toegelicht. Dan volgt een beschrijving van enkele toepassingen waarbij geo-informatie een rol kan spelen. Vervolgens worden de privacyregels en -gedaanten bezien in het licht van de beschreven toepassingen.

2.1 Privacy globaal, Europees en nationaal

Op verschillende bestuurlijke niveaus is het recht op privacy geregeld. Het gaat van wereldniveau – privacy als universele waarde – via Europees, tot nationaal niveau. In deze paragraaf zal de bescherming van privacy op elk van deze niveaus uiteengezet worden. Daarbij wordt tevens kort aangegeven wat de rol van deze verschillende regelingen kan zijn voor de (omgang met) geo-informatie.

2.1.2 Privacy globaal UVRM en IVBPR

In de preambule van de Universele Verklaring voor de Rechten van de Mens (UVRM)[11] wordt verwezen naar gelijke en onvervreemdbare rechten van alle leden van de mensengemeenschap die de grondslag zijn voor de vrijheid, gerechtigheid en vrede in de wereld. Een aantal van deze onvervreemdbare rechten –basisrechten – heeft betrekking op privacy. Een deel daarvan kan in relatie gebracht worden met geo-informatie. Dit zijn in het bijzonder:

- het recht op leven, vrijheid en onschendbaarheid van de persoon (art. 3);

---

[8] Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw, Anton Vedder, Leo van der Wees, Bert-Jaap Koops en Paul de Hert, Rathenau Instituut, 2007. In te zien via <www.rathenau.nl/autoparse.asp?item=2099>.
[9] Gluurstaat. De oorverdovende stilte rond privacy, Groene Amsterdammer, 13/2008.
[10] Google 'Street View' invaded suburban Pa. couple's privacy, suit claims, LegalNewsline.com, 7 april 2008 (<www.legalnewsline.com> zoeken naar *street view*).
[11] Universele Verklaring voor de Rechten van de Mens, Parijs, 10 december 1948, Tractatenblad 1969, 99.

- het verbod op willekeurige inmenging in iemands persoonlijke aangelegenheden, gezin, huis, briefwisseling of aantasting van iemands eer (art. 12);
- het recht om zich vrij te verplaatsen (bewegingsvrijheid) en te vertoeven binnen de zijn land en om zijn land te verlaten en weer terug te keren (art. 13).

Zo kan het volgen van burgers via zendmasten en satellieten op gespannen voet staan met artikel 3. Daarnaast kan het ongevraagd gestoord worden door commerciële boodschappen die binnenkomen op de mobiele telefoon omdat men zich op een bepaalde locatie bevindt, gezien worden als een willekeurige inmenging in iemands persoonlijke aangelegenheden. En ook kan men zich afvragen in hoeverre burgers zich nog vrij kunnen verplaatsen als zij niet alleen via de mobiele telefoon, maar ook via het navigatiesysteem van hun auto overal gevolgd kunnen worden (artikel 13).

Aan de andere kant betekent het natuurlijk niet dat het leven minder aangenaam geworden is als gevolg van de introductie van mobiele telefoons, navigatiesystemen, etc. Het gebruik van de mobiele telefoon zorgt er immers ook voor dat burgers bijvoorbeeld het thuisfront op de hoogte kunnen houden van vertragingen tijdens reizen. En het navigatiesysteem in de auto voorkomt nodeloos zoeken en zorgt daardoor dus ook voor minder overbodig gereden kilometers en daardoor weer voor minder vervuiling.

Wel dienen we ons bewust te zijn van het feit dat een nieuwe technologie een bedreiging voor universele waarden als bijvoorbeeld privacy zou kunnen opleveren, hoeveel gemak we ook ondervinden van het gebruik ervan. Voorwaarden en regels zijn daarom soms gewenst.

De Universele Verklaring van de Rechten van de Mens is als verklaring niet bindend. De verklaring heeft echter wel als basis gediend voor het wel bindende Internationaal verdrag inzake burgerrechten en politieke rechten (IVBPR).[12] Dit internationale verdrag is op 25 juni 1969 door Nederland ondertekend en geratificeerd op 11 december 1978.

De hiervoor genoemde rechten genoemd in de UVRM zijn het IVBPR terecht gekomen in de artikelen 9 (recht op vrijheid en veiligheid van de persoon, verbod op willekeurige arrestatie of gevangenhouding), 12 (recht op vrije verplaatsing en vrije vestiging) en 17 (recht op privacy).

2.1.3 Privacy Europa EVRM en Handvest van de Grondrechten van de Europese Unie

Het recht op privacy is ook op Europees niveau vastgelegd. In navolging van de hiervoor besproken Universele Verklaring van de Rechten van de Mens is in 1950 het Europees Verdrag voor de Rechten van de Mens en Fundamentele Vrijheden (EVRM) opgesteld.[13] Net als het IVBPR is het EVRM bindend en heeft het in Nederland directe werking. Artikel 94 van onze Grondwet stelt dan ook:

Binnen het Koninkrijk geldende wettelijke voorschriften vinden geen toepassing, indien deze toepassing niet verenigbaar is met een ieder verbindende bepalingen van verdragen en van besluiten van volkenrechtelijke organisaties.

In het EVRM zijn de eerder genoemde rechten terecht gekomen in de artikelen 5 (recht op vrijheid en veiligheid) en 8 (recht op privacy).

[12] De Nederlandse tekst van het IVBPR staat onder meer op de website van de Vlaamse Organisatie voor Mensenrechteneducatie <www.vormen.org/informatie/downloads/BuPo.pdf>.
[13] Een verwijzing naar de tekst van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, Rome, 04-11-1950 staat op Recht.nl, <www.recht.nl/4555>.

Ook in het Handvest van de Grondrechten van de Europese Unie zijn deze rechten opgenomen.[14] Het handvest vormt de synthese van de gemeenschappelijke waarden van de lidstaten van de Europese Unie en brengt de traditionele burgerrechten en politieke rechten, alsmede de economische en sociale rechten, in één enkele tekst bijeen. Het doel ervan is uiteengezet in de preambule: "…het (is) noodzakelijk de bescherming van de grondrechten in het licht van de ontwikkelingen in de maatschappij, de sociale vooruitgang en de wetenschappelijke en technologische ontwikkelingen te versterken door die rechten zichtbaarder te maken in een handvest."

Het handvest is opgesteld door een Conventie die bestond uit vertegenwoordigers van de staatshoofden en regeringsleiders van de lidstaten, een vertegenwoordiger van de voorzitter van de Europese Commissie en leden van het Europees Parlement en van de nationale parlementen. Het werd in december 2000 formeel door de voorzitters van het Europees Parlement, de Raad en de Commissie aangenomen. Het Verdrag van Lissabon, dat zich momenteel in de ratificatiefase bevindt, verleent het handvest bindende kracht door de opname van een vermelding waardoor het dezelfde rechtskracht krijgt als de andere Europese verdragen.

In artikel 6 van het handvest wordt het recht op vrijheid en veiligheid geregeld, in artikel 7 de eerbiediging van het privé-leven en het familie- en gezinsleven en in artikel 8 de bescherming van persoonsgegevens.

2.1.4 Privacy nationaal

Ook de Nederlandse Grondwet laat zich niet onbetuigd wat privacy betreft.[15] De bescherming van de persoonlijke levenssfeer wordt geregeld in de artikelen 10 (persoonsgegevens), 11(lichamelijke integriteit), 12 (bescherming van de woning) en 13(vertrouwelijkheid van communicatie).

Daarnaast staan in een groot aantal nationale wetten bepalingen die betrekking hebben op de bescherming van de persoonlijke levenssfeer. Van deze nationale regels zijn met name de Wet bescherming persoonsgegevens (WBP) en de Telecommunicatiewet (Tw) van belang in relatie tot geo-informatie en locatiegebonden diensten.

2.1.4.1 Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (WBP) is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op handmatig beschikbare gegevens, voor zover deze in een bestand voorkomen of bestemd zijn om daarin te worden opgenomen (art. 2 lid 1 WBP).[16] Om vast te stellen of de WBP van toepassing is, moet men zich dus afvragen of de gegevens waarover men beschikt ‘persoonsgegevens’ zijn en vervolgens of er sprake is van een ‘verwerking’ van deze persoonsgegevens en van een ‘bestand´.

Persoonsgegevens
Onder het begrip ‘persoonsgegeven’ vallen alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon. Er bestaat dus een onderscheid tussen gegevens en informatie.

Gegevens kunnen een beslissing weergeven die over een bepaalde persoon is genomen. Gegevens kunnen ook betrekking hebben op een product of een proces en daarbij tevens informatie verschaffen over een persoon. Zo kan de arbeidsproductiviteit van een werknemer

[14] Handvest van de Grondrechten van de Europese Unie, website Europees Parlement <www.europarl.europa.eu/charter/pdf/text_nl.pdf>
[15] Een verwijzing naar de Nederlandse Grondwet staat op Recht.nl, <wetten.recht.nl/link/24468>.
[16] Een verwijzing naar de WBP staat op Recht.nl, <wetten.recht.nl/link/24702>.

bijvoorbeeld in kaart worden gebracht. Het gegeven dat een bepaalde persoon aangifte heeft gedaan van diefstal van een auto is ook een persoonsgegeven omdat het informatie verschaft over die persoon als slachtoffer van een misdrijf. In deze context wordt met een persoonsgegeven gedoeld op een gegeven over een persoon dat vervolgens informatie kan verschaffen over die persoon.

De memorie van toelichting bij de WBP[17] wordt uitgelegd dat het begrip 'persoonsgegeven' twee elementen bevat:

1. Om een persoonsgegeven te zijn moet een gegeven informatie opleveren 'betreffende' een natuurlijke persoon. Gegevens verschaffen informatie over een persoon, als die gegevens mede bepalend zijn voor de wijze waarop een persoon wordt beoordeeld of behandeld door degene die over die gegevens beschikt. In dat geval zijn die gegevens 'persoonsgegevens'. Sommige gegevens bevatten duidelijk feitelijke informatie over een persoon. Dat zijn bijvoorbeeld iemands naam, geboortedatum of geslacht. Maar ook telefoonnummers, kentekens van auto's en postcodes met huisnummers zijn persoonsgegevens.
2. De identificeerbaarheid van de persoon is het tweede element dat bepaalt of al dan niet sprake is van een 'persoonsgegeven'. Een persoon is identificeerbaar indien redelijkerwijs, zonder onevenredige inspanning, zijn identiteit vastgesteld kan worden. Bepalend daarvoor zijn de aard van de gegevens en de mogelijkheden waarover de verantwoordelijke beschikt om de identificatie tot stand te brengen.

In verband met de aard van de gegevens bestaat onderscheid tussen direct en indirect herleidbare gegevens:

- Direct herleidbare gegevens horen bij personen waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen. Dat zijn gegevens als naam, adres, geboortedatum, die in combinatie met elkaar gemakkelijk een persoon kunnen identificeren.
- Indirect herleidbare gegevens zijn gegevens die zijn ontdaan van naam, maar door combinatie met andere gegevens tot een persoon herleidbaar zijn. Daarnaast zijn sommige gegevens zo uniek, dat zij ook herleidbaar zijn. Voorbeelden hiervan zijn het burgerservicenummer en biometrische gegevens, zoals stem, vingerafdruk of DNA-profiel.

Ook de mogelijkheden waarover de verantwoordelijke beschikt om een persoon te kunnen identificeren zijn mede bepalend voor de vraag of sprake is van 'persoonsgegevens'. Het gaat hierbij om alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke zijn in te zetten om een persoon te identificeren. Daarbij wordt uitgegaan van een redelijk toegeruste verantwoordelijke.

Verwerken van persoonsgegevens
Als is vastgesteld dat gegevens persoonsgegevens zijn, moet men zich afvragen of men die persoonsgegevens ook 'verwerkt' in de zin van de WBP. De 'verwerking van persoonsgegevens' is 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens.' Dit wil in feite zeggen dat alles wat men met persoonsgegevens kan doen, vanaf het verzamelen tot en met het vernietigen van persoonsgegevens (inclusief het raadplegen, verstrekken, e.d.), onder het begrip 'verwerken van persoonsgegevens' valt. Bepalend daarvoor is of men enige feitelijke macht of invloed over de gegevens kan uitoefenen, al dan niet via een computersysteem. Men moet dus een handeling met de gegevens kunnen verrichten. Als men geen macht of invloed kan uitoefenen op de persoonsgegevens, hoeft men niet aan de eisen van de WBP te voldoen.

Materiële normen in de WBP

[17] *Kamerstukken II* 1997-1998, 25892, nr. 3, p.45 en verder.

Een klassieke tweedeling in het recht is die in materieel recht en formeel recht. Materieelrechtelijke regels verlenen, verruimen, beperken of ontzeggen aanspraken, verplichtingen of bevoegdheden. Formeel recht regelt procedures en bevat vormvoorschriften en organisatorische bepalingen.

Zo bevat de WBP materiële normen in de zin van voorwaarden die deze wet stelt aan het verwerken van persoonsgegevens. Voor elke handeling met persoonsgegevens geldt dat deze moet voldoen aan deze voorwaarden. Deze voorwaarden houden in dat de handeling altijd in overeenstemming met de wet, behoorlijk en zorgvuldig moet zijn (art. 6 WBP). Het verzamelen van persoonsgegevens is alleen toegestaan als dat gebeurt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (art. 7 WBP). Deze gerechtvaardigde doeleinden zullen in de praktijk meestal overeenkomen met een of meer van de grondslagen waarop elke verwerking van en handeling met persoonsgegevens moet berusten (art. 8 WBP):

(a) de ondubbelzinnige toestemming van de betrokkene;
(b) de noodzakelijkheid voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor het treffen van voorbereidende maatregelen daartoe;
(c) de noodzakelijkheid om een wettelijke verplichting van de verantwoordelijke na te kunnen komen;
(d) de noodzakelijkheid ter vrijwaring van een vitaal belang van de betrokkene;
(e) de noodzakelijkheid ter vervulling van een publiekrechtelijke taak door een bestuursorgaan;
(f) de noodzakelijkheid voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het (privacy) belang van de betrokkene voorrang verdient.

Deze gronden zijn alternatieve gronden, dat wil zeggen dat het voldoende is als men een gegevensverwerking kan baseren op één van deze gronden (meer dan één kan en mag ook).

Wanneer men eenmaal op rechtmatige wijze verzamelde persoonsgegevens wil gebruiken (verder verwerken), dan is dat uitsluitend toegestaan als:
- het doel van dat gebruik niet in strijd is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld (art. 9 WBP);
- de persoonsgegevens niet langer in tot personen herleidbare vorm worden bewaard dan noodzakelijk is voor de verwerkelijking van de doelen waarvoor ze oorspronkelijk zijn verzameld (art. 10 WBP). Langer bewaren is wel toegestaan mits de gegevens uitsluitend voor historische, statistische of wetenschappelijke doeleinden worden gebruikt;
- de persoonsgegevens die worden verwerkt juist, volledig en actueel te zijn (art. 11 WBP);
- deze onder geheimhouding worden verwerkt (art. 12 WBP). Dit artikel neemt niet weg dat bijvoorbeeld reeds op grond van het medisch beroepsgeheim of ambtsgeheim een plicht tot vertrouwelijkheid kan bestaan;
- de verantwoordelijke voor de gegevensverwerking passende technische en organisatorische maatregelen treft om de persoonsgegevens voldoende te beveiligen (art. 13 WBP);
- in het geval een verantwoordelijke de feitelijke verwerking van de persoonsgegevens heeft uitbesteed aan een ‘bewerker’, daaraan een overeenkomst of andere rechtshandeling ten grondslag ligt (art. 14 WBP);
- de verantwoordelijke er voor zorgt dat de artikelen 6 tot en met 14 uit de eerste groep worden nageleefd (art. 15 WBP).

Uitzonderingen WBP
In enkele uitzonderingsgevallen is de WBP niet van toepassing (art. 2 lid 2 WBP). Zo is de WBP niet van toepassing op gegevensverwerkingen die uitsluitend voor persoonlijke of huishoudelijke doeleinden bestemd zijn. Veel professionals houden, ook in het kader van hun werk, eigen lijstjes bij, bijvoorbeeld adresbestanden van personen met wie zij regelmatig contact onderhouden. Zij

hebben het karakter van persoonlijke aantekeningen, dienend als geheugensteun. Deze laatste zijn voor persoonlijke doeleinden en dus van de werking van de WBP uitgezonderd. Zodra een verwerking beoogd is voor gebruik door meerdere personen, is de WBP wel van toepassing.

De 'huishoudelijke doeleinden' betreffen de situatie dat in een gezinssituatie persoonsgegevens worden verwerkt. Ook wanneer meerdere personen die gezamenlijk een huishouden voeren, gebruik maken van deze gegevens, is de WBP niet van toepassing. Het Hof van Justitie van de EG is echter van mening dat het ontsluiten van gegevens voor een onbepaald aantal personen, bijvoorbeeld door vermelding op het internet, moeilijk kan worden bestempeld als gebruik voor persoonlijke of huishoudelijke doeleinden. De uitspraak van het Hof van Justitie is relevant omdat het uitleg geeft aan de Europese privacyrichtlijn , die in ons land is geïmplementeerd door middel van de WBP.[18]

Andere gegevensverwerkingen waarop de WBP niet van toepassing is, zijn verwerkingen:
- door of ten behoeve van de inlichtingen- en veiligheidsdiensten;
- ten behoeve van de uitvoering van de politietaak;
- door gemeenten in de gemeentelijke basisadministratie;
- ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens;
- ten behoeve van de uitvoering van de Kieswet.

2.1.4.2 Wet politiegegevens

Nauw verwant met de Wet bescherming persoonsgegevens is de nieuwe Wet politiegegevens, afgekort Wpolg.[19] Met deze wet wordt beoogd om, met eerbiediging van de beginselen van de persoonlijke levenssfeer, meer ruimte te bieden dan de daarvoor geldende wetgeving (Wet politieregisters) voor het verwerken van gegevens ten behoeve van een optimale uitvoering van de politietaak. De wet dient een nieuw evenwicht te creëren in de bescherming van de privacy van de burger enerzijds en het belang van de rechtshandhaving anderzijds. Waar aan de rechtshandhavingskant uitdrukkelijk is gekozen voor verruiming van de wettelijke mogelijkheden tot opslag, gebruik en verstrekking van persoonsgegevens door de politie voorziet de wet aan de privacykant de nodige waarborgen voor de burger tegen ongerechtvaardigde inbreuken op zijn persoonlijke levenssfeer, althans dat zou het geval dienen te zijn volgens de memorie van toelichting.[20] Of dat daadwerkelijk zo zal zijn en of er inderdaad een nieuw evenwicht gecreëerd zal zijn met de inwerkingtreding zal de toekomst moeten uitwijzen. De wet is nog te kort van kracht om daar nu reeds zinvolle uitspraken over te kunnen doen.

Politiegegevens
De Wet politiegegevens is van toepassing op de verwerking van politiegegevens die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen, aldus artikel 1 Wpolg.

Vraag die daarbij aan de orde komt is dan wanneer een gegeven een politiegegeven is. Volgens artikel 1a Wpolg is een politiegegevens een gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt. De definitie sluit daarmee nauw aan bij die van de Wet bescherming persoonsgegevens. Een gegeven is echter pas een politiegegeven als dat wordt verwerkt in het kader van de politietaak. Een politiegegeven is dus een persoonsgegeven dat wordt verwerkt in het kader van de politietaak. Het gaat dus om het *verwerken* en om de *politietaak*.

Bewaren
Naast de definitie van een politiegegeven is het in het kader van dit rapport van belang hoe lang politiegegevens bewaard kunnen worden, zoals in het onderdeel over privacy zal blijken.

[18] EHvJ 6 november 2003 Zaak C-101/01 (Lindqvist).
[19] De Wet Politiegegevens is 1 januari 2008 in werking getreden.
[20] *Kamerstukken II* 2005-2006, 30327, nr. 3, p.1.

Indien een gegeven een politiegegeven is, kan dit volgens artikel 8 Wpolg gedurende een periode van één jaar na de datum van de eerste verwerking worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak. Daarna zijn evenwel ook nog verwerkingen toegestaan en (uiterlijk) vijf jaar na de eerste verwerking worden de gegevens uiteindelijk verwijderd. Dat laatste overigens pas als zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaak.

2.1.4.3 Telecommunicatiewet

Een andere nationale regeling die in het kader van dit rapport aandacht behoeft is de Telecommunicatiewet (Tw).[21] Het recht om met rust gelaten te worden, zoals ook wel over privacy gesproken wordt, heeft in deze wet een plek gekregen in artikel 11.7. Daarin staat dat het ongevraagd versturen van elektronische commerciële, ideële of charitatieve berichten uitsluitend is toegestaan, als aangetoond kan worden dat daarvoor toestemming is verleend. Indien het laatste het geval is, dan zijn de berichten immers niet meer ongevraagd en heeft men als het ware toestemming gegeven de rust te verstoren. Als men dit gedaan heeft is de verzender van de berichten overigens verplicht bij elke verzending duidelijk te maken dat men het verzenden kan stop zetten. Hiermee wordt het belang van het recht om rust gelaten te worden, en dat zelf ook in de hand te hebben, nog eens benadrukt.

Naast het recht om rust gelaten te worden, kan er in de Telecommunicatiewet ook een link gelegd worden met de verwerking van persoonsgegevens, de informationele privacy.
Ter implementatie van richtlijn 2002/58/EG - de richtlijn Privacy en elektronische communicatie - bevat de Telecommunicatiewet namelijk onder meer regels met betrekking tot het verwerken van verkeersgegevens en locatiegegevens.

Onder verkeersgegevens verstaat de Tw: “gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan.” Deze definitie volgt rechtstreeks uit genoemde richtlijn 2002/58/EG. Verkeersgegevens van spraaktelefonie zijn bijvoorbeeld: het oproepende en opgeroepen nummer, begin en einde van een oproep en duur van de oproep. Verkeersgegevens van mobiele telefonie omvatten tevens de locatiegegevens. De locatie van de mobiele beller is immers van belang voor het te berekenen tarief.

Voor de facturering is het vervolgens nodig dat verkeersgegevens worden gekoppeld aan de abonnees. Abonnees kunnen rechtspersonen of natuurlijke personen zijn. Gaat het om natuurlijke personen dan vallen de verkeersgegevens onder het begrip ‘persoonsgegeven’ en is de WBP ook van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking ervan.

Met de verwerking van verkeersgegevens wordt bedoeld: “verwerking als bedoeld in artikel 1, onderdeel b, van de Wet bescherming persoonsgegevens, met dien verstande dat de desbetreffende handelingen mede betrekking hebben op verkeersgegevens van abonnees die geen natuurlijke personen zijn.” Hierboven is reeds vermeld dat de WBP onder verwerking van persoonsgegevens verstaat: “elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens.” In de Tw wordt de reikwijdte van dit begrip uitgebreid tot verkeersgegevens van abonnees die geen natuurlijke personen zijn, zoals werkgevers.

Onder locatiegegevens verstaat de Tw: “gegevens die worden verwerkt in een elektronisch communicatienetwerk waarmee de geografische positie van de randapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven.” Met randapparatuur wordt hier gedoeld op bijvoorbeeld een mobiele telefoon, pocket pc, e.d. De geografische positie van een apparaat op het aardoppervlak wordt aangegeven via de breedte-,

[21] Een verwijzing naar de Tw staat op Recht.nl, <wetten.recht.nl/link/24635>.

hoogte- en lengtegraad. Met locatiegegevens kan echter niet alleen de locatie van een mobiel apparaat worden weergegeven, maar ook de reisrichting, de netwerkcel waarbinnen de randapparatuur zich bevindt en het tijdstip waarop die locatiegegevens zijn opgeslagen.

Locatiegegevens kunnen tegelijkertijd verkeersgegevens zijn, bijvoorbeeld gegevens die voor mobiele telefonie worden verwerkt over het basisstation waar het randapparaat contact mee heeft en die noodzakelijk zijn voor het overbrengen van de communicatie tussen de oproepende en opgeroepen gebruiker. Locatiegegevens moeten ook als verkeersgegevens worden beschouwd wanneer locatiegegevens worden gebruikt voor de levering van toegevoegde waardediensten.[22] Diensten met toegevoegde waarde zijn bijvoorbeeld adviezen over de voordeligste tariefpakketten, routegeleiding, verkeersinformatie, weerberichten, toeristische informatie, e.d. Vaak gaat het hierbij om locatiegebonden diensten omdat de informatie is toegespitst op de locatie waar de ontvanger zich bevindt.

Verkeersgegevens kan men onderverdelen in verschillende categorieën. Ekker illustreert dat in de volgende tabel:[23]

Doel van de verwerking	**Object van het verkeersgegeven**
- *Transmissie* De locatie van de eindapparatuur, herkomst en bestemming, routering, het netwerk waarop de communicatie begint en eindigt. - *Facturering* Duur, tijdstip (begin en einde), datum, herkomst en bestemming, het netwerk waarop de communicatie begint en eindigt, volume, de locatie van de eindapparatuur, het type van de onderliggende dienst. - *Toegevoegde waarde-dienst* De locatie van de eindapparatuur.	- *Algemeen* Duur, tijdstip (begin en einde), datum, de locatie van de eindapparatuur, het type van de onderliggende dienst. - *Routering* Herkomst en bestemming, het netwerk waarop de communicatie begint en eindigt. - *Vorm en omvang* Volume (grootte), het gebruikte protocol, het formaat.

Verkeersgegevens kunnen, aldus Ekker, voor tenminste drie verschillende doelen worden verwerkt: het mogelijk maken van transmissie, de facturering en het leveren van toegevoegde waarde-diensten. Ook kan een onderscheid worden gemaakt in het object van de verkeersgegevens: algemene gegevens over het communicatiegedrag van een gebruiker, gegevens over het transport (routering) van de communicatie en gegevens over de vorm waarin de communicatie wordt getransporteerd. Hoewel soms deze onderscheidingen door elkaar heen kunnen lopen (bijvoorbeeld gegevens over bezochte websites en klikgedrag), wijst Ekker er op dat dit geen probleem is zolang maar duidelijk is dat het beschermingsniveau steeds gelijk is.

[22] Een 'dienst met toegevoegde waarde' is een "dienst die de verwerking vereist van verkeersgegevens of locatiegegevens, niet zijnde verkeersgegevens, en die verder gaat dan hetgeen noodzakelijk is voor de overbrenging van een communicatie of de facturering daarvan."
[23] Anton Ekker, Publiekrechtelijke bescherming van verkeersgegevens. In: L.F. Asscher en A.H. Ekker (red.), *Verkeersgegevens. Een juridische en technische inventarisatie*. Amsterdam: Instituut voor Informatierecht, 2003, <www.ivir.nl/publicaties/overig/gedeelteverkeersgegevens.pdf>.

Verkeersgegevens zijn privacygevoelig omdat zij in verband kunnen worden gebracht met individuele natuurlijke personen (gebruikers en abonnees). Zij kunnen een beeld geven van het communicatiegedrag, het feitelijk handelen en zelfs van de inhoud van de communicatie van personen. Ekker onderscheidt drie stadia waarin verkeersgegevens zich kunnen bevinden:[24]

1. ruwe verkeersgegevens: de gegevens zijn bij de transporteur maar nog niet gekoppeld aan personen.
2. verwerkte verkeersgegevens: de verkeersgegevens zijn wel gekoppeld aan personen, bijvoorbeeld ter facturering. De gegevens bevatten informatie over het communicatiegedrag van personen. Als voorbeelden noemt Ekker:
    - Alice heeft Bob om zes uur 's avonds opgebeld;
    - Alice heeft Bob om tien uur 's ochtends een e-mail gestuurd;
    - Alice en Bob hebben van 2 tot 3 uur 's middags samen deelgenomen aan een chat-sessie;
    - Alice heeft Bob om 3 uur 's middags opgebeld vanaf Den Haag Centraal Station, terwijl Bob zich bevond op het Museumplein te Amsterdam en zich verplaatste richting het Leidseplein.

Dit laatste voorbeeld van informatie bevat tevens locatiegegevens die kunnen worden gegenereerd bij mobiele communicatie.

3. verkeersgegevens gecombineerd met andere gegevens: door verkeersgegevens te combineren met andere gegevens, kan soms al meer informatie worden gegenereerd over de mogelijke inhoud van de communicatie. Enkele voorbeelden kunnen dat verduidelijken:
    - Alice heeft gebeld met haar advocaat, haar psycholoog, het ziekenhuis, de nummerinformatie van KPN, het Centrum voor Werk en Inkomen, het Bureau Kredietregistratie, of het alarmnummer 1-1-2.
    - Alice heeft ingelogd op de website van Alcoholics Anonymous en deelgenomen aan een chatsessie.
    - Alice heeft ingelogd op de website van de gemeente Amsterdam en op een bulletin-board kritiek geuit op het parkeerbeleid van de gemeente.
    - Alice heeft van de website van een politieke partij het partijprogramma gedownload en een folder besteld waarmee zij lid kan worden van die partij.

Een conclusie die hieruit kan worden getrokken is dat het kan lijken dat verkeersgegevens niet van invloed zijn op de privacy van gebruikers van elektronische communicatiediensten, maar dat door koppeling van verkeersgegevens aan personen meer of minder gevoelige informatie kan worden gegenereerd over het communicatiegedrag van personen en over de inhoud daarvan.

2.2 De verschillende gedaanten van privacy

Het voorgaande heeft duidelijk gemaakt dat privacy toch vooral te maken heeft met het recht om rust gelaten te worden. 'The right to be left alone', zoals Warren en Brandeis dat meer dan 100 geleden al beschreven in hun beroemde artikel *The Right to Privacy*.[25] Dat is de kern, maar niet de sluitende definitie. Die is namelijk tot op heden niet gegeven, bewust niet. Althans, niet door het Europees Hof van de Rechten voor de Mens (EHRM) dat in 1992 stelde: 'The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "*private life*".'

[24] Ekker, a.w., p. 47.
[25] Samuel Warren & Louis Brandeis, The Right to Privacy, Harvard Law Review, No.5, 1890. Dit artikel is onder meer beschikbaar op de website van de Lawrence University, Appleton, Wisconsin, <www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html>

Wel staat vast staat dat het Hof vandaag de dag een ruime invulling hanteert van het privacybegrip en gerelateerde begrippen zoals communicatie en correspondentie.[26] Zo stelde het Hof in het arrest *Niemietz*[27] over het privacybegrip dat werknemers een gerechtvaardigd belang hebben om ook gedurende het uitvoeren van bedrijfsmatige activiteiten relaties met andere mensen aan te kunnen gaan. Een zekere mate van vrijheid om met anderen al dan niet persoonlijk te kunnen communiceren zonder inmenging door de werkgever is in dat kader onontbeerlijk. Artikel 8 EVRM beschermt het individu dus niet alleen tegen inbreuken door de overheid, maar ook tegen inbreuken door particulieren, zoals werkgevers. In het arrest *Halford* maakte het Hof duidelijk dat ook telefoongesprekken, gevoerd met een zakelijk toestel, of onder een zakelijk nummer, onder de bescherming van artikel 8 vallen.[28]

Hiernaast blijkt uit het arrest *P.G. en J.H.* dat het voortaan denkbaar is om niet alleen in de private of professionele sfeer, maar ook in de publieke sfeer een beroep te doen op de bescherming geboden door het privacygrondrecht.[29] Deze principiële erkenning van het concept *publieke privacy* gebeurde een jaar eerder in het arrest *Rotaru t. Roemenië*.[30] Steunend op eerdere arresten zoals *Amann t. Zwitserland* en verwijzend naar de beginselen van het *data protection* recht (zie onder), verklaarde het Hof, in deze zaak over door de overheid opgeslagen

[26] In *Klass* bepaalde het EHRM dat ook telefoonverkeer onder de bescherming van artikel 8 valt. Het Hof kiest daarbij niet voor een extensieve interpretatie van het begrip correspondentie maar voor een combinatie van privé-leven en correspondentie. In *Malone* gaf het Hof aan dat ook *metering records* en in het bijzonder het gekozen telefoonnummer integraal deel uitmaken van de beschermde communicatie. Cf. EHRM 2 augustus 1884 (*Malone*), *NJ* 1988, 534; Hofman 1995, 70-71; A.J. Nieuwenhuis, 'Vertrouwde en virtuele bescherming', *NJCM-Bulletin* 4, 1998, 429. In het arrest *P.G. en J.H. t. het Verenigd Koninkrijk* (*infra*) is het EHRM is van mening dat de opname van het stemgeluid aangemerkt dient te worden als een registratie van een persoonsgegeven (§ 59) en onder de werking van art. 8 EVRM valt (§ 60), Tevens wordt het opvragen van de nummers die gedraaid waren met de telefoon eveneens gezien als een handeling die onder toepassing van het privacygrondrecht valt. Over nieuwere toezichttechnieken zijn nog geen uitspraken. Over het algemeen wordt echter aangenomen dat het EHRM te zijner tijd door een verdragsdynamische interpretatie ook e-mail onder artikel 8 zal brengen. Cf. H.H. de Vries, 'Vertrouwelijkheid van e-mail in arbeidsverhoudingen', 116-117 in H.W.K Kaspersen & C. Stuurman, *Juridische aspecten van e-mail*, Deventer: Kluwer, 2001, 111-139; L. Ascher. & W. Steenbruggen, 'Het Emailgeheim op de werkplek. Over de toelaatbaarheid van inbreuken op het communicatiegeheim van de werknemer in het digitale tijdperk', *Nederlands juristenblad*, 2001-37, 1788.

[27] EHRM 16 december 1992 (*Niemietz*), *NJ* 1993, 400.

[28] EHRM 25 juni 1997 (*Halford*), *NJ* 1998, 506. Mevrouw Halford was Assistant Chief Constable bij een Engels politiekorps. In verband met een rechtszaak tegen haar werkgever wegens ongelijke behandeling had zij de beschikking over een tweede telefoon die was uitgezonderd van de standaardcontrole van de telefoons van het politiebureau. Uit het bewijs dat in de rechtszaak was overlegd, kon worden afgeleid dat de werkgever waarschijnlijk de gesprekken die via de speciale telefoon waren gevoerd, had afgeluisterd. Het Hof overwoog dat 'the right to private life and correspondence' zich ook uitstrekt tot de werkplek. Omdat er geen waarschuwing was gegeven dat de telefoongesprekken werden opgenomen, had zij een 'reasonable expectation of privacy', hetgeen werd versterkt door bijkomende factoren waaronder het feit dat de telefoon specifiek ter beschikking was gesteld voor privé-gebruik. Het enkele bekend zijn van de mogelijkheid tot meeluisteren of opnemen rechtvaardigt op zichzelf het gebruik daarvan evenwel niet. Kenbaarheid van de (mogelijkheid tot) controle is niet meer dan een basisvoorwaarde voor de rechtmatigheid ervan.

[29] EHRM, 25 september 2001 (*P.G. en J.H. t. Verenigd Koninkrijk*). Cf. P. De Hert, , 'Het Europees Hof Rechten van de Mens erkent publieke privacy. De legaliteitseis en het politioneel optreden in het licht van artikel 8 EVRM', *Nieuw Juridisch Weekblad*, 2002, Vol. 1/4, 9 oktober 2002, 116-122.

[30] EHRM, 4 mei 2000 (*Rotaru t. Roemenië*), *ECHR*, 2000-V. Het arrest is tevens opgenomen in *Revue trimesterielle des droits de l'homme*, 2001, 138-183, noot O. De Schutter.

persoonsgegevens , dat 'publieke informatie' over een persoon onder de werking van art. 8 EVRM valt, wanneer deze systematisch wordt verzameld of blijvend wordt opgeslagen in overheidsbestanden.[31]

In het arrest *P.G. en J.H. t. het Verenigd Koninkrijk* wordt naar deze passage uit *Rotaru* verwezen, maar gaat het Europees Hof verder. Het Hof stelt voorop dat het begrip 'privé-leven' een ruim begrip is dat moeilijk te definiëren is. Het begrip omvat in ieder geval het recht op identiteit, op persoonlijke ontwikkeling en het recht op het ontwikkelen en onderhouden van relaties met anderen en de buitenwereld. Deze relaties kunnen ook een zakelijk karakter hebben. Dit betekent dat de bescherming van het privé-leven zich tot het publieke domein kan uitstrekken.[32]

Hiermee is weliswaar geen definitie gegeven, maar is wel duidelijk dat het recht om rust gelaten te worden verder gaat dan eigen lichaam, huis en tuin. Daarbij is er ruimte om uiteenlopende waarden te beschermen. [33]

Het aantal beschermde waarden is nog toegenomen met het recht op bescherming van persoonlijke gegevens. Dit recht, dat recentelijk als nieuw grondrecht is opgenomen in art. 8 van het Handvest van de Grondrechten van de Europese Unie, overlapt slechts ten dele met het privacyrecht. Het focust tevens op aspecten van procedurele rechtvaardigheid en gelijkheid die aan de orde komen bij het verwerken van persoonsgegevens. Het recht op bescherming van persoonsgegevens legt om die reden ook andere klemtonen dan het privacyrecht. Zo is het bijvoorbeeld verre van evident om een telefoonnummer in alle gevallen te laten vallen onder de bescherming van het privacyrecht, terwijl over de toepassing van het gegevensbeschermingsrecht op telefoonnummers geen enkele twijfel bestaat. Telefoonnummers zijn immers bijna altijd persoonsgegevens zoals de Registratiekamer in 1993 al vaststelde.[34]

Het (ruime) recht om met rust gelaten te worden en het gegevensbeschermingsrecht kunnen dus een rol spelen bij diensten waarbij geo-informatie verwerkt wordt. Bij de beoordeling van geo-diensten in het licht van privacy dient daarom beoordeeld te worden of de rust in het geding is, of de regels die betrekking hebben op (persoonlijke) gegevens, of misschien wel allebei. Dan kan bepaald worden, welke ((inter)nationale) regels van toepassing zijn.

---

[31] EHRM*, Rotaru t. Roemenië*, *l.c.*, § 43.

[32] Cf. EHRM, 25 september 2001 (*P.G. en J.H. tegen het Verenigd Koninkrijk*), § 56. Ten aanzien van het antwoord op de vraag wanneer zich een inmenging in het privé-leven voordoet in geval een persoon zich in het publieke domein bevindt, zijn volgens het Hof een aantal factoren relevant. In een situatie waarin iemand weet dat hij gefilmd wordt of anderszins wordt waargenomen, zijn *reasonable expectations of privacy* van belang, maar niet doorslaggevend. Het privé-leven komt in het geding wanneer het (opgenomen) materiaal systematisch of blijvend wordt opgeslagen. Het is daarom dat het EHRM eerder heeft uitgemaakt (in de zaak *Rotaru tegen Roemenië*) dat een dossier met daarin de door de veiligheidsdienst verzamelde gegevens over een persoon onder de werking van art. 8 EVRM valt, ook in geval de gegevens niet op een heimelijke of slinkse wijze zijn verkregen. Het Hof wijst verder nog op de zaak *Amann tegen Zwitserland*, waarin het aannam dat een kaartsysteem met gegevens over de klager een inbreuk op zijn privé-leven vormde, ook al betrof het geen gevoelige gegevens en ook al waren deze waarschijnlijk nooit geraadpleegd.

[33] Huidige bescherming privacy loopt ver achter, A. Vedder, Trouw, 23-10-2007. Een verwijzing naar het artikel staat op Recht.nl, <www.recht.nl/30387>.

[34] Registratiekamer, 8 juli 1993, 93.A.002 (Bestrijding van misbruik van het 06-11 alarmnummer). In: B.J. Crouwers-Verbrugge, B.M.A. van Eck, E. Schreuders (red.), *Persoonsgegevens beschermd. Uitspraken van de Registratiekamer.* Den Haag: Sdu Uitgevers Juridisch & Fiscaal, 1997, p. 101 e.v.

2.3 Privacy en geodiensten

Bij diensten waarbij geo-informatie een rol speelt, wordt in dit rapport – als eerder gezegd - een onderscheid gemaakt tussen (mobiele) locatiegebonden diensten (ook location based services, LBS genoemd) en GIS (geografische informatiesystemen).

In het geval van locatiegebonden diensten wordt geo-informatie gebruikt om de locatie van objecten of subjecten te bepalen en kunnen aan de hand daarvan verschillende diensten worden geleverd. Zo zou iemand een bericht op zijn mobiele telefoon kunnen ontvangen indien hij zich in een gebied begeeft waar giftige stoffen vrijgekomen zijn als gevolg van een brand. De dienst hoeft hierbij dus niet tot gevolg te hebben dat er een grafische weergave van (de locatie van) het object of het subject gegeven wordt, maar op basis van de locatie wordt een subject van informatie voorzien.

GIS heeft een andere inslag. Een geografisch informatiesysteem is een informatiesysteem waarmee (ruimtelijke) informatie over geografische objecten kan worden opgeslagen, beheerd, bewerkt, geanalyseerd en/of gepresenteerd. Met name het laatste, het presenteren, het visualiseren van de ruimtelijke informatie is de bekendste toepassing. [35] Een GIS zal veelal geen informatie bevatten betreffende een geïdentificeerde of identificeerbare natuurlijke persoon en om die reden minder vaak in verband gebracht worden met privacy. Het kan echter wel, zoals hieronder nader wordt toegelicht.

Vanzelfsprekend kan een systeem ook een combinatie zijn van een LBS en een GIS. Zo bepaalt een navigatiesysteem in een auto de locatie, de plaats, waar de gebruiker zich bevindt en zal het systeem vervolgens een kaart weergeven van die betreffende locatie.

Hierna volgt een korte beschrijving van een aantal locatiegebonden systemen en een enkel geografisch informatiesysteem. De keuze is daarbij gevallen op diensten die een meer dan gemiddelde aandacht hebben genoten of nog steeds genieten in de maatschappij.

2.4 Locatiegebonden diensten

2.4.1 Sms-dienstverlening

Sms-dienstverlening is er in verschillende vormen. Deze verschillende vormen hebben elk een eigen relatie tot geo-informatie en worden voor verschillende doeleinden ingezet. In dit rapport komen de sms-alert, de groeps-sms en de sms-bom aan de orde.

2.4.1.1 Sms-alert

Sms-alert is een dienst die voor het eerst is gebruikt door het politiekorps Midden en West Brabant. Het is een dienst die dit korps in staat stelt om bewoners te informeren over allerlei zaken die met veiligheid in de wijk te maken hebben. Zo kan de politie via een sms-bericht informatie geven over bijvoorbeeld een inbreker die in de buurt is gesignaleerd of over een buurtbewoner die vermist is. Door de burgers erbij te betrekken hoopt de politie dat dit zal leiden tot een snelle aanhouding van de inbreker of tot het vinden van de vermiste persoon.

Daarnaast kan de politie via sms-alert preventieberichten versturen. Indien er bijvoorbeeld personen in een buurt actief zijn die met babbeltrucs mensen proberen geld afhandig te maken, kunnen bewoners door middel van een alert daarvoor gewaarschuwd worden.

Behalve voor burgers is er ook een soortgelijke dienst voor winkeliers. Ook in Noord-Brabant. Aldaar hebben winkeliers zich aangemeld voor een sms-dienst waarbij berichten verstuurd

[35] Geografisch informatiesysteem, <nl.wikipedia.org/wiki/Geografisch_informatiesysteem>

worden indien de veiligheid van de winkels in het geding is of ander gevaar dreigt. Zo heeft de politie deze winkeliers enige tijd geleden gewaarschuwd dat een man in een winkel had geprobeerd met een vals biljet van 100 euro af te rekenen. Omdat de politie vermoedde dat de man dit bij andere winkels ook zou proberen, is een sms-alert verstuurd om de andere winkeliers te waarschuwen.[36]

De sms-alert kan dus ingezet worden om de assistentie van burgers in te roepen bij het politiewerk, maar kan ook voor preventie ingezet worden.[37]

Inmiddels heeft sms-alert in ons land ruim 160.000 deelnemers verspreid over 10 politieregio´s. Het middel is in 2007 378 keer ingezet en heeft in 55 gevallen tot resultaat geleid. Zo zijn inbrekers aangehouden, gevaarlijke medicijnen terug bezorgd, en vermiste personen gevonden.[38]

De geo-informatie die een rol speelt bij het gebruik van sms-alert is statisch. Het betreft immers de postcode van burgers of winkels in de verschillende regio´s en die zijn niet regelmatig aan verandering onderhevig. Sterker, de postcode verandert nooit. Alleen degene die zich aanmeldt voor de dienst zou zich op een zeker moment kunnen afmelden omdat hij, of de winkel waarvan hij eigenaar is, verhuist.

Indien zich een incident voordoet, wordt allereerst de postcode vastgesteld. Vervolgens wordt een straal bepaald en wordt aan de deelnemers die binnen die straal wonen of een winkel hebben, een sms-bericht gestuurd. Als mensen zich, om wat voor reden dan ook, niet in hun eigen postcodegebied ophouden, zullen zij ook een bericht ontvangen. Deelnemers aan sms-alert worden dus niet gevolgd. De politie stuurt een bericht op basis van de postcode en zal niet controleren of de deelnemers zich daadwerkelijk in het postcodegebied bevinden.

Deelname aan sms-alert vindt plaats op vrijwillige basis. Men kan zich op elk gewenst moment afmelden.

De enige kosten die aan sms-alert verbonden zijn, betreffen de kosten van de sms, die men verstuurt om zich aan te melden.

2.4.1.2 Groeps-sms

Sms-alert wordt ingezet voor opsporing en preventie in bepaalde postcodegebieden. Het is echter heel goed denkbaar dat een incident zich voordoet in een zeker postcodegebied, en dat er op het moment dat het incident plaatsvindt ook mensen in het gebied zijn, die niet wonen in het betreffende gebied. Soms is het echter wel wenselijk als de politie ook die personen zou kunnen benaderen. Het gaat dan eigenlijk om een sms-alert die verzonden wordt naar personen die op een zeker moment op een bepaalde plek aanwezig waren. Ter onderscheid van de sms-alert die in ons land vooral wordt ingezet voor buurtpreventie, wordt een dergelijk bericht hier een groeps-sms genoemd. Het is immers een bericht naar een bepaalde groep mensen, die op een zeker moment iets gemeen hadden, zoals het in de nabijheid zijn van een bepaalde gebeurtenis.

De groeps-sms is door de politie ingezet in een aantal geruchtmakende zaken. Zo heeft de politie een groeps-sms gestuurd naar zo´n 3000 personen die 15 november 2005 rond 21.00 uur, de avond dat Louis Sévèke werd vermoord, in het centrum van Nijmegen waren. De politie verzocht

[36] Politie stuurt groeps-sms over vals geld, Zibb.nl, 21 juli 2006 (<www.zibb.nl> vul groeps-sms in in het zoekveld).
[37] Sms-alerts kunnen overigens voor tal van zaken ingezet worden. Zo waarschuwt Waterbedrijf Oasen hun klanten per sms als er iets mis is met het drinkwater. Zie de website van Oasen <www.oasen.nl>.
[38] SMS-Alert van politie 55 keer raak, NU.nl, 28 december 2007, <www.nu.nl/news.jsp?n=1370369&c=50>

in het bericht deze personen 's avonds te kijken naar de uitzending van AVRO's Opsporing Verzocht.

Ook in het kader van het onderzoek naar de moord op Anneke van de Stap heeft de politie een groeps-sms gestuurd, tot twee keer toe zelfs.[39]

Niet alleen in moordzaken is een groeps-sms ingezet. De allereerste keer dat het middel gebruikt werd, was kort na de rellen die plaatsvonden bij de Rotterdamse Kuip na de wedstrijd Feyenoord – Ajax enige tijd geleden. De politie stuurde destijds een sms naar 17.000 telefoons op zoek naar getuigen.[40]

In de beschreven gevallen was het doel van het bericht hetzelfde als bij de sms-alert, namelijk assistentie vragen aan burgers. Belangrijk verschil is gelegen in het feit dat een sms-alert alleen ontvangen wordt door een burger die zich daarvoor vrijwillig heeft opgegeven, terwijl bij de groeps-sms zoals beschreven, iedere bezitter van een geactiveerde mobiele telefoon en in de buurt bij de genoemde incidenten, een bericht ontvangt.

De geo-informatie die bij deze zaken een rol speelde, betrof de locatiegegevens van de mobiele telefoons in de buurt én geactiveerd ten tijde van de incidenten. Deze gegevens had de politie nodig om een sms naar de betreffende groep te kunnen sturen. Daartoe zijn deze locatiegegevens opgevraagd op basis van de Wet vorderen gegevens telecommunicatie. Een wet ter aanpassing van het Wetboek van Strafvordering die in 2004 in werking getreden is en die naast verkeersgegevens, de zogenaamde gebruikersgegevens (naam, adres, postcode, woonplaats, nummer en soort dienst waarvan personen gebruikmaken) introduceerde als gegevens die ten behoeve van de strafvordering en door de inlichtingen- en veiligheidsdiensten kunnen worden opgevraagd.

Interessant hierbij lijkt het detail dat de bovengenoemde gegevens alleen door een opsporingsambtenaar opgevraagd mogen worden in geval van verdenking van een misdrijf. Was het nodig dat alle personen die ge-sms't zijn na de voetbalrellen en de moorden op Sévèke en Van der Stap - zo'n 50.000 in totaal –verdacht waren van een misdrijf? Volgens Sjoera Nas. destijds van de stichting Bits of Freedom, zou dit inderdaad het geval moeten zijn en zij stelde dan ook al kort na de groeps-sms inzake de voetbalrellen dat de actie van justitie onwettig was. Een signaal dat overigens door niets of niemand is opgepikt, want in de zaken Sévèke en Van der Stap werden immers weer duizenden "verdachten" ge-sms't. Er zou hier dus sprake kunnen zijn van een juridische drempel voor het gebruik van de groeps-sms door politie en justitie.[41] Of dit daadwerkelijk het geval is wordt in hoofdstuk 2.6.3 nader uiteengezet.

Vooralsnog is het evenwel zo dat bezitters van mobiele telefoons die aanwezig zijn in de buurt van incidenten een bericht van de politie kunnen verwachten als het onderzoek dat vereist. Het is iets dat mogelijk zal gebeuren en waaraan men zich niet kan onttrekken. Men is evenwel niet verplicht te reageren op een groeps-sms.

2.4.1.3 Sms-bom

Zijn de sms-alert en de groeps-sms technieken met behulp waarvan de burger om assistentie gevraagd kan worden of om burgers te waarschuwen, de sms-bom heeft vooral als doel dieven van mobiele telefoons te dwarsbomen. Indien een mobiele telefoon is gestolen en daarvan is

[39] Tweede SMS actie in zaak Anneke van der Stap, Rijksrecherche.nl, 11 september 2006 (<www.rijksrecherche.nl> vul *anneke* in in het zoekveld).
[40] Politie spoort hooligans op met sms, Webwereld, 31 augustus 2005 (<www.webwereld.nl> vul *hooligans* in in het zoekveld)
[41] SMS-actie politie is onwettig en immoreel, Sjoera Nas, Friesch Dagblad, 5 september 2005. Dit stuk is ook beschikbaar op de site van Bits of Freedom, <www.bof.nl/docs/opiniesmsactie.pdf>.

aangifte gedaan, dan kan de politie de sms-bom inzetten om het gebruik van de telefoon onaangenaam te maken. De politie stuurt dan met een bepaalde regelmaat sms´jes naar het gestolen toestel met de tekst: 'Dit toestel is gejat, koop of verkoop is strafbaar. De Politie'. Met de sms-bom hoopt de politie dat het stelen van een mobiele telefoon onaantrekkelijk wordt gemaakt.

Verschil met de sms-alert en de groeps-sms is dat er niet één bericht naar een (groot) aantal mobiele telefoons gestuurd wordt, maar juist een groot aantal van dezelfde berichten naar één en dezelfde telefoon.

Overigens worden in het geval van een sms-bom de berichten niet naar het telefoonnummer gestuurd, maar naar het zogenaamde IMEI (International Mobile Equipment Identity)-nummer, een unieke cijfercombinatie die op iedere mobiele telefoon opgeslagen is en die in principe niet verwijderd kan worden. De vermeende dief kan dus niet de simkaart uit het gestolen toestel halen om het vervolgens ongestoord te kunnen gebruiken.

Om de sms-bom te gebruiken heeft de politie dus alleen het IMEI-nummer nodig, geen locatiegegevens. Zonder geo-informatie is de politie dus in staat het leven van de gebruiker van een gestolen mobiele telefoon op zijn minst iets zuurder te maken. Aan de andere kant zou men het toestel wel kunnen traceren op basis van het genoemde IMEI-nummer in combinatie met locatiegegevens en zo wellicht de dief in de kraag kunnen pakken. Echter, gezien het feit dat een persoon mobiel is en dat de plaatsbepaling (nog) niet op de centimeter nauwkeurig kan plaatsvinden, zou dat veel moeite kosten. Gekoppeld aan de steeds goedkoper wordende mobiele telefoons, maakt dat het niet proportioneel is dergelijke middelen in te zetten. De relatief eenvoudige sms-bom lijkt, kijkend naar kosten en baten, een adequater middel.

Van de drie besproken toepassingen maakt de sms-alert gebruik van statische geo-informatie, de postcode, maakt de groeps-sms gebruik van dynamische geo-informatie, locatiegegevens van de gebruiker van een mobiele telefoon, en wordt in het geval van de sms-bom geen gebruik gemaakt van geo-informatie, maar van een uniek toestelnummer, het IMEI.

2.4.2 Cell broadcast

Een middel dat nogal eens in één adem genoemd wordt met sms is cell broadcast.[42] Niet vreemd, want ook cell broadcast wordt toegepast om tekstberichten te versturen naar mobiele telefoons . Anders dan bij sms worden met een cell broadcast echter berichten gestuurd naar een gebied, een cell. Alle mobiele telefoons binnen zo´n cell ontvangen dan het verzonden bericht, waarbij het niet nodig is te weten welke telefoonnummers het betreft.

Cell broadcast is als middel nog niet operationeel. Wel hebben er enkele proeven plaatsgevonden.[43] Deze maakten duidelijk dat cell broadcast geschikt is om bijvoorbeeld mensen tijdens een ramp te informeren. Naast de melding kunnen mensen via het bericht namelijk ook eenvoudig en snel informatie krijgen hoe te handelen. Bij overbelasting van het mobiele netwerk is er geen mobiel telefoonverkeer mogelijk. Een voordeel van cell broadcast is, dat het daar geen last van heeft. En door de toevoeging van een “tekst naar spraak”-applicatie kan een tekstbericht dat naar de mobiele telefoon wordt verzonden ook worden uitgesproken, zodat ook slechtzienden en automobilisten kunnen worden bereikt.[44]

Cell broadcast kan hiermee als een aanvulling op, en op termijn mogelijk zelfs als vervanging van, het bekende sirenesysteem worden gezien. De bezitter van een mobiele telefoon heeft deze

[42] Cell broadcast, Wikipedia, <en.wikipedia.org/wiki/Cell_Broadcast>
[43] Overheid informeert burger met tekstbericht, Digitaal Bestuur, 6 april 2007, (<digitaalbestuur.nl> *tekstbericht* invullen in zoekveld)
[44] Rampeninformatie via de mobiele telefoon binnen handbereik, ministerie van BZK, 6 april 2007 (<www.minbzk.nl> zoeken naar *cell broadcast*)

immers bijna altijd bij zich en met een penetratie van boven de 100% is deze telefoon ook alom aanwezig.[45]

Juridisch lijken er weinig haken en ogen te zitten aan het gebruik van cell broadcast. Bij het gebruik van cell broadcast is het niet nodig te weten, wie, of welke mobiele telefoon zich in het rampgebied bevindt. Privacy speelt zodoende geen rol.

Het enige aspect dat wellicht via regulering tot stand gebracht zou moeten worden, is de samenwerking tussen telecomproviders. Om dit systeem te kunnen realiseren dienen namelijk alle telecomproviders mee te werken. Pas dan kan het landelijk en voor elke gebruiker van een mobiele telefoon toegepast worden. Het laten samenwerken van natuurlijke concurrenten zal echter lastig zijn. Dit zou gerealiseerd kunnen door er geld tegenover te stellen, of wellicht door bij wet te regelen dat telecomproviders cell broadcast moeten toestaan voor publieke locatiegebonden diensten.[46]

2.4.3 Kilometerprijs

Mobiliteit vormt een essentieel onderdeel van ons welzijn, onze vrijheid en onze economie. Probleem is evenwel dat de mobiliteit groeit en dat de infrastructuur slechts in beperkte mate wordt uitgebreid. Nederland dreigt daardoor vast te lopen met alle gevolgen van dien voor welzijn, vrijheid en economie. Hierbij komt dat de huidige systematiek voor het betalen voor automobiliteit onvoldoende transparant en eerlijk is.[47]

Om het vastlopen van ons land te voorkomen en om de lasten eerlijker over de gebruikers te verdelen wordt al jaren lang gesproken over het invoeren van een andere manier van betalen voor mobiliteit. Het aanvankelijk bedachte systeem werd rekeningrijden genoemd.[48] Dit was simpel gezegd een systeem van elektronische tolpoorten rond met name de grote steden dat er toe zou moeten leiden dat mensen op een andere manier of op een ander tijdstip naar die steden zouden gaan. Het zou met name rond de spits actief dienen te zijn. Dit systeem heeft het na lang wikken en wegen niet gehaald.

Grote tegenstander van het rekeningrijden, voormalig ANWB-baas Nouwen is later voorzitter van het Nationaal Platform Anders Betalen voor Mobiliteit geworden. Dit platform heeft in 2005 een advies geschreven over een andere manier van betalen voor mobiliteit.[49] Over dezelfde materie is eind 2007 het rapport *Starten met de Kilometerprijs* verschenen.[50] Een en ander heeft er toe geleid dat er een ander systeem gaat komen voor het betalen voor mobiliteit: de kilometerprijs. Althans dat zijn de plannen.

Het systeem kilometerprijs houdt in dat de burgers niet langer betalen voor het bezit, maar voor het gebruik van de auto. De motorrijtuigenbelasting (MRB) en de aanschafbelasting, de BPM, worden afgebouwd en de burgers gaan per kilometer betalen. Wie weinig rijdt betaalt minder, wie

---

[45] Zie voor laatste informatie over Nederland <ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3304>, geraadpleegd op 10 december 2007.
[46] Rapport Locatiegebonden Publieke Diensten, ministerie van BZK (<www.minbzk.nl> zoeken naar *locatiegebonden*)
[47] Rapport Nationaal Platform Anders Betalen voor Mobiliteit, zie de website van het platform (<www.andersbetalenvoormobiliteit.nl> onder de knop *Advies*.
[48] Dossier Rekeningrijden, NRC Handelsblad <www.nrc.nl/W2/Lab/Rekeningrijden/>.
[49] Zie noot 15.
[50] Starten met de kilometerprijs. Overzicht van voorbereidend onderzoek bij het kabinetsbesluit over de kilometerprijs., ministerie van Verkeer en Waterstaat. Het rapport staat op de site van dit ministerie, <www.verkeerenwaterstaat.nl>. Klik op *Mobiliteit en bereikbaarheid* en vervolgens op *Anders Betalen voor Mobiliteit*.

veel rijdt betaalt meer. Maar ook zal men meer moeten gaan betalen voor auto's die meer vervuilen en voor het rijden op drukke tijden en drukke wegen. En in tegenstelling tot rekeningrijden gaat het systeem niet gelden voor drukke gebieden, maar voor het gehele land.

Voor het kilometerprijssysteem heeft men verschillende technologieën bestudeerd. Het zogenaamde eindbeeld dat in het rapport inzake de kilometerprijs wordt geschetst houdt in dat er een satellietnavigatie (gps/Galileo) in elk voertuig komt en dat er mobiele telecommunicatie (gsm/GPRS) van ritgegevens plaatsvindt naar een rekencentrum. Het laatste is onder meer nodig voor de facturering. Hierbij kan het te betalen bedrag in de voertuigapparatuur berekend worden en dan ter facturering middels mobiele communicatie naar een rekencentrum gestuurd worden, of kunnen de verplaatsingsgegevens naar een rekencentrum worden gestuurd en wordt pas daar het bedrag uitgerekend. Het zal duidelijk zijn dat de eerstgenoemde systematiek minder privacygevoelig is dan de tweede. De verplaatsingsgegevens blijven dan immers in het voertuig. Het College bescherming persoonsgegevens (CBP) heeft dan ook een voorkeur voor die eerste.[51]

Behalve privacy speelt nog een tweetal juridische zaken een rol bij de ontwikkeling van het systeem dat betalen per kilometer mogelijk moet maken. De eerste betreft de organisatie waarbij gekeken wordt naar de juridische kwalificatie van het systeem: prijs, retributie, bestemmingsheffing en belasting. De tweede staat in verband met Europese regelgeving en heeft betrekking op de interoperabiliteit van het systeem. Beide juridische onderwerpen hebben weinig met geo-informatie te maken, maar zijn wel van belang voor het systeem van betalen per kilometer.

2.4.4 Locatiebepaling gsm bij gebruik 112

Locatiebepaling met gsm´s wordt steeds populairder. Zo wordt de bepaling van de plaats waar een gsm zich bevindt, gebruikt bij commerciële diensten om vrienden te lokaliseren die in de buurt zijn. Ook kan de locatie van de gsm aanleiding zijn de gebruiker informatie aan te bieden over restaurants, parkeerplaatsen, bioscopen, etc.[52] Dit soort diensten wordt ook steeds beter omdat de plaatsbepaling steeds nauwkeuriger wordt.

Naast commerciële partijen heeft ook de overheid te maken met locatiebepaling van mobiele telefoons. Zo is de bepaling van de locatie van een persoon die het alarmnummer 112 belt van groot belang. Die bepaling is bij gebruik van een vaste lijn eenvoudig te achterhalen. Indien iemand evenwel zijn mobiele telefoon gebruikt, is dit een stuk lastiger. Aan de adresgegevens van de gebruiker van een mobiele telefoon heb je immers niet veel, omdat de kans groot is dat deze niet van huis uit belt naar 112. Om die reden komt een mobiele beller van het alarmnummer dan ook terecht bij het callcenter van het Korps Landelijke Politie Diensten (KLPD) in Driebergen. Het callcenter bepaalt vervolgens in samenspraak met de beller de locatie om deze daarna door te geven aan de hulpdiensten.[53]

Het zou desalniettemin makkelijk en beter zijn als de locatie van een mobiele beller (ook) bepaald kan worden met technische hulpmiddelen. Een gebruiker van een mobiele telefoon die 112 belt bevindt zich immers in of nabij een noodsituatie waardoor hij wellicht niet goed kan overzien waar hij zicht bevindt. Daarnaast kan een dergelijke persoon in een voor hem onbekende omgeving zijn en om die reden moeilijk kunnen inschatten waar hij is. Ook kan er verwarring ontstaan als gevolg van het feit dat er plaatsen in ons land zijn die (zo goed als) dezelfde naam hebben. Zo

[51] Brief hoorzitting kilometerprijs 31 januari 2008, CBP (<www.cbpweb.nl> en zoek op trefwoord *kilometerprijs*).
[52] Gebruik locatiebepaling gsm via satelliet in opmars, Tweakers.net, 10 april 2006 (<tweakers.net> zoeken naar locatiebepaling gsm.
[53] Hoe werkt 1-1-2?, website 1-1-2 <www.sos112.nl/hoe-werkt-1-1-2>.

kent ons land drie plaatsen met de naam Rijswijk[54] en is het verschil tussen Oudorp (Noord-Holland) en Ouddorp (Zeeland) niet hoorbaar.

Belangrijkste voordeel van een (nauwkeurige) plaatsbepaling van een mobiele beller is uiteraard dat hulpdiensten dan sneller op de juiste plek zijn hetgeen tot minder leed kan leiden. Daarnaast kan in geval van meerdere meldingen eenvoudig vastgesteld worden dat die meldingen hetzelfde noodgeval betreffen. En prettige bijkomstigheid van een nauwkeurige plaatsbepaling van mobiele bellers van alarmnummers zou ook nog kunnen zijn dat dit misbruik tegen gaat. [55] Misbruikers kunnen met behulp van nauwkeurige plaatsbepaling immers makkelijker in de kraag gevat worden.

Bij het bellen van het alarmnummer 112 door gebruikers van mobiele telefoons – of in de toekomst door voertuigen zelf[56] - en de daaropvolgende bepaling van de locatie van deze personen is overduidelijk sprake van geo-informatie en spelen juridische aspecten een rol. Zo wordt in een aanbeveling[57] van de Europese Commissie inzake de verwerking van locatie-informatie door noodoproepdiensten verwezen naar de richtlijn betreffende privacy en elektronische communicatie.[58] Dit in verband het weergeven van oproepgegevens van de beller in geval van noodsituaties. In het hoofdstuk inzake juridische aspecten wordt hier nader op ingegaan.

2.4.5 OV-chipkaart

De OV-chipkaart is een kaart die gebruikers toegang moet geven tot alle onderdelen van het openbaar vervoer: trein, bus, tram, metro. In 2005 is men gestart met een pilot in de Rotterdamse metro en 1 januari 2009 moet de kaart landelijk ingevoerd zijn. Of dat laatste daadwerkelijk gaat lukken valt gezien recente perikelen omtrent de veiligheid van de chip op de kaart te betwijfelen, maar dat is voor dit stuk niet belangrijk.[59] Dat die chip niet veilig blijkt te zijn, is daarentegen uitermate relevant voor dit rapport.

Bij de totstandkoming van de OV-chipkaart zijn drie partijen betrokken. De OV-bedrijven zijn betrokken bij de ontwikkeling en invoering. Een tweede partij wordt gevormd door de decentrale overheden. Zij zijn verantwoordelijk voor tariefbeleid en concessieverlening. Dit laatste houdt in dat ze bepalen wie op welk traject mag vervoeren. De derde partij is de rijksoverheid. Als de 'bewaker' van de nationale kaartintegratie zorgt het Rijk voor een nette afbouw van de strippenkaart en een eenmalige financiële bijdrage. Bovendien is de rijksoverheid concessieverlener voor de Nederlandse Spoorwegen.[60]

Het plan is dat er te zijner tijd drie verschillende OV-chipkaarten gebruikt gaan worden: de persoonlijke OV-chipkaart, een anonieme OV-chipkaart en een wegwerpkaart. Afhankelijk van

---

[54] Rijswijk, Wikipedia <nl.wikipedia.org/wiki/Rijswijk>.
[55] Ir.ing. J.G.M. Steenbruggen, mw.dr.ir. K.I. van Onselen, Als elke seconde telt - Inzet van locatiegegevens bij de 112-alarmdienst, GeoNieuws 2004-4
[56] In-vehicle emergency call system "eCall" (Second eSafety Communication), SCADPlus, Europese Unie <europa.eu/scadplus/leg/en/lvb/l31103a.htm>.
[57] Aanbeveling van de Commissie betreffende de verwerking van locatie-informatie over de oproeper in elektronische communicatienetwerken met het oog op locatie-uitgebreide noodoproepdiensten, PbEU 2003, L 189/49.
[58] Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, PbEG 2002, L 201/37.
[59] Toekomst OV-chipkaart onduidelijk, Automatisering Gids, 17 januari 2008 (<www.automatiseringgids.nl>, zoek op OV-chipkaart)
[60] Zie voor meer informatie over de OV-chipkaart de website van het ministerie van Verkeer en Waterstaat, <www.verkeerenwaterstaat.nl>. Klik op Openbaar vervoer, en vervolgens op OV-chipkaart.

het reispatroon zullen reizigers een keuze gaan maken. Indien men gebruik wil maken van een abonnement of automatisch opladen, dan dient men de persoonlijke OV-chipkaart te gaan gebruiken. Indien een persoon slechts incidenteel met het openbaar vervoer gaat, dan kunnen de anonieme OV-chipkaart of de wegwerpkaart gebruikt worden. De anonieme kaart is niet op naam gesteld en kan bijvoorbeeld niet automatisch opgeladen worden. De wegwerpkaart is een OV-chipkaart met een vooraf ingestelde geldigheid, bijvoorbeeld voor een vast aantal dagen of ritten. Ook deze kaart is niet op naam gesteld en niet oplaadbaar.

De OV-chipkaart maakt gebruik van een zogenaamde RFID (Radio frequency identification)-chip.[61] RFID is een technologie die door middel van radiosignalen de unieke identificatie van producten, dieren en personen op afstand mogelijk maakt.[62] Dit betekent in het geval van de OV-chipkaart dat een reiziger zijn kaart slechts langs een lezer behoeft te halen en deze niet dus niet ergens tegenaan moet houden of ergens in moet stoppen. Deze systematiek is gekozen om de doorstroom van reizigers te bespoedigen.

Een gebruiker van de OV-chipkaart haalt deze dus bij het instappen of het betreden van een perron langs een lezer, waarmee het beginpunt van de reis geregistreerd wordt. Bij het uitstappen of het verlaten van het perron op de plaats van bestemming doet de reiziger dit opnieuw, waarna de reisafstand en de prijs berekend worden. Indien de reiziger een geldig abonnement heeft voor de betreffende afstand gebeurt er verder niets. Als deze echter met een anonieme kaart of een wegwerpkaart reist dan wordt het bedrag van het saldo op de kaart afgetrokken.

2.4.6 Burgernet

Burgernet is een telefonisch netwerk van bewoners en ondernemers in een bepaalde regio. Deze bewoners en ondernemers kunnen gebeld worden als door de politie wanneer deze een zoekactie gaat starten, naar bijvoorbeeld naar een inbreker, een verdwaald kind of een gestolen voertuig. De Burgernetdeelnemer ontvangen dan van de politiemeldkamer telefonisch een bericht om vanuit de woning of de werkplek uit te kijken naar een duidelijk omschreven persoon of voertuig. Op het moment dat u een deelnemer de gezochte persoon of het voertuig ziet, belt deze terug naar de politiemeldkamer. De politie kan dan door de meldkamer sneller naar de juiste plek gestuurd worden.

Burgernet is een dienst die te vergelijken is met sms-alert. Het verschil is dat de deelnemers op hun vaste lijn in woning of werkplek worden gebeld en niet via hun mobiele telefoon een bericht krijgen. Wat wel hetzelfde is dat op basis van de plek van het incident alleen de deelnemers in de buurt een bericht krijgen. Op basis van geografische gegevens, postcode en huisnummer, wordt een bericht verstuurd.

Veiligheid is een kerntaak van de overheid en een basisvoorwaarde voor een samenleving waarin mensen zich vertrouwd, vrij en verbonden voelen. De criminaliteit neemt de laatste jaren af. Die trend moet worden voortgezet. Het terugdringen van het aantal geweldsdelicten is echter nog onvoldoende gelukt en verdient daarom een stevige extra investering. Nederland moet nog veiliger. De overheid denkt dat Burgernet daarbij kan helpen en het is dan ook het plan dat Burgernet landelijk uitgerold gaat worden na een succesvolle proef in Nieuwegein.

Deelnemers aan Burgernet hebben het gevoel meer grip te hebben op hun eigen veiligheid. Dat verandert hun kijk op hun woon- en leefomgeving. Daarnaast komt de drempel voor burgers lager te liggen om op de politie af te stappen en stijgt hun vertrouwen in politie en gemeente, aldus een evaluatie van Burgernet in Nieuwegein.

[61] Radio frequency identification (RFID), Wikipedia <nl.wikipedia.org/wiki/RFID>.
[62] Wat is RFID?. RFID Platform Nederland, <www.rfidnederland.nl/index.php?link=RFID>.

Door de ogen en oren van de deelnemers te gebruiken, kunnen deze de politie ondersteunen bij het signaleren van gezochte personen of voertuigen.

De eerste tien minuten na een incident zijn vaak cruciaal voor opsporing. Daarom is het belangrijk dat mensen in de buurt van een incident worden ingelicht en daarmee ingeschakeld. De kans dat een bepaalde zaak wordt opgelost wordt daarmee groter.

Daarnaast denkt men het rendement van Burgernet te kunnen vergroten door het systeem niet alleen te gebruiken voor opsporing van acute zaken maar ook voor preventie.

2.4.7 GPS-toepassingen

2.4.7.1 Verlof tbs'ers

Het zich tijdens het verlof aan de begeleiding onttrekken door ter beschikking gestelden (tbs'ers) en het vervolgens niet direct kunnen opsporen van deze personen leidt tot grote commotie in de samenleving. Ter voorkoming van ontsnappingen, of in ieder geval om bij een ontsnapping tijdens verlof dan toch op zijn minst een tbs'er weer snel te kunnen opsporen, heeft men het idee opgevat tbs'ers uit te rusten met een enkelband. Mocht een tbs'er dan toch ontsnappen dan zou deze middels het door de enkelband afgegeven GPS-signaal weer eenvoudig te traceren moeten zijn.

Dit lijkt evenwel makkelijker bedacht dan succesvol toegepast. De eerste proef – in 2005 - met een elektronische enkelband mislukte jammerlijk. Technische redenen lagen hieraan ten grondslag. Zo zouden de banden te makkelijk voor de satelliet verborgen gehouden kunnen worden. Een beetje aluminiumfolie zou daartoe al afdoende zijn.[63] In Amerika bleek een en ander echter wel te werken en dus is men gaan werken aan de verbetering van de band.[64] Wat de status is van de ontwikkeling van de mogelijk verbeterde enkelband voor tbs'ers was op het moment van schrijven onduidelijk. Mogelijk dat het strengere verlofbeleid ertoe geleid heeft dat de ontwikkeling van een enkelband minder prioriteit heeft gekregen. De enkele tbs'er die nog verlof krijgt kan wellicht tegen lagere kosten dan die van een dure GPS-enkelband, intensiever begeleid worden.

Wel is duidelijk dat, bij het eventuele gebruik van enkelbanden die een GPS-signaal afgeven, geo-informatie een rol speelt, en dat het daarbij gaat om persoonsgegevens. De gegevens die worden verzonden via de enkelband wijzen immers naar een bepaalde tbs'er die met naam en toenaam bekend is.

2.4.7.2 Noodhulpfunctie ouderen middels GPS

Met veel moderne mobiele telefoons, zo niet met alle, kan men meer dan alleen bellen en gebeld worden. Zij bevatten vaak een veelvoud aan functies: een e-mailprogramma, een agenda, navigatie, spelletjes, etc.

Als gevolg van deze vele functies hebben ouderen vaak moeite om van dergelijke toestellen gebruik te maken. Dit heeft tot gevolg dat een steeds groter wordende groep mensen, steeds moeilijker met het mobieltje kan omgaan. En dat terwijl ze, als de gezondheid dat toelaat, alle tijd hebben om mobiel te zijn. Het is dan ook niet vreemd dat er speciale telefoons voor oudere

[63] Proef met enkelband tbs'ers mislukt, Planet.nl, 8 december 2005 (<www.google.nl> zoek naar *tbs enkelband*).
[64] 'Nieuwe enkelband tbs'ers, meer geld Amsterdam', Elsevier, 2 januari 2007 (<www.elsevier.nl> zoeken naar *enkelband*).

mensen zijn ontwikkeld.[65] Telefoons die vooral veel minder functies hebben, en eigenlijk zo goed als alleen dat doen waar telefoons oorspronkelijk voor gemaakt zijn, te weten bellen.

Behalve de belfunctie hebben de seniorentelefoons vaak tevens een simpel en vaak groter toetsenbord zodat een oudere bijvoorbeeld in geval van nood toch nog in staat is te bellen. Er zijn zelfs toestellen met een alarmknop waarop gedrukt kan worden als men snel hulp nodig heeft. Als een oudere deze knop gebruikt, wordt vervolgens contact gemaakt met een medisch gespecialiseerd callcenter en kan de oudere, mits daartoe in staat, met raad worden bijgestaan.

Gezien het feit dat een oudere natuurlijk niet altijd in staat zal zijn het call center te woord te staan, of omdat na overleg het call center het wellicht nodig acht hulpdiensten in te schakelen is er soms nog een GPS-functie (met zender) aan de telefoon toegevoegd. Middels deze functie kan bepaald worden waar een oudere zich bevindt en zodat hulpdiensten naar de betreffende plek gestuurd kunnen worden. [66]

In geval van opsporing van een oudere is het niet anders dan met een tbs'er, er is geo-informatie in het geding en die informatie is te herleiden tot een persoon. Het laatste zal in de nabije toekomst zelfs wel eens heel belangrijk kunnen worden bij het redden van levens of het voorkomen van (meer) letsel. Als de persoonsgegevens bekend zijn, kunnen deze immers gekoppeld worden aan een medisch dossier dat al ingezien is door de uitrukkende hulpdiensten voordat zij ter plekke zijn om hulp te verlenen.

2.4.7.3 GPS-locator tegen diefstal goederen

Tegenwoordig zijn veel voertuigen standaard uitgerust met een navigatiesysteem. Het systeem kan met behulp van GPS de bestuurder van een voertuig helpen zijn weg te vinden. Hiertoe is (slechts) een GPS-ontvanger nodig. Het voertuig kan niet gevolgd worden.

Indien echter een voertuig beschikt over een GPS-zender dan is het wel mogelijk het voertuig te volgen. In geval van diefstal is het voertuig dan op een eenvoudige wijze te traceren.[67] [68]

Vooralsnog kan een eigenaar ervoor kiezen om zijn voertuig met een GPS-zender uit te rusten. Deze zender wordt op een verborgen plaats gemonteerd zodat in geval van diefstal het voertuig weer gevonden kan worden. Er gaan echter ook stemmen op om een GPS-zender te verplichten voor auto´s boven een zeker bedrag.[69]

Vanzelfsprekend speelt geo-informatie een rol bij dit soort GPS-systemen. Zonder locatie-gegevens zal een voertuig niet (eenvoudig) gevonden kunnen worden. Juridische aspecten lijken minder relevant. Persoonsgegevens hoeven geen rol te spelen. Het gaat om de locatie van een gestolen voertuig. Van wie het voertuig is, is voor de zoektocht niet relevant. Uiteraard wel voor het terug bezorgen.

2.4.7.4 Personeelsvolgsystemen

---

[65] Website GSMvoorSenioren.nl, <www.gsmvoorsenioren.nl>.
[66] Zie bijvoorbeeld de Secufone, </www.secufone.nl/>.
[67] Gestolen auto's op te sporen met gps, Elsevier, 5 april 2007 en Gestolen auto na kwartier terug door GPS-techniek, www.blikopnieuws.nl, 5 februari 2008 (<www.google.nl> zoeken naar *gestolen auto´s gps).*
[68] GPS Guard en Boat Guard, Security webshop (<www.securitywebshop.nl> zoeken naar *GPS Guard*).
[69] Steeds meer nieuwere auto´s gestolen, Elsevier, 14 juli 2006 (<www.elsevier.nl> zoeken naar *nieuwere auto´s).*

Personeelsvolgsystemen – ook personeelsinformatiesystemen genoemd – kunnen worden gedefinieerd als "een doorgaans geautomatiseerd systeem waarin individuele en geaggregeerde gegevens van en over werknemers worden vastgelegd en dat als doel heeft 1) het ondersteunen van beslissingen ten aanzien van individuele werknemers en/of 2) het verschaffen van informatie met het oog op het voeren van een doelmatig en efficiënt personeelsbeleid en personeelsmanagement.[70]

Een voorbeeld van een dergelijk systeem is een zogenaamd voertuigvolgsysteem. In dit soort systemen kunnen de mogelijkheden van GPS, mobiele telefonie en het internet, gecombineerd worden waardoor een werkgever kan volgen waar zijn voertuigen zijn en/of waren. Vanzelfsprekend wordt bij dit soort toepassingen geo-informatie verwerkt. Het doel van dergelijke systemen is immers onder meer een werknemer, op basis van de locatie waar hij zich bevindt, naar een volgende werkplek te kunnen sturen.

Een ander soort volgsysteem dat in de toekomst wellicht gebruikt zou kunnen gaan worden is een systeem dat gebruik makend van radio frequency identification (RFID) werknemers binnen een gebouw volgt.[71] Het betreft hier dan als het ware lokale geo-informatie.

RFID is in dergelijke gevallen een technologie die gebruikt wordt in een personeelsvolgsysteem, dat verglijkbaar is met het gebruik van bewakingscamera´s in een gebouw. Het gebruik van RFID-technologie binnen een personeelsvolgsysteem vergemakkelijkt veelal het verzamelen en verwerken van gegevens over de werknemers. Het gebruik van RFID brengt daarmee een kwantitatief en – vanuit de optiek van de werkgever bezien ook - een kwalitatief verschil met zich mee ten opzichte van bewaking met camera´s. Zo kunnen met behulp van wat men noemt ‘active badge monitoring’ door middel van elektronische ogen (RFID-readers) en badges werknemers door het hele gebouw worden gevolgd en kunnen dus de tijdstippen waarop de werknemer een bepaalde reader passeert direct worden opgeslagen in een achterliggende database.[72]

2.5 Geografische informatie systemen (GIS)

2.5.3 Google Maps / Google Earth en geografische overheidsdiensten

Google Maps is een service van Google die kaarttechnologie combineert met bedrijfsinformatie, zoals locatieaanduidingen, contactgegevens en routebeschrijvingen. Google Earth combineert satellietbeelden, kaarten, terreingegevens en 3D-gebouwen met de zoektechnologie van Google om geografische gegevens van de hele wereld binnen handbereik te brengen.[73]

Google Earth is een vrij te downloaden applicatie van Google Inc. waarmee men vrijwel elke plek op de wereld kan opzoeken met behulp van satellietfoto's en luchtfoto's. Tegen betaling kan een GPS of GIS aan het programma worden gekoppeld. De data die Google Earth gebruikt, zijn dezelfde als die Google Maps gebruikt, Google Earth heeft echter meer mogelijkheden.[74]

Naast particulieren en het bedrijfsleven maken steeds meer overheidsdiensten gebruik van de mogelijkheden die Google aanbiedt. Zo gebruikt de gemeente Amsterdam, stadsdeel

---

[70] Personeelsinformatiesystemen en privacybescherming, Drs. J.H.J. Terstegge <home.planet.nl/~privacy1/pis2107.htm>.
[71] Radio frequency identification, Wikipedia, <nl.wikipedia.org/wiki/RFID>.
[72] Werknemers en RFID, Jessica Verwer. In: Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen, NVvIR, 2005, <www.nvvir.nl/doc/rfid-tekst.pdf>.
[73] Website Google Maps <maps.google.nl>.
[74] Website Google Earth <earth.google.nl>.

Geuzenveld-Slotermeer Google Maps om klachten van burgers weer te geven.[75] De gemeente Nijmegen gebruikt dit systeem om de verschillende aanvragen voor bouwvergunningen in de gemeente weer te geven.[76] Zo zijn er nog meerdere overheden en publieke onderdelen die van deze dienst gebruik maken.[77] Gegevens van verschillende aard worden middels een geografische weergave van een gebied met elkaar gecombineerd. Deze diensten zijn in die zin dus anders dan de eerder besproken locatiegebonden systemen, dat het niet gaat om (locatie)gegevens betreffende bewegende subjecten of objecten, maar om (verschillende lagen van) gegevens over zich op het aardoppervlak bevindende objecten. Daar waar de eerste informatie vaak dynamisch is en niet altijd in de vorm van kaartgegevens wordt weergegeven, is de informatie in geo-informatiesystemen statisch(er) en is er in veel gevallen sprake van weergave in kaartvorm. Dit betekent overigens dat privacy geen rol zou kunnen spelen, zoals hieronder wordt toegelicht.

2.6 Privacy en de beschreven toepassingen

2.6.1 Inleiding

In het voorgaande zijn de privacyregels en -gedaanten besproken, evenals een aantal toepassingen; locatiegebonden diensten en geografische informatiesystemen. Nu worden de toepassingen bezien in het licht van de regels en gedaanten .

2.6.2 Sms-alert

De sms-alert zoals deze bijvoorbeeld door verschillende politiediensten wordt gebruikt, is een dienst waarvoor gebruikers zich vrijwillig aanmelden. Daarbij verstrekt de aanmelder niet meer gegevens dan het mobiele nummer, postcode en huisnummer. De geo-informatie die bij sms-alert dus een rol speelt zijn de (statische) adresgegevens van een aanmelder. Natuurlijk heeft men een mobiel telefoonnummer nodig om berichten te kunnen versturen naar de aangemelde personen, maar waar deze personen zich bevinden op het moment dat het bericht verstuurd wordt, is niet relevant. Zo kan iemand die de dienst niet tijdelijk op pauze zet als hij op vakantie gaat, een sms-alert ontvangen terwijl hij bijvoorbeeld in Italië zit.
De (dynamische) geo-informatie die bekend is/wordt door het gebruik van de mobiele telefoon is voor sms-alert niet relevant.

Recht om met rust gelaten te worden
Met de aanmelding voor een sms-alert-dienst van de politie levert iemand iets in van zijn privacy. Het geeft als het ware aan dat de politie zijn rust mag verstoren als er iets gebeurt in de buurt van zijn woonadres, waarvan de politie het nodig vindt dat hij daarvan op de hoogte wordt gebracht. Dat kan iets betreffen waarbij de politie assistentie nodig heeft, of het kan een bericht zijn ter voorkoming van een misdrijf. In het eerste geval kan men denken aan het zoeken naar een vermiste burger, in het tweede aan bijvoorbeeld een waarschuwing dat er in de buurt iemand gesignaleerd is die middels een babbeltruc mensen probeert op te lichten.

Het is in dergelijke gevallen de burger die van zijn zelfbeschikkingsrecht gebruik maakt en er daarbij dus voor kiest iets van zijn privacy in te leveren. Het ontvangen van een sms-bericht in het kader van de dienst waar men zich voor opgegeven heeft, is dus overduidelijk geen inbreuk op de privacy van de aanmelder.

---

[75] In Google Maps kan men klikken op de ballonnetjes met een M om informatie meldingen te krijgen. Zie: <mor.amsterdam.asp4all.nl/MORGeuzenveld.aspx>.
[76] Procedures Online, overzicht van lopende procedures in uw buurt, Gemeente Nijmegen, <www5.nijmegen.nl/voifrontend>.
[77] Zie bijvoorbeeld het filmpje Brandweer 100% mobiel, Google <video.google.com/videoplay?docid=-3595427297132990648>

Persoonsgegevens of politiegegevens
Iets anders betreft de gegevens van de personen (abonnees) die zich hebben aangemeld. Deze abonnees overleggen het nummer van hun mobiele telefoon, de postcode en het huisnummer. Zijn dit nu persoonsgegevens of politiegegevens? Ofwel zijn het gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 1 WBP), of zijn het gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon die in het kader van de uitoefening van de politietaak worden verwerkt (artikel 1 Wpolg). En is dus de Wet bescherming persoonsgegevens van toepassing of de Wet politiegegevens?

Volgens de (voormalige) Registratiekamer vormen combinaties van postcode en huisnummer samen persoonsgegevens.[78] Het betreft immers gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Vraag is nu of de persoonsgegevens van personen die zich hebben aangemeld voor een alert worden verwerkt in het kader van een politietaak.

Er is iets te zeggen voor een positief antwoord op deze vraag. Ook binnen de politiewereld gaat men daar van uit.[79] Bestudering van de Wet politiegegevens en de bijbehorende memorie van toelichting maakt evenwel duidelijk dat de wet niet is geschreven voor iets als de verkrijging van gegevens bij een politietaak.

In de memorie van toelichting staat onder meer:

'Bij de uitvoering van de dagelijkse politietaak komt de politie in contact met veel burgers ter zake van zeer diverse gebeurtenissen. Het gaat bijvoorbeeld om burgers die zich om hulp tot de politie wenden, betrokken zijn bij verstoringen van de openbare orde, meldingen van overlast doen, aangifte doen of slachtoffer, getuige of verdachte zijn van een strafbaar feit.[80]

Een burger komt dus naar aanleiding van een gebeurtenis in aanraking met de politie en op grond daarvan worden gegevens verwerkt. In het geval van aanmelding voor een sms-alert is er geen gebeurtenis, maar geeft men vrijwillig aan bereid te zijn de politie te helpen en/of dat men op de hoogte gehouden wil worden van bepaalde zaken die zich in de woonomgeving afspelen. Als er vervolgens een gebeurtenis plaatsvindt, dan worden de gegevens verwerkt en wordt een nader bepaalde aangemelde burgers om assistentie gevraagd of gewaarschuwd, maar dat is een fase verder. De gegevens van de deelnemers aan de alert staan daartoe klaar.

Volgens deze redenering vindt de verkrijging van de gegevens dus niet plaats in het kader van de politietaak, die volgens art.2 van de Politiewet zowel de daadwerkelijke handhaving van de rechtsorde betreft als het verlenen van hulp aan hen die deze behoeven. Er is bij verkrijging nog geen sprake van een concrete taak waarbij gegevens ingezet en verwerkt gaan worden.

Hierbij komt dat de Wpolg geen betrekking heeft op de *verkrijging* van politiegegevens.[81] De wet geeft regels voor de *verwerking* van persoonsgegevens die in het kader van de uitvoering van de politietaak zijn verkregen. Hoe gegevens verkregen zijn, stoelt op een andere basis; in het geval van sms-alert op vrijwilligheid. Dus de gegevens van de vrijwillig bij een alert aangesloten personen worden politiegegevens op het moment van verwerking voor het inzetten bij een alert. Het *verkrijgen* van de gegevens van de betreffende persoon valt niet onder de Wpolg.

Los van het bovenstaande zou het ook niet echt praktisch zijn als de verkrijging van abonnee-gegevens voor sms-alert onder de Wpolg zou vallen. Politiegegevens dienen namelijk uiterlijk 5 jaar na de eerste verwerking verwijderd te worden uit de politiebestanden, aldus artikel 8 lid 6 Wpolg. Bovendien zijn politiegegevens een jaar na de eerste verwerking al niet meer vrij

[78] Registratiekamer 21 juni 1996, 95.O.043
[79] Zoals blijkt uit de notitie 'SMS-Alert en de privacywetgeving', van Vts-Politie Nederland.
[80] *Kamerstukken II* 2005-2006, 30327, nr. 3, p. 10.
[81] *Kamerstukken II* 2005-2006, 30327, nr. 3, p. 25.

toegankelijk (artikel 8 lid 1 Wpolg). Ze verdwijnen dan 'achter een schot' aldus de memorie van toelichting.

Moeten dan jaarlijks of vijfjaarlijks de abonneegegevens opnieuw toegestuurd worden door de personen die zich vrijwillig hebben aangemeld, omdat de politie hun gegevens anders niet meer (zomaar) kan inzetten? De vraag is bovendien of het dan wel weer mag, want het zijn immers dezelfde persoonsgegevens die dan weer ingezet worden.

Is dan het regime van de WBP van toepassing op de (vrijwillige) *verkrijging* van gegevens in het kader van een sms-alert? De vraag die dan aan de orde dient te komen is of er sprake is van een verwerking van die gegevens in het kader van WBP. De WBP beschrijft de verwerking van persoonsgegevens als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Volgens de memorie van toelichting bij de WBP is het verkrijgen van gegevens een vorm van verwerken van gegevens. Dit betekent naar onze mening dat het verkrijgen van gegevens van personen die zich vrijwillig aanmelden voor sms-alert een verwerking is in de zin van de WBP.

Dit brengt de volgende interessante vraag naar voren: is de verwerking van de gegevens van personen die zich hebben aangemeld voor sms-alerts bij de verschillende korpsen volgens de regels van de Wet bescherming persoonsgegevens aangemeld bij het CBP (artikel 27 e.v. WBP)? Raadpleging van het openbare meldingenregister en navraag bij de korpsen heeft geleerd dat het niet geval is.

Er dient dus onderscheid gemaakt te worden tussen de verkrijging van de gegevens door de politie en de verwerking van de gegevens bij een politietaak. Op het eerste is de WBP van toepassing, op het tweede de Wpolg.

Los van de kwestie of de WBP, de Wpolg of beiden een rol spelen bij sms-alert, is het niet voor iedereen duidelijk wat er nu precies gebeurt met de gegevens van de personen die zich hebben aangemeld bij een alert-dienst. Zo blijkt bijvoorbeeld het mobiele nummer niet te worden doorgegeven aan een telecomprovider ter versturing van een sms-alert, maar voert de politie de verzending van de sms zelf uit via de gemeenschappelijke meldkamer. Minder duidelijk is of de gegevens bij opzegging onmiddellijk worden verwijderd? En hoe zit dat met gegevens die zijn ingezet bij een alert en als gevolg daarvan onder het regime van de Wpolg vallen?

Daarnaast is er sprake van dat de politie behalve 06-nummer, postcode en huisnummer andere gegevens, zoals het bezit van een hond, zou willen gaan opslaan van de personen die mee doen aan de alert. Is het dan zo dat de politie in het geval van een incident met een persoon en een hond in een bepaalde buurt, even de databank van de alert raadpleegt om snel te bekijken wie mogelijk bij het incident betrokken zou kunnen zijn? Een dergelijk gebruik is vanzelfsprekend onverenigbaar met het doel waarvoor de gegevens zijn verkregen en schaadt dit het vertrouwen van de burger. Ter bevordering van de transparantie is het dan ook het overwegen waard het proces van opslag en verwerking van de gegevens, en wat er wel en niet mee gedaan zal worden op te nemen in een gedragscode. Het zou duidelijkheid verschaffen en vertrouwen in alert-diensten doen toenemen.

2.6.3 Groeps-sms

Het is denkbaar dat een groeps-sms ingezet kan worden voor verschillende doeleinden door verschillende (overheids)organisaties. Kwestie die daarbij vooral aandacht behoeft, is hoe men aan de mobiele telefoonnummers komt, en wat de status van die nummers – die gegevens - is.

Tot op heden is deze dienst vooral ingezet door de politie bij enkele zeer ernstige incidenten. Zo heeft de politie bij enkele moordzaken het middel ingezet omdat men op een dood spoor leek te zitten. Wat men vervolgens gedaan heeft, is de gegevens opvragen van gebruikers van mobiele telefoons die ten tijde van de moord in de buurt waren. Vervolgens heeft men deze personen een bericht gestuurd met bijvoorbeeld de vraag om naar Opsporing verzocht te kijken en tips door te geven aan de politie.

Recht om met rust gelaten te worden
Eerder genoemde praktijkvoorbeelden geven aan dat iemand die in het bezit van een mobiele telefoon in de buurt is geweest van een ernstig incident de kans loopt dat hij een sms-bericht ontvangt van de politie. Uiteraard moet de mobiele telefoon dan wel aangestaan hebben. Als dat niet het geval is, zend de telefoon immers geen signaal uit.

De ontvangst van het bericht, verstuurd in het kader van een groeps-sms, verstoort overduidelijk de rust. Gezien het feit dat het middel (vooralsnog) slechts wordt ingezet bij ernstige incidenten, zou dat echter tot de overweging kunnen leiden dat die toch wel minimale verstoring van de rust, niet opweegt tegen het belang van de opsporing van de dader(s) en het om die reden is toegestaan.

In dit kader is het van belang te weten dat artikel 10 van onze Grondwet in lid 2 vermeldt dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. En om iemand een bericht te kunnen sturen die in de buurt is geweest van een ernstig incident heeft de politie een persoonsgegeven nodig: het nummer van de mobiele telefoon.[82] Vraag is nu of er wetgeving is die het toestaat in bepaalde gevallen persoonsgegevens op te vragen en de rust van een persoon te verstoren. Hieronder wordt daar nader op ingegaan.

Persoonsgegevens
Als gezegd, heeft de politie de nummers nodig van de mobiele telefoons van de personen die in de buurt waren van een ernstig incident om deze te kunnen benaderen. Eerder werd reeds opgemerkt dat het CBP reeds in 1993 heeft gesteld dat telefoonnummers (bijna altijd) persoonsgegevens zijn. Daar kunnen we nog een CBP-onderzoek van recenter datum aan toevoegen waarin het college stelt dat een telefoonnummer een persoonsgegeven is omdat het onder meer bedoeld is als middel tot toegang en als middel tot identificatie van gebruikers. Als een nummer zonder onevenredige inspanning kan leiden tot identificatie van een persoon, wordt dit nummer als een persoonsgegeven beschouwd, aldus het CBP. Waarna zij vervolgt dat bij telefoonnummers gevorderd door opsporende instanties waarbij er nog geen naw-gegevens zijn opgevraagd, sprake is van persoonsgegevens omdat het voor opsporende instanties relatief weinig inspanning kost de bijbehorende naw-gegevens alsnog te achterhalen.[83]

Vraag is nu op basis van welke regels opsporende instanties telefoonnummers – en dus persoonsgegevens – mogen opvragen, om vervolgens met behulp van die telefoonnummers de rust te verstoren van de personen die in de buurt waren van een ernstig incident. De wet die deze mogelijkheid schept is het Wetboek van Strafvordering. Sinds september 2004 is dit wetboek aangepast waardoor nauwkeurig bepaald kan worden welke *telecommunicatieverkeersgegevens* van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst (telefoon, fax, internet en e-mailverkeer) gevorderd kunnen worden.[84] Met deze wet zijn naast de verkeersgegevens, gegevens over de gevoerde of nog te voeren communicatie, de zogenaamde *gebruikersgegevens* (naam, adres, postcode, woonplaats, nummer en soort dienst waarvan

[82] Registratiekamer 8 juli 1993, 93.A.002
[83] Onderzoek fotopublicaties op internet, CBP, 23 februari 2006, <www.cbpweb.nl/downloads_uit/z2005-0844.pdf>.
[84] Eerste Kamer stemt in met wetsvoorstel Vorderen gegevens telecommunicatie, 17 maart 2004, <www.recht.nl/16884>.

personen gebruikmaken) geïntroduceerd als gegevens die ten behoeve van de strafvordering en door de inlichtingen- en veiligheidsdiensten kunnen worden opgevraagd.

Biedt deze wet nu de mogelijkheid aan de politie om in een geval als dat van Louis Sévèke de telefoonnummers op te vragen van de personen die ten tijde van de moord in de buurt waren? Nummers dus van personen die (nog) niet als verdachte zijn aangemerkt zijn, maar die slechts in de buurt waren en de politie dus mogelijk van nuttige informatie zouden kunnen voorzien?

Artikel 126na van het Wetboek van Strafvordering (Sv) stelt dat in geval van verdenking van een misdrijf een opsporingsambtenaar in het belang van het onderzoek een vordering kan doen gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst.
Moeten we uit dit artikel nu opmaken dat alle personen die ge-sms't zijn na de moord op Sévèke, maar ook na de voetbalrellen en de moord op Anneke van der Stap - zo'n 50.000 in totaal – verdacht waren van een misdrijf? Of was dat wellicht helemaal niet noodzakelijk om de gegevens te mogen opvragen?

Artikel 126na Sv spreekt weliswaar over verdenking van een misdrijf. Er staat niet met zoveel woorden dat de verdenking moet slaan op een verdachte gebruiker. Degene wiens gegevens in het kader van artikel 126na Sv afgetapt mogen worden lijkt dus niet dezelfde te hoeven zijn als de verdachte. De memorie van toelichting beaamt dit ook. Daarin staat dat de bevoegdheid tot het vorderen van telecommunicatiegegevens door de Wet vorderen gegevens telecommunicatie in vijf opzichten wordt gewijzigd. Een van deze opzichten betreft de eis dat de vordering alleen betrekking kan hebben op gegevens betreffende de verdachte. Deze eis is door deze wet komen te vervallen. De memorie van toelichting stelt daarover dat in het geval van het vorderen van gegevens toepassing jegens andere personen dan de verdachte kan bijdragen aan de opsporing. Het kan bijvoorbeeld nodig zijn na te gaan met welke personen een slachtoffer van een misdrijf contacten heeft gehad vlak voordat het misdrijf werd gepleegd. Op die manier kan men op het spoor van de verdachte komen. Dit kan er dan weer aan bijdragen dat weloverwogen kan worden besloten tot het op een selectieve en effectieve wijze aftappen van telecommunicatie, aldus de memorie van toelichting.[85]

Het feit dat er een misdrijf heeft plaatsgevonden kan er dus toe leiden dat telecommunicatiegegevens opgevraagd worden van gebruikers niet zijnde de verdachte. De hierboven staande argumentatie waarom dat moet kunnen, lijkt echter wel aan te geven dat de personen wiens gegevens gevorderd worden dicht bij de daad, dicht bij het slachtoffer moeten staan.
Dit is ook in overeenstemming met het vereiste dat de toepassing van de bevoegdheid tot het vorderen van verkeersgegevens dient plaats te vinden 'in het belang van het onderzoek`. Temeer daar het een bevoegdheid betreft tot het vorderen van gegevens van derden die door particulieren voor specifieke doeleinden zijn vergaard en die dan dus aangewend gaan worden voor andere doeleinden. Een goede afweging van enerzijds het belang dat zorgvuldig wordt omgegaan met persoonsgegevens en anderzijds het opsporingsbelang is dan ook vereist.[86]
Daarbij speelt onder meer een rol dat de bevoegdheid inzake gebruikersgegevens betrekking heeft op een beperkte categorie gegevens: naam, adres, woonplaats, nummer en soort dienst. De memorie van toelichting stelt hierover dat het vorderen van de gebruikersgegevens niet leidt tot een min of meer volledig beeld van bepaalde aspecten van iemands leven. Met andere woorden aan het vorderen van dit soort (persoons)gegevens moet niet zo zwaar getild worden.

Gezien het feit echter dat er sprake is van gegevens die voor een ander doel worden gebruikt dan waartoe ze aangewend zijn, dient er wel een toetsing plaats te vinden met het oog op de omgang met persoonsgegevens in relatie tot het opsporingsbelang.

[85] *Kamerstukken II* 2001-2002, 28059, nr. 3, p. 9.
[86] *Kamerstukken II* 2001-2002, 28059, nr. 3, p. 3-6.

In dit kader wordt in de memorie van toelichting verwezen naar het Databeschermingsverdrag van de Raad van Europa.[87] Artikel 9 van het verdrag bepaalt namelijk dat doelafwijkend gebruik mogelijk is, indien dit bij wet is voorzien en noodzakelijk is in een democratische samenleving in het belang van het bestrijden van strafbare feiten. Er dient dus voldaan te worden aan het noodzakelijkheidscriterium. Bovendien dient de vergaring van gegevens rechtmatig te zijn en dient zij niet bovenmatig te zijn.

Over het noodzakelijkheidscriterium in relatie tot het vorderen van gebruikersgegevens wordt vervolgens in de memorie van toelichting gesteld dat dit soort gegevens een opsporingsambtenaar in staat stelt te weten met welke persoon hij te maken heeft, als hij een bepaald nummer of adres heeft, dan wel welk nummer een bepaalde persoon heeft. Dit zou een onmisbaar onderdeel van veel strafrechtelijke onderzoeken zijn. Men heeft dan namelijk bij de start van een onderzoek kennis van enkele feiten en personen en men kan door het vergaren van aanvullende gegevens verbanden leggen. Daarnaast zijn de gebruikersgegevens ook nodig alvorens andere bevoegdheden kunnen worden toegepast, bijvoorbeeld de bevoegdheid tot het vorderen van verkeersgegevens en de bevoegdheid tot het opnemen van telecommunicatie. Deze bevoegdheden kunnen namelijk pas worden toegepast wanneer de gebruiker in samenhang met het nummer van telecommunicatie kan worden geïdentificeerd. Het belang dat de opsporingsinstanties bij deze categorie gegevens hebben is dus groot. Er wordt daarom voldaan aan het noodzakelijkheidscriterium, aldus de memorie van toelichting.

Men kan zich nu afvragen of hetgeen in de memorie van toelichting gesteld wordt, geschreven is met een toepassing als groeps-sms in het achterhoofd. Het lijkt veel meer te wijzen op een beperkte kring rond een verdachte of een slachtoffer, maar niet op willekeurige passanten. Terughoudendheid zou daarom in acht genomen moet worden bij het inzetten van het middel van de groeps-sms en de daaraan gekoppelde eis daarvoor eerst gebruikersgegevens te moeten opvragen. Het dient niet te pas en te onpas ingezet te worden. Het opsporingsbelang dient het niet altijd zomaar te winnen van het privacybelang. Met andere woorden de eisen van subsidiariteit en proportionaliteit zijn van groot belang bij de afweging tot het vorderen van gebruikersgegevens over te gaan. Overigens wijst het aantal keren dat groeps-sms is ingezet erop dat de opsporingsautoriteiten daarbij zorgvuldig te werk gaan.

Mocht men na zorgvuldige overweging hebben besloten gebruikersgegevens op te vragen en te gebruiken voor een groeps-sms, dan zijn dit gegevens die worden verwerkt in het kader van de uitoefening van een politietaak en zijn het dus politiegegevens in het kader van de Wet politiegegevens. Gegevens die in die gevallen dus ingevolge artikel 8 van Wpolg gedurende een periode van één jaar na de datum van de eerste verwerking verwerkt mogen worden en die uiterlijk vijf jaar na de datum van eerste verwerking verwijderd worden. Het feit dat deze gegevens dus nog aan nadere verwerking onderworpen kunnen worden en vijf jaar lang bewaard mogen blijven, zijn redenen te meer zorgvuldig met het middel van groeps-sms om te gaan, daar waar het willekeurige passanten betreft.

Het laatste lijkt ons een reden om *ook* voor de groeps-sms een gedragscode op te stellen.

2.6.4 Sms-bom

Indien een mobiele telefoon is gestolen en daarvan is aangifte gedaan, dan kan de politie de sms-bom inzetten om het gebruik van de telefoon onaangenaam te maken. Met de sms-bom hoopt de politie dat het stelen van een mobiele telefoon onaantrekkelijk wordt gemaakt.

[87] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. CETS No.: 108. Tractatenblad 1988, 7 of zie <conventions.coe.int>, klik op *Full list* en zoek verdrag 108.

De sms-bom schijnt overigens nauwelijks nog te worden ingezet. Wellicht heeft dat te maken met het feit dat mobiele telefoons in veel gevallen zo goed als gratis bij een abonnement worden verstrekt en het daarom geen inzet van veel politiemiddelen waard is.

Bij het gebruik van de sms-bom speelt geo-informatie eigenlijk geen rol. Men gebruikt slechts het IMEI (International Mobile Equipment Identity)-nummer, een unieke cijfercombinatie die op iedere mobiele telefoon opgeslagen, om berichten naar de gestolen telefoon te sturen. Waar die telefoon, of de gebruiker ervan, zich op dat moment bevindt, is niet relevant. Men kan zich evenwel bedenken dat geo-informatie wel een rol zou kunnen spelen, omdat de locatiebepaling van mobiele telefoons steeds nauwkeuriger wordt en de politie het gebruik van een gestolen telefoon niet alleen kan verstoren, maar deze tevens makkelijk kan opsporen. Ook hierbij kan men zich evenwel afvragen of de inzet van dergelijke politiemiddelen voor de steeds goedkoper wordende mobiele telefoons wel proportioneel is.

Recht om met rust gelaten te worden
Indien de sms-bom toch wordt ingezet, wordt de rust van de dief van de mobiele telefoon absoluut verstoord. Dat geldt uiteraard ook voor de rust van de heler indien de dief de telefoon zou hebben doorverkocht. In het geval dief en/of heler is deze verstoring volstrekt legitiem. Het privacybelang legt het in deze af tegen de handhaving van de rechtsorde, waarbij die handhaving in dit geval met name gericht is op preventie. Geen dief of heler zal naar de rechter gaan om te klagen dat zijn privacy wordt aangetast door een sms-bom, maar mocht het al wel gebeuren dan zal een rechter een dergelijk middel absoluut proportioneel vinden. Het is een minimale inbreuk die de dief of heler er bovendien continu op wijst dat hetgeen hij gedaan heeft in strijd is met het geldende recht.

Persoonsgegevens
In het geval van een sms-bom is er geen sprake van persoonsgegevens in het kader van de WBP of politiegegevens in het kader van de Wpolg. De politie heeft slechts een IMEI-nummer nodig om een sms-bom te kunnen inzetten.

2.6.5 Cell broadcast

Een op sms gelijkende techniek is die van cell broadcast. Deze techniek zou bijvoorbeeld kunnen worden ingezet bij burgeralamering, zeker als daarbij bedacht wordt dat deze dienst goed inzetbaar is als bij bijvoorbeeld overbelasting van het mobiele netwerk er geen mobiel telefoonverkeer mogelijk is.

Het is een techniek waarbij geo-informatie in zoverre een rol speelt, dat personen die zich in een bepaalde cell bevinden en cell broadcast op hun mobiele telefoon hebben geactiveerd via cell broadcast geïnformeerd kunnen worden over bijvoorbeeld een zich in hun buurt afspelende ramp.

Recht om met rust gelaten te worden
Het versturen van een bericht via cell broadcast heeft evenals het Waarschuwings Alarmerings Systeem (WAS) - het bekende sirenestelsel dat naar alle waarschijnlijkheid rond 2015 zal worden afgeschaft – als doel burgers te alarmeren in geval van calamiteiten.[88] De sirenes gaan straks ook loeien in de mobieltjes zoals soms al enigszins gekscherend wordt gezegd. Dat dat zal gebeuren zal overigens niemand als storend ervaren. Men zal graag de rust laten verstoren door de overheid die de burgers wil waarschuwen voor een zeker gevaar.

Persoonsgegevens
Persoonsgegevens spelen geen rol bij cell broadcast. Via cell broadcast wordt in geval van burgeralarmering een bericht gestuurd naar een of meer cellen in de buurt van het gevaar. Welke

[88] Antwoorden op kamervragen over cell broadcast voor burgeralarmering, ministerie van BZK, 25 juni 2007 (<www.minbzk.nl> zoeken naar *cell broadcast*)

personen zich in die cel of cellen bevinden is volstrekt onbekend. Voor de verzending van een bericht worden geen persoonsgegevens verwerkt.

2.6.6 Kilometerprijs

Als het aan het kabinet Balkende IV ligt gaan in 2011 de eerste vrachtwagens rijden volgens het principe van de kilometerprijs. Uiteindelijk moeten alle auto´s in 2016 volgens het systeem van kilometerprijs over de weg bewegen.

Op het moment van het schrijven van dit stuk is nog niet bekend welke techniek ten grondslag zal komen te liggen aan het systeem van kilometerprijs. Wel bestaat er een grote kans dat auto´s uitgerust gaan worden met wat men noemt een OBU, een on board unit. Deze unit, een kleine computer, zal gebruikt worden om de prijs van het weggebruik te berekenen. De OBU communiceert vervolgens met andere apparatuur, waardoor de automobilist uiteindelijk een rekening toegestuurd krijgt voor het gebruik van de weg. Afhankelijk van de inhoud van de diverse gegevensstromen zal hierbij de privacy in het geding zijn, waarover hieronder meer.

Dat geo-informatie een rol speelt bij kilometerprijs is evident. De prijs kan immers niet berekend worden als niet bekend is, over welke wegen wanneer is gereden met wat voor soort voertuig.

Recht om met rust gelaten te worden
Het feit dat elke auto wellicht op een zeker moment een OBU heeft, hoeft nog geen gevolgen te hebben voor de privacy. Anders wordt het ingeval de OBU ook de mogelijkheid schept dat men in de auto bepaalde berichten zou kunnen ontvangen die gerelateerd zijn aan het weggebruik. Op zich is dat niet ondenkbaar want het idee is de OBU en de installatie daarvan te bekostigen door ook de mogelijkheid te creëren zogenaamde toegevoegde waardediensten aan te laten bieden via de OBU. Dit zou kunnen betekenen dat commerciële partijen automobilisten zouden kunnen benaderen met diensten als zij zich in hun auto over het wegennet voortbewegen.

Deze diensten kunnen natuurlijk nuttig zijn, maar het dient wel zo te zijn dat deze dienstenaanbieders pas hun informatie naar een auto mogen sturen, indien de bestuurder via de OBU heeft aangegeven heeft dat hij daar prijs op stelt; opt-in. Het dient toch vooral voorkomen te worden dat burgers in de auto ook al gespamd gaan worden. Artikel 11.7 van de Telecommunicatiewet staat daaraan ook in de weg. Ook in een auto met OBU heeft men dus het recht om met rust gelaten te worden.

Persoonsgegevens
Dat er persoonsgegevens in het geding zijn bij de kilometerprijs lijkt duidelijk. De prijs wordt berekend op basis van de gereden kilometers, waarna deze gegevens doorgestuurd worden en er uiteindelijk een factuur naar de eigenaar van de auto wordt gestuurd. Er is dus sprake van verwerking van gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hetgeen betekent dat de WBP van toepassing is.

Iets wat hierbij nog een rol speelt, is of de geo-informatie – de gegevens waar en wanneer iemand ergens gereden heeft – in de OBU dienen te blijven en dat alleen het totaal bedrag ter verdere verwerking (facturering) wordt verstuurd, of dat de geo-informatie ook verstuurd wordt en dat degene die de factuur opmaakt ook de prijs berekent.

Of nu het ene of het andere alternatief gekozen wordt maakt niet uit voor het feit of er sprake is van persoonsgegevens. Het maakt wel iets uit voor de mogelijke beschikbaarheid en de beveiliging van die gegevens. Indien de rijgegevens bij een derde worden verwerkt en opgeslagen, is de kans altijd aanwezig dat deze gegevens door justitie opgevraagd worden of wellicht als gevolg van beveiligingslekken bij onbevoegden terecht komen. Die kans zal aanmerkelijk kleiner zijn indien de geo-informatie in de on board unit blijft. Het zal dan ook niet

verbazen dat het College bescherming persoonsgegevens een voorstander is van de verwerking van rijgegevens in de OBU zelf.[89]

2.6.7 Locatiebepaling gsm bij gebruik 112

Locatiebepaling met gsm´s wordt steeds populairder. Zo wordt bijvoorbeeld de bepaling van de plaats waar een gsm zich bevindt, gebruikt bij commerciële diensten om vrienden te lokaliseren die in de buurt zijn, maar zijn ook tal van andere diensten in ontwikkeling waarbij de locatiebepaling van de mobiele telefoon een rol speelt.[90] Dit soort diensten wordt ook steeds beter omdat de plaatsbepaling steeds nauwkeuriger wordt.

Naast commerciële partijen heeft ook de overheid te maken met locatiebepaling van mobiele telefoons. Zo is de bepaling van de locatie van een persoon die het alarmnummer 112 belt van groot belang. Het belang van locatiebepaling van mobiele bellers wordt onder meer onderkend door de Europese Commissie. Deze heeft dan ook een aanbeveling gedaan waarin wordt gesteld dat aanbieders van openbare telefoonnetwerken of –diensten alles in het werk moeten stellen om voor alle oproepen naar het alarmnummer 112 de meest betrouwbare locatiegegevens over de beller te bepalen en door te zenden. Hierbij is overigens niet gekozen voor verplichte specifieke prestatiekarakteristieken voor locatiebepaling, maar is de voorkeur gegeven aan de toepassing van het zogenaamde *best effort*-principe.

In de aanbeveling worden de lidstaten aangemoedigd de ontwikkeling van diensten voor hulp in noodsituaties, zoals verwerkingsprocedures voor de verzending van locatie-informatie en andere informatie in verband met noodsituaties of ongevallen aan alarmcentrales, te bevorderen en te steunen. Daarnaast dienen lidstaten de ontwikkeling en tenuitvoerlegging van gemeenschappelijke interface-specificaties te steunen teneinde de interoperabiliteit van dergelijke diensten over heel Europa te waarborgen. Tevens worden lidstaten aangemoedigd het gebruik van locatietechnologie met een hoge precisie te bevorderen, zoals locatietechnologie voor cellulaire netwerken van de derde generatie en satellietnavigatiesystemen.[91]

Dit betekent dat wat vandaag *best effort* is, dat morgen niet meer behoeft te zijn, omdat er een verbeterde technologie is geïntroduceerd. Dat geldt niet alleen als er een betere technologie is ter bepaling van de locatie, maar ook als er nieuwe technologieën zijn die het mogelijk maken dat voertuigen met alarmcentrales kunnen gaan communiceren. Bijvoorbeeld de technologie die het mogelijk maakt dat wanneer de airbags in een auto geactiveerd worden, via het mobiele netwerk automatisch een noodoproep verstuurd wordt naar een centrale. Met behulp van meegestuurde geo-informatie over de exacte locatie van het ongeval, kunnen hulpdiensten dan nog sneller ter plaatse zijn.[92] [93]

Een dergelijke communicatie geïnitieerd door het voertuig zelf kan ook gebruikt worden bij het vervoer van gevaarlijke stoffen. In geval van een ongeval bij een dergelijk transport zou dan ook informatie meegezonden kunnen worden over de aard van het vervoerde materiaal en op basis

---

[89] Brief hoorzitting kilometerprijs 31 januari 2008, CBP (<www.cbpweb.nl> en zoek op trefwoord *kilometerprijs*).
[90] Friend FindA, Optus Zoo, <mobile.optuszoo.com.au>, klik op Friend FindA onder FindA in de linker kantlijn.
[91] Aanbeveling van de Commissie betreffende de verwerking van locatie-informatie over de oproeper in elektronische communicatienetwerken met het oog op locatie-uitgebreide noodoproepdiensten, PbEU 2003, L 189/49.
[92] In-vehicle emergency call system "eCall", Europese Commissie, DG Informatiemaatschappij <europa.eu/scadplus/leg/en/lvb/l31103a.htm>.
[93] Europa gaat ontwikkeling slimme auto's aanjagen, Tweakers.net, 18 september 2007 (<tweakers.net>, zoeken naar slimme auto's)

daarvan actie ondernomen kunnen worden. In deze gevallen moeten alarmcentrales dan natuurlijk wel die extra informatie kunnen verwerken.

Recht om met rust gelaten te worden
Het recht om rust gelaten moet ook in het geval van noodoproepdiensten een stap opzij doen. In Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten (de Universeledienstrichtlijn) wordt daartoe bepaald dat exploitanten van openbare telefoonnetwerken, voor zover dat technisch haalbaar is, voor alle oproepen naar het uniforme Europese alarmnummer 112 locatie-informatie over de oproeper ter beschikking moeten stellen van de instanties die noodsituaties behandelen.[94]

Ook in Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (de richtlijn betreffende privacy en elektronische communicatie) wordt verwezen naar noodoproepdiensten.[95] In deze richtlijn wordt namelijk bepaald dat de aanbieder van een openbaar telecommunicatienetwerk en/of een openbare elektronische communicatiedienst de uitschakeling van de weergave van de identificatie van de oproepende lijn en het tijdelijk weigeren of ontbreken van de toestemming van de abonnee of gebruiker voor
de verwerking van locatiegegevens per afzonderlijke lijn voor organisaties die noodoproepen behandelen en als zodanig door een lidstaat erkend zijn, met inbegrip van wetshandhavingsinstanties en ambulance- en brandweerdiensten, met het oog op de beantwoording van die oproepen kan opheffen.

Het vorenstaande heeft zijn weerslag gekregen in artikel 11.10 van de Telecommunicatiewet.

Persoonsgegevens
De gegevens – telefoonnummer en locatiegegevens – die door een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst worden verstrekt aan beheerders van een alarmnummer voor publieke diensten worden door deze beheerders vastgelegd met het oog op de hulpverlening in noodsituaties of de bestrijding van het misbruik van een alarmnummer voor publieke diensten. Volgens artikel 11.10 lid 4 zijn deze beheerders verantwoordelijk voor de *vastlegging* van deze gegevens, net zoals deze beheerders verantwoordelijk zijn voor de *verstrekking* van deze gegevens. Hierbij wordt in de Telecommunicatiewet verwezen naar het begrip verantwoordelijke zoals genoemd in de Wet bescherming persoonsgegevens: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verstrekking van telefoonnummers en locatiegegevens met het oog op de bestrijding van het misbruik van een alarmnummer voor publieke diensten vindt overigens alleen plaats aan degene die op grond van artikel 141 of 142 van het Wetboek van Strafvordering is belast met de opsporing van strafbare feiten. Dit zijn onder meer officieren van justitie, ambtenaren van politie en de door Onze Minister van Justitie in overeenstemming met Onze Minister van Defensie aangewezen militairen van de Koninklijke marechaussee.

Tot slot is in het kader nog van belang te melden dat de nummers en de locatiegegevens slechts een zekere periode bewaard mogen worden. De termijn bedraagt ten hoogste twee maanden indien de nummers en gegevens betrekking hebben op gevallen waarbij sprake was van een verzoek om hulpverlening in een noodsituatie. De termijn is zes maanden indien de nummers en

[94] Zie artikel 26 van de richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten, PbEG2002, L 108/31.
[95] Zie artikel 10 en overweging 36 van de richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, PbEG2002, L 201/37.

gegevens betrekking hebben op gevallen waarin kennelijk sprake is van misbruik van een alarmnummer voor publieke diensten en is slechts 24 uur in alle overige gevallen.

2.6.8 OV-chipkaart

Of er ooit een OV-chipkaart komt, is de vraag. De laatste berichten over deze kaart voor het openbaar vervoer doen het ergste vrezen. Er wordt al voorzichtig gerept over het gebruik van de mobiele telefoon als betaalmiddel in het openbaar vervoer, een systeem dat in Duitsland en Frankrijk gebruikt gaat worden.[96]

Welk systeem er ook gebruikt gaat worden – ov-chipkaart of mobiele telefoon – er zal vanzelfsprekend sprake zijn van geo-informatie bij de verwerking van de reisgegevens. De plaats waar de reis van een subject begint wordt vastgesteld, evenals de eindbestemming. Daarbij zal ook de tijd geregistreerd worden voor het geval iemand tijdens daluren reist en daarvoor een kortingsabonnement heeft. Op grond van het gebruik van de ov-chipkaart kan evenwel niet vastgesteld worden, waar iemand zich bevindt. Althans, dit kan niet indien gebruik gemaakt wordt van de anonieme chipkaart of de wegwerpkaart, deze zijn immers aan een persoon gebonden. Het kan enigszins als een reiziger gebruik maakt van de persoonlijk ov-chipkaart. Van een dergelijke persoon zou op basis van op- en overstapgegevens achterhaald kunnen worden op welk traject hij zich bevindt, maar niet de exacte locatie. Die zou misschien weer wel achterhaald kunnen worden als een persoon een mobiele telefoon bij zich heeft. Een opsporingsambtenaar zou in een dergelijk geval de reisgegevens moeten opvragen bij de ov-organisatie en de telefoongegevens bij de telecomprovider.

Bij het gebruik van de mobiele telefoon als betaalmiddel zou de exacte locatie eenvoudiger bepaald kunnen worden en zouden de gegevens ook makkelijker achterhaald kunnen worden. Reisgegevens en telefoongegevens zijn dan immers gekoppeld en zullen door één organisatie beheerd worden, al is het alleen maar om een factuur te kunnen versturen of een verrekening te kunnen uitvoeren met het reistegoed op de telefoon.

Recht om met rust gelaten te worden
Los van de juridische aspecten gekoppeld aan het opzetten van de organisatie en het ontwikkelen van de technologie die het gebruik van de ov-chipkaart mogelijk moeten maken, is het met name de privacy die aandacht behoeft bij de introductie van deze kaart. Datzelfde geldt voor het eventuele gebruik van de mobiele telefoon als betaalmiddel voor het openbaar vervoer.

Het recht om rust gelaten te worden is in zoverre niet aan de orde, dat een ov-chipkaart of een mobiele telefoon die bij het reizen wordt gebruikt slechts een registratiemiddel is. De gebruiker wordt op basis van het gebruik niet gestoord in zijn rust. Althans, niet bij gebruik van chip-kaarten. De kaart is immers geen apparaat waarop berichten of anderszins ontvangen zouden kunnen worden. Dat zal anders kunnen zijn, indien we uiteindelijk toch met de mobiele telefoon gaan reizen. Op die telefoon zou na afloop van een reis een bericht over de kosten kunnen verschijnen. Een legitieme verstoring uiteraard. De telefoon in combinatie met reisgegevens zou echter ook gebruikt kunnen worden door commerciële partijen om personen te attenderen op winkels, restaurants, hotels, etc. in de buurt van de plek van aankomst.[97] Indien dit zou gebeuren zijn evenwel de regels van de Telecommunicatiewet van toepassing zoals eerder omschreven in hoofdstuk 4.2.1.3.3. Het ongevraagd versturen van commerciële, ideële of charitatieve berichten uitsluitend is in een dergelijk geval alleen toegestaan, als aangetoond kan worden dat daarvoor toestemming is verleend.

---

[96] Zie Duits mobieltje haalt ov-chip in, Trouw, 25 januari 2008 en OV-chip was in 1992 een prachtidee, Trouw, 22 april 2008.
[97] Gerwin Franken, Leo van der Wees, Locatiegebonden diensten, een verkenning. In: *Recht en locatie*, Leo van der Wees, Sjaak Nouwt (red.), Nederlandse Vereniging voor Informatietechnologie en Recht, Den Haag: Elsevier Juridisch, 2008

Persoonsgegevens
Een andere zaak betreft de persoonsgegevens die verwerkt worden in het geval van het gebruik van een persoonlijke ov-chipkaart of, eventueel, een mobiele telefoon bij het reizen per openbaar vervoer. Dat daar op een zeker moment sprake van is lijkt evident. De reisgegevens – geo-informatie – zijn gekoppeld aan het gebruik van de mobiele telefoon en deze dienen op een zeker moment gekoppeld te worden aan een persoon om deze een reisfactuur te kunnen sturen.

Hoe een en ander exact zal gaan bij het gebruik van de mobiele telefoon valt moeilijk te bepalen. Wel staat vast dat gegevens van de gebruiker van een mobiele telefoon in relatie gebracht dienen te worden met reisgegevens. En ook staat vast dat het College bescherming persoonsgegevens in een rapport heeft gesteld dat de omgang met gegevens van personen bij het gebruik van de ov-chipkaart in het Amsterdamse metronet is in strijd met de Wet bescherming persoonsgegevens.[98]

In het onderzoeksrapport van het CBP wordt vastgesteld dat er *teveel* persoonsgegevens worden vastgelegd en gebruikt, dat de gegevens *te lang* bewaard en *onvoldoende* beveiligd worden en dat de reiziger *geen helder inzicht* heeft in wat er met zijn gegevens gebeurt. “Dat kan ertoe leiden dat Amsterdammers onverhoeds geconfronteerd worden met hun reisgedrag van jaren”, aldus Jacob Kohnstamm, voorzitter van het CBP. Het CBP eist dan ook ten aanzien van de chipkaart in het Amsterdamse metronet naleving van de wettelijke normen en ziet zich anders genoodzaakt handhavend op te treden.

Nu is de Amsterdamse ov-chipkaart niet exact hetzelfde als het landelijke systeem dat men wellicht ooit gaat gebruiken in het openbaar vervoer, wel zullen bij welk systeem dan ook dezelfde soort gegevens verwerkt gaan worden. Het CBP geeft middels het rapport naar de gang van zaken in het Amsterdamse metronet overduidelijk aan dat alleen de hoogst noodzakelijke gegevens gebruikt moeten worden, dat deze niet te lang bewaard morgen worden en goed beveiligd dienen te worden. Bovendien moeten reizigers inzicht hebben in het gebruik van hun gegevens. Er dient voldoende transparantie te zijn.

Indien de technische perikelen van de ov-chipkaart ooit overwonnen zijn, dan verdienen de bovengenoemde aspecten dus nog de nodige aandacht alvorens tot definitieve ingebruikname over te gaan. Dat zal overigens ook het geval zijn indien de mobiele telefoon gebruikt gaat worden voor het reizen in het openbaar vervoer.

En dan hebben we het nog niet over de beveiliging van ov-chipkaart zelf. Deze schijnt inmiddels in enkele seconden gekraakt te kunnen worden.[99] [100] Nu is dat niet erg in het geval van anonieme of wegwerpkaarten, althans wat de persoonsgegevens betreft. Die staan immers niet op die kaarten. In het geval van persoonsgebonden kaarten kan een kraak echter wel een inbreuk op de informationele privacy vormen. Dat zal afhangen van de gegevens die op de kaart opgeslagen worden. Tevens biedt het kraken wellicht mogelijkheden om op naam van een ander te reizen (identiteitsdiefstal) en op deze wijze bijvoorbeeld de (digitale) kortingskaart van een ander te gebruiken.

2.6.9 Burgernet

Op 1 oktober 2008 is in acht gemeenten (Gouda, Delft, Ede, Leeuwarden, Dantumadeel, Breukelen, Maarssen en De Ronde Venen) begonnen met de werving voor een proef met Burgernet. Mensen die wonen of werken in deze plaatsen kunnen zich aanmelden als deelnemer.

---

[98] Reisgedrag Amsterdammers onnodig in beeld door OV-chipkaart GVB, CBP, 15 januari 2008 (<www.cbpweb.nl> zoeken naar *reisgedrag)*.
[99] Kraken ov-chip secondenwerk, Trouw, 12 april 2008
[100] Ov chipkaart definitief gekraakt, YouTube (<www.youtube.com> zoeken naar OV chipkaart).

De proef zelf start begin november. In Nieuwegein loopt al sinds 2004 een proef met Burgernet. Het ligt in de bedoeling om Burgernet stapsgewijs landelijk in te voeren.

Met Burgernet betrekt de politie het publiek bij een zoekactie naar een verdachte, een voertuig of een vermist persoon. Het is vergelijkbaar met SMS-alert. Bij Burgernet worden echter ook andere communicatiemiddelen gebruikt. De deelnemers krijgen een ingesproken mededeling over een gezocht persoon of voertuig te horen op hun vaste of hun mobiele telefoon, of ze krijgen een sms-bericht. Aanvullende informatie kan ook per e-mail worden ontvangen. Ook is het systeem al gereed voor toekomstig gebruik door bijvoorbeeld de brandweer en geneeskundige hulpverlening bij ongevallen en rampen.

De juridische problemen van Burgernet zijn vergelijkbaar met die van sms-alert. Het is daarom nodig aandacht te besteden aan de opslag en verwerking van de persoonsgegevens en wellicht een niets aan duidelijkheid te wensen over latende gedragscode annex privacy-statement op te stellen inzake het gebruik van Burgernet.

2.6.10 Verlof tbs'ers

Het zich tijdens het verlof aan de begeleiding onttrekken door ter beschikking gestelden (tbs'ers) en het vervolgens niet direct kunnen opsporen van deze personen leidt tot grote commotie in de samenleving. Er is daarom geëxperimenteerd met een enkelband die een GPS-signaal afgeeft dat er toe moet leiden dat een eventueel ontsnapte tbs'er snel weer in de kraag gevat kan worden.

Recht om met rust gelaten te worden
Los van het gegeven dat het nog maar de vraag is of deze enkelbanden ooit daadwerkelijk in gebruik genomen gaan worden, is het duidelijk dat bij het gebruik van enkelbanden die een GPS-signaal afgeven geo-informatie een rol speelt.

Daarnaast is het duidelijk dat het gebruik van de enkelband een inbreuk is op de persoonlijke levenssfeer van de ter beschikking gestelde. Het is evenwel evident dat die inbreuk een krachtens de wet gestelde beperking is, zoals aangeven in artikel 10 van de Grondwet, en daarmee legitiem is. Die wet is in dit geval titel IIB van het Wetboek van Strafvordering waarin regels neergelegd zijn inzake rechtsplegingen in verband met de terbeschikkingstelling en de plaatsing in een psychiatrisch ziekenhuis.

Persoonsgegevens
Het gaat bij gebruik van een enkelband door een tbs'er ook om gegevens betreffende een persoon. Het signaal van de enkelband verwijst immers naar een bepaalde tbs'er die met naam en toenaam bekend is. Er vanuit gaande dat in het geval van een ontsnapping de signalen, geografische gegevens, naam en toenaam worden opgeslagen en verwerkt in systeem in het kader van een politietaak, opsporing, maakt deze gegevens politiegegevens in de zin van de Wet politiegegevens. Dit betekent onder andere dat deze gegevens tot een jaar na de eerste verwerking verwerkt mogen worden, en pas vijf jaar na de eerste verwerking verwijderd hoeven te worden.

2.6.11 Noodhulpfunctie ouderen middels GPS

In een vergrijzende maatschappij waarin steeds minder mensen een werkzaam bestaan leiden en waarin de gezondheidszorg als gevolg daarvan onder druk komt te staan, zullen ouderen langer zelfstandig blijven wonen. Om in gevallen van nood toch snel en adequaat geholpen te kunnen worden, zullen toepassingen bedacht worden waarbij onder meer gebruik gemaakt zal worden van GPS. Dat stelt immers noodhulpdiensten in staat snel naar de goede plek te gaan om daar de gewenste hulp te verlenen.

Recht om met rust gelaten te worden
Indien een noodhulpfunctie voor ouderen verloopt via een door de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangewezen beheerder van een alarmnummer voor publieke diensten, dan zijn dezelfde regels van toepassing als beschreven in het onderdeel over locatiebepaling bij gebruik van 112. De Telecommunicatiewet staat toe dat nummer en locatiegegevens worden doorgegeven.

Het zal duidelijk zijn dat indien iemand zich aansluit bij een specifieke noodhulpdienst voor ouderen dat deze persoon daarmee aangeeft absoluut niet met rust gelaten te willen worden in geval van calamiteiten. Een soort opt-in.

Persoonsgegevens
Telefoonnummers en locatiegegevens die in het kader van een noodhulpdienst voor ouderen zijn doorgegeven mogen een bepaalde periode bewaard blijven, aldus artikel 11.10 van de Telecommunicatiewet. Deze periode is evenwel niet langer dan 6 maanden en dat kan alleen zo lang zijn in het geval men een misbruik van de noodhulpdienst vermoedt.

Wellicht dat deze regeling aanpassing behoeft, indien bijvoorbeeld medische gegevens meegezonden gaan worden met een oproep voor hulp. Iets wat niet ondenkbaar is, en zelfs levensreddend zou kunnen zijn. Een hulpverlener kan dan immers onderweg al een medisch dossier inzien en wellicht alvast bepaalde voorbereidingswerkzaamheden verrichten.

Stel dat medische gegevens meegezonden worden, maar dat er sprake is geweest van misbruik van de noodhulpdienst, dan lijkt het niet noodzakelijk ook de medische gegevens 6 maanden te bewaren. Om een eventuele misbruiker te kunnen aanpakken zijn nummer en locatiegegevens afdoende. Aan de Telecommunicatiewet zou dan toegevoegd kunnen worden dat medische gegevens bijvoorbeeld maximaal twee maanden bewaard mogen worden. In geval er iets mis gaat bij de hulpverlening en dat nader onderzoek behoeft, dan is er in het geval van 2 maanden nog voldoende gelegenheid om na te gaan welke medische gegevens bekend waren bij de hulpverleners.

In het kader van de informationele zelfbeschikking kan ook in dit geval sprake zijn van opt-in. Het kan aan de oudere zelf worden overgelaten om te bepalen of hij zijn medische gegevens wil meesturen bij een oproep voor noodhulp.

2.6.12 GPS- locator tegen diefstal auto's

In het geval van een GPS-locator beschikt een voertuig over een GPS-zender en is het mogelijk een voertuig te volgen en te traceren. In geval van diefstal is een voertuig dan op betrekkelijk eenvoudige wijze terug te vinden.

Recht om met rust gelaten te worden
Vooralsnog kan een eigenaar er zelf voor kiezen om zijn voertuig met een GPS-zender uit te rusten. Er gaan echter ook stemmen op om een GPS-zender te verplichten voor auto´s boven een zeker bedrag. En wellicht komt er een moment dat alle auto´s een dergelijke zender hebben. Misschien gaat dat niet eens zo lang meer duren. Als immers auto´s voorzien gaan worden van een on board unit voor de kilometerprijs dan kan die OBU immers eenvoudig als locator dienen om auto´s te kunnen traceren in geval van diefstal of vermissing. Het gebruik van de OBU voor andere zaken dan waar deze voor geïnstalleerd is, dient echter wel met waarborgen omkleed te worden. Zo zal er bijvoorbeeld sprake moeten zijn van een aangifte en een daarbij gegeven (schriftelijke) toestemming van de eigenaar van de auto deze te lokaliseren.

Persoonsgegevens
Gegevens over personen spelen in zoverre een rol dat naam van de eigenaar en autogegevens bekend zullen zijn na aangifte. Deze gegevens zijn daarmee politiegegevens, worden dan in het

kader van een politietaak verwerkt en zullen dan conform de eerder genoemde termijnen van de Wet politiegegevens bewaard kunnen worden.

2.6.13 Geografische informatie systemen en privacy

Tot slot van dit onderdeel over de toepassing van privacyregels en –gedaanten kort aandacht voor geografische informatiesystemen. Daarbij wordt in dit geval gedoeld op informatiesystemen waarbij geo-informatie in bijvoorbeeld een grafische vorm of een foto wordt weergegeven. Het kan dan bijvoorbeeld gaan om overheidsdiensten die gebruik maken van commerciële toepassingen zoals Google Maps, maar hierbij kan eveneens gedacht worden aan het hergebruik van geografische systemen van de overheid door derden in het kader van de vernieuwde Wet openbaarheid van bestuur.

Recht om met rust gelaten te worden
Het is denkbaar dat een GIS-systeem kaarten bevat van bijvoorbeeld postcodegebieden en dat men op basis van de gemiddelde prijs van huizen in die gebieden, de bewoners ervan voorziet van bepaald foldermateriaal. Bewoners van die betreffende gebieden stellen dit wellicht niet op prijs maar kunnen de folders direct in de prullenbak gooien of middels een sticker op de brievenbus de overlast tot een minimum beperken.

Anders zou het zijn indien GIS-systemen met daarin tevens gegevens zoals het e-mailadres of het (mobiele) telefoonnummer bevraagd zouden kunnen worden, waarop vervolgens op de persoon gerichte acties plaatsvinden. Indien dergelijke acties op digitale wijze plaatsvinden, is opnieuw de eerder genoemde Telecommunicatiewet van toepassing en dient een persoon dus eerst toestemming te geven alvorens deze kan worden benaderd.

Google Street View
De persoonlijke levenssfeer zou mogelijk wel aangetast kunnen worden door een toepassing als Street View van Google.[101] Dit is een soort toevoeging aan Google Maps die het mogelijk maakt foto´s te zien van de straten die een gebruiker op de kaart ziet. En dat dan op straatniveau, hetgeen betekent dat op de foto´s de voorkanten van huizen en ook mensen te zien zijn. De mensen worden daarbij overigens wel wazig en daardoor (zo goed als) onherkenbaar afgebeeld. Het is Google immers ook niet te doen om de mensen die toevallig passeerden tijdens de opnamen, maar om het beeld van de straat, zodat een aanstaande bezoeker zich alvast kan oriënteren. Ook foto´s zonder personen erop kunnen evenwel problemen opleveren bleek begin april 2008, toen een Amerikaans echtpaar besloot een rechtszaak aan te spannen tegen Google in verband met de foto van hun huis in Street View.[102] Zij hebben het huis gekocht om met rust gelaten te worden. Het ligt dan ook aan een weg die in eigendom van de huizenbezitters in de straat. Een auto is desondanks die weg opgereden en heeft foto´s van de huizen gemaakt zonder daarvoor toestemming te vragen. Gezien deze situatie heeft de actie wellicht kans van slagen en zal Google zorgvuldiger moeten omgaan met het opnemen van foto´s voor Street View.

Het Nederlandse College bescherming persoonsgegevens heeft aangegeven vooralsnog geen bezwaar te hebben tegen Street View gezien het feit dat Google verschillende maatregelen heeft genomen om mogelijk privacygevoelige beelden van gezichten, kentekens, en anderszins onherkenbaar te maken.[103]

In dit kader is het evenwel goed alert te zijn op de mogelijkheid die tegenwoordig bestaat om gemaskeerde foto´s van personen weer duidelijk te maken. Een voorbeeld daarvan is de man die dacht zonder problemen foto´s te kunnen verspreiden van zichzelf waarop hij jonge jongens

[101] Street View, Google <maps.google.com/help/maps/streetview/>.
[102] Google 'Street View' invaded suburban Pa. couple's privacy, suit claims, LegalNewsline.com, 7 april 2008 (<www.legalnewsline.com> zoeken naar *street view*).
[103] Street View mag van CBP, Automatisering Gids, 8 augustus 2008.

misbruikt, omdat hij zichzelf onherkenbaar had gemaakt. Interpol heeft de zogenaamde roerbakfoto evenwel bewerkt waardoor de man herkenbaar werd en uiteindelijk opgepakt kon worden.[104] Indien dit soort technieken gemeengoed wordt, dan kunnen Google en andere aanbieders van online straatgezichten wellicht beter opnames maken van straten op momenten dat daar niemand loopt, of op foto´s aanwezige personen met een daartoe geschikt programma (definitief) verwijderen.

Persoonsgegevens
Veel geo-informatie die is opgeslagen in geografische informatiesystemen kan worden aangemerkt als persoonsgegevens. Hierbij kan bijvoorbeeld worden gedacht aan de registraties bij het Kadaster en de gemeenten, registraties voor grondgebonden belastingen bij de waterschappen en gemeenten, alsmede aan de registraties van aansluitingen bij nutsbedrijven. Deze gegevens zijn gecombineerd herleidbaar tot een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van artikel 1 WBP.

Om die reden bevat bijvoorbeeld de Kadasterwet in afdeling 2 specifieke regels inzake de bescherming van de persoonlijke levenssfeer. Zo staat in artikel 107b van de Kadasterwet dat ter bescherming van de persoonlijke levenssfeer van personen die in het Kadaster vermeld staan, ten aanzien van de verstrekking van inlichtingen beperkingen vastgesteld kunnen worden. Daarbij kunnen tevens regels worden vastgesteld voor de behandeling van verzoeken tot afscherming van persoonsgegevens.

De memorie van toelichting bij de WBP zegt in dit verband dat het onverenigbaar zou zijn met het doel van het Kadaster wanneer een eventuele, digitaal ter beschikking staande versie van de registratie, tot gevolg zou hebben dat een ieder zonder bijzondere inspanning daarop zoekfuncties zou kunnen loslaten die bijvoorbeeld een lijst zouden opleveren van alle personen die een pand in eigendom hebben boven een bepaalde waarde.[105]

Aan de andere kant is niet elk technisch of toevallig verband tussen een gegeven en een persoon voldoende om dat gegeven een persoonsgegeven te doen zijn. Gegevens die naar hun aard niet op personen betrekking hebben noch – gezien de context waarin ze worden verwerkt – mede bepalend zijn voor de wijze waarop een persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, zijn geen persoonsgegevens. Een voorbeeld hiervan zijn gegevens die bijvoorbeeld onroerende zaken of andere registergoederen identificeren. Het feit dat deze zaken via een openbaar register zoals het Kadaster tot een individuele natuurlijke persoon kunnen worden herleid, doet hieraan op zichzelf niet af. Het zou anders zijn indien bij een verstrekking van dergelijke objectgegevens op CD-ROM, aanvullende gegevens omtrent personen worden vermeld, waardoor de zoekbaarheid op personen mogelijk wordt. Gegevens van een netwerkbeheerder over het gebruik van het netwerk via aansluitpunten teneinde het goed functioneren van het netwerk te waarborgen, zijn ook geen persoonsgegevens zolang elke reële mogelijkheid is uitgesloten dat die gegevens worden gebezigd om het gebruik van het netwerk door individuele personen in ogenschouw te nemen.[106]

Procedures Online Nijmegen
In relatie tot een concreet gebruik door een gemeentelijke overheid – Nijmegen – van de commerciële toepassing Google Maps in combinatie met bouw- en milieuvergunningen heeft het College bescherming persoonsgegevens overigens gesteld dat deze publicatiewijze onrechtmatig was.

De artikelen 7 en 8 van de WBP bepalen dat persoonsgegevens alleen voor een gerechtvaardigd doeleinde mogen worden verzameld en dat de verantwoordelijke de gegevens alleen mag

[104] Interpol maakt 'roerbakfoto' pedofiel ongedaan, Tweakers.net, 8 oktober 2007 (<www.tweakers.net> zoeken naar *roerbakfoto*).
[105] *Kamerstukken II* 1997-1998, 25892, nr. 3, p.24.
[106] *Kamerstukken II* 1997-1998, 25892, nr. 3, p.47.

verwerken met toestemming van de betrokkenen of indien het noodzakelijk is in de zin van één van de in artikel 8 WBP genoemde grondslagen. De gemeente Nijmegen stelde zich aanvankelijk op het standpunt dat zij wettelijk verplicht zou zijn om de documenten integraal op internet te publiceren. Daarmee zou de gemeente een grondslag hebben onder artikel 8 onder c WBP en een gerechtvaardigd doeleinde, namelijk het moeten voldoen aan een wettelijke verplichting.

De vermeende wettelijke verplichting zou voortvloeien uit de Wet openbaarheid van bestuur (Wob), in combinatie met verplichtingen uit de Algemene wet bestuursrecht (Awb) en de Woningwet. Zoals de gemeente naderhand echter ook erkende, bevatten de genoemde wetten geen expliciete verplichting om documenten met persoonsgegevens integraal te publiceren op internet. De gemeente kan zich derhalve niet beroepen op een grondslag onder 8 onder c WBP.

De gemeente kon zich voor de integrale publicatie op internet evenmin beroepen op toestemming van de betrokkenen (artikel 8 onder a WBP), op de noodzaak om te publiceren voor een goede vervulling van de publiekrechtelijke taak (artikel 8 onder e WBP) of op de noodzaak om te publiceren na afweging van haar gerechtvaardigd belang tegen het privacybelang van elke betrokkene (artikel 8 onder f WBP). Door het ontbreken van een gerechtvaardigd doeleinde en grondslag was de publicatiewijze van Nijmegen dan ook in strijd met artikel 7 en 8 WBP en daardoor onrechtmatig. Het CBP stelde dat Nijmegen ofwel een veel beperktere set persoonsgegevens zou moeten gaan publiceren ofwel ondubbelzinnige toestemming van betrokkenen zou moeten vragen. [107]

Het gebruik van commerciële geografische toepassingen lijkt dus eenvoudig gekoppeld te kunnen worden aan overheidsdiensten. Het Nijmeegse voorbeeld geeft evenwel aan dat voorzichtigheid geboden is bij de ontsluiting van persoonsgegevens via dit soort toepassingen.

Inspire
Die zelfde voorzichtigheid dient overigens betracht te worden bij de implementatie van het wetsvoorstel op basis van de EG richtlijn 2007/2/EG informatiestructuur ruimtelijke informatie (Inspire, Infrastructure for Spatial Information in Europe).

Doel van dit voorstel is het harmoniseren van ruimtelijke gegevens van overheidsorganisaties ten behoeve van het milieubeleid en het oprichten van een infrastructuur hiertoe. Door deze infrastructuur dient de uitwisselbaarheid en toegankelijkheid van geo-informatie voor overheden binnen de lidstaten en tussen de lidstaten, organen binnen de Europese Unie en voor burgers te worden vergroot. Het betreft enerzijds geo-informatie zoals coördinaten, adressen, kadastrale kaart en topografische namen en anderzijds ruimtelijke gegevens van objecten die te maken hebben met milieu zoals habitats, meteorologie en bodemgebruik.

Bij het ministerie van VROM bestond enige zorg met betrekking tot dit wetsvoorstel in relatie tot het verwerken van persoonsgegevens. Om die reden heeft het ministerie het CBP om advies gevraagd. Het College bescherming persoonsgegevens stelde daarop dat het wetsvoorstel geen nieuwe verwerkingen van persoonsgegevens introduceert naast de reeds bestaande. Het wetsvoorstel implementeert slechts een Europese richtlijn ten behoeve van het gedigitaliseerd en geharmoniseerd toegankelijk maken van geo-informatie voor overheden en burgers.

Wel acht het CBP het wenselijk dat in de memorie van toelichting expliciet aandacht wordt besteed aan het begrip persoonsgegeven in relatie tot geo-informatie om misverstanden bij databeheerders te voorkomen.[108]

[107] Integrale publicatie vergunningaanvragen op internet onrechtmatig, Recht.nl, 04/04/2008, <http://recht.nl/32202>.
[108] Toegankelijkheid geo-informatie, CBP, 20 februari 2008 (<www.cbpweb.nl> zoeken op *inspire*).

De richtlijn zelf zegt in overweging 24 dat de verstrekking van netwerkdiensten dient te geschieden in overeenstemming met de beginselen inzake de bescherming van persoonsgegevens overeenkomstig richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. En in artikel 1f staat dat lidstaten de publieke toegang tot verzamelingen van ruimtelijke gegevens en diensten met betrekking tot ruimtelijke gegevens mogen beperken indien de toegang afbreuk zou doen aan de vertrouwelijkheid van persoonsgegevens en/of -dossiers met betrekking tot een natuurlijk persoon wanneer die persoon niet heeft ingestemd met bekendmaking van de informatie aan het publiek, wanneer in deze vertrouwelijkheid is voorzien in het nationale recht of het Gemeenschapsrecht.

Indien het wetsvoorstel conform het advies van het CBP en het gestelde over persoonsgegevens in de richtlijn wordt opgesteld, lijkt de bescherming van deze gegevens afdoende te zijn geregeld voor de ontwikkeling van de infrastructuur voor ruimtelijke informatie. Op het moment van schrijven van dit rapport lag overigens het wetsvoorstel voor advies bij de Raad van State waardoor het niet openbaar toegankelijk was.

3. Conclusie privacy

3.1 Inleiding

Hiervoor zijn allereerst de privacyregels besproken. Vervolgens is een aantal toepassingen genoemd: locatiegebonden diensten en geografische informatiesystemen, waarna deze toepassingen zijn toegelicht in het kader van de beschreven regels. In dit hoofdstuk worden enige gevolgtrekkingen op een rij gezet. Net als in de voorgaande hoofdstukken wordt daarbij een onderscheid gemaakt tussen locatiegebonden diensten en geografische informatiesystemen. Tevens wordt aandacht besteed aan privacy in de publieke ruimte en aan de mate waarin burgers privacy mogen verwachten, twee zaken waarin op zijn minst enige verandering teweeggebracht wordt door met name de toename van locatiegebonden diensten.

3.2 Locatiegebonden diensten

Met de beschrijving van een aantal locatiegebonden systemen en de gevolgen voor privacy-gerelateerde informatie (zoals geo-informatie) die verwerkt wordt door of via deze systemen, is geprobeerd om aan te tonen dat er niet echt een grote gemene deler is. Ook al lijken sommige systemen technisch op elkaar, elk systeem dient op zijn privacy-merites beoordeeld te moeten worden. Men zou dat 'contextuele privacy' kunnen noemen,[109] hetgeen betekent dat binnen de context waarin een systeem gebruikt wordt of gaat worden, dit systeem wordt beoordeeld op de gevolgen die het kan hebben voor privacy (recht om rust gelaten te worden én gegevensbescherming). De vier typen morele redenen voor de bescherming van identiteitsgerelateerde informatie, eerder genoemd in de AVB-studie *Waardengevoelig ontwerp en de automatiserende overheid: het voorbeeld van identiteitsinfrastructuur* kunnen daarbij een rol spelen.[110]

Daarbij zou de leidraad moeten zijn dat zo weinig mogelijk gegevens verwerkt dienen te worden, maar vanzelfsprekend genoeg om een systeem naar behoren te kunnen laten functioneren. Dus het vervoersbedrijf Amsterdam kan met minder af, zoals het CBP constateerde, en voor de verwerking van reisgegevens inzake de kilometerheffing lijkt het niet noodzakelijk dat deze door een derde partij worden opgeslagen en verwerkt. Dat leidt immers to onnodige risico's en stelt hoge(re) eisen aan de beveiliging van systemen.

Dit sluit aan bij het principe *less is more* zoals vaak vermeld in relatie tot privacy enhancing technologies (PET).[111] Dit houdt in dat vooraf duidelijk en goed onderbouwd dient te worden welke gegevens van individuen men minimaal nodig heeft en in welke gevallen aanvullende informatie nodig is. En daarbij dient men dan uit te gaan van de verwerking van zo weinig mogelijk persoonsgegevens, de goede werking van een systeem in ogenschouw nemend. Er dienen dus geen onnodige dan wel ongewenste verwerkingen van persoonsgegevens plaats te vinden. Deze gedachten zijn ook terug te vinden in de laatste volzin van artikel 13 van de WBP, waarin staat dat er passende (technische en organisatorische) maatregelen genomen moeten

[109] Privacy as Contextual Integrity, Helen Nissenbaum, *Washington Law Review* 2004/79: 101-140.
[110] Jeroen van den Hoven, Adrienne van de Bogaard, *Waardengevoelig ontwerp en de automatiserende overheid: het voorbeeld van identiteitsinfrastructuur*. TUDelft, November 2006 (<www.google.nl> zoeken naar "*contextuele integriteit*")
[111] Zie het dossier Privacy by Design op de website van he CBP (<www.cbpweb.nl> onder Themadossiers).

worden gericht op het voorkomen van de onnodige verzameling en verdere verwerking van persoonsgegevens.

Bij de beoordeling van de context van het gebruik van privacy-gevoelige gegevens en de toepasbaarheid van het principe *less is more* zou een privacyfunctionaris of FG (functionaris voor de gegevensbescherming) of een EDP-auditor ingeschakeld kunnen worden, die tevens een oordeel – een privacy-audit – velt over het ontwerp van te gebruiken of te ontwikkelen systeem. Enkele ministeries (SZW en OCW) beschikken al over een dergelijke persoon.

Daarnaast is en blijft transparantie een groot goed. Het moet consumenten te allen tijde duidelijk zijn wie welke gegevens over hen verzamelt en zij moeten eenvoudige middelen hebben om hun gegevens te kunnen (laten) wijzigen, verwijderen of anderszins. Om die reden kan een privacyregeling of gedragscode bij het gebruik van diensten als sms-alert en groeps-sms wenselijk zijn.

In zijn algemeenheid past bij de verlening van dit soort diensten een actief overheidsbeleid. Het moet niet de burger zijn die op zoek moet gaan naar plekken waar zijn gegevens opgeslagen kunnen zijn; de overheid moet actief – op eigen initiatief – aangeven bij wie welke gegevens voor hoe lang zijn opgeslagen.

3.3 Geografische informatiesystemen

In relatie tot geografische informatiesystemen kan in feite hetzelfde gezegd worden als in de zaak van Procedures Online van de gemeente Nijmegen naar voren kwam. Het CBP oordeelde daarover dat in het licht van het doel van het systeem vooral teveel gegevens via internet toegankelijk waren.

Bij het commerciële Street View werd in datzelfde kader door het College bescherming persoonsgegevens bepaald dat het verwijderen of maskeren van privacygevoelige gegevens door Google afdoende geregeld is, zodat maatregelen tegen Street View (vooralsnog) niet nodig zijn. Mocht de overheid van zins zijn een soortgelijke publieke dienst op te zetten of gebruik te gaan maken van Street View dan lijkt dat vooralsnog toelaatbaar.

Elke keer weer dient men evenwel opnieuw alert te zijn op de mogelijke gevolgen voor de (contextuele) privacy. En elke keer weer dient er dus daaromtrent een zorgvuldige afweging plaats te vinden, zoals dat bijvoorbeeld ook is gedaan door het College bescherming persoonsgegevens betreffende het wetsvoorstel voor het opzetten van een infrastructuur van ruimtelijke informatie.

3.4 Privacy in de publieke ruimte en de verwachting van privacy

Bij geografische informatie en privacy denkt men vooral aan de openbare, publieke ruimte. Deze informatie kan betrekking hebben op de positie van het huis, de auto, de boot, het strandhuis, etc. – objecten - maar natuurlijk ook op de positie van de personen – subjecten- die zich door de publieke ruimte bewegen. Daar waar steeds meer diensten gebruikt en ontwikkeld worden waarbij geo-informatie van subjecten een rol spelen lijkt als gevolg daarvan die publieke ruimte steeds minder vrij te worden. Zeker als we bedenken dat naast geografische informatiesystemen en locatiegebonden diensten er in de publieke ruimte tegenwoordig steeds vaker camera's aanwezig zijn die opnames maken van passerende burgers.[112] Om nog maar niet te spreken van de digitale openbare ruimte[113] – het internet – waar u ook zonder exhibitionistisch gedrag

[112] Ross Clark, The Road to Southend Pier: One Man's Struggle Against the Surveillance Society, Harriman House Publishing, 2007

[113] Over het internet als publieke ruimte kan gediscussieerd worden. Zie: Van oude en nieuwe kennis : de gevolgen van ICT voor het kennisbeleid, WRR, r61 2002, p.69.

(YouTube, Hyves, etc.) moet vrezen voor uw privacy. Zoekmachines schijnen immers al uw zoekwoorden te registreren. Woorden die u ingeeft om informatie te vergaren over de meest persoonlijke zaken belanden allemaal in de databank van de gebruikte zoekmachine.[114] Dit alles heeft tot gevolg dat langzaam maar zeker afbreuk plaatsvindt aan de in dit rapport beschreven universele waarden. Immers, hoe vrij kan iemand leven als hij in de (virtuele) openbare ruimte constant bespied kan worden - en vaak wordt - door camera's op straat, door zendmasten en satellieten, door zoekmachines, etc. En in hoeverre vormen deze ontwikkelingen een inmenging in iemands leven, en hoe vrij is iemand om zich te verplaatsen als hij continu in de gaten gehouden kan worden?[115] Of dient de mens simpelweg als gevolg van de ontwikkeling van technologie iets van zijn waarden in te leveren, iets van zijn privacy in te leveren? Dient het begrip openbare ruimte aangepast te worden aan de stand van de huidige technologische ontwikkelingen? Technologie lijkt immers een steeds belangrijkere rol te spelen bij het reilen en zeilen in de wereld, in welke sector dan ook. Technologie zal blijven, en zich verder ontwikkelen. Daarbij lijkt het echter verstandig de negatieve aspecten niet uit het oog te verliezen en een regulatief kader te realiseren, en desgewenst aan te passen, om deze effecten te beperken. Denk daarbij bijvoorbeeld aan de regulering inzake de bewaartermijnen van gegevens van klanten van telecombedrijven. Daarnaast dient men bij het ontwerpen van nieuwe technische toepassingen al rekening te houden met eventuele negatieve gevolgen voor privacy, en met de context waarin technologie gebruikt wordt, zoals hierboven aangegeven.

Maar natuurlijk moeten we ook niet vergeten dat technologie gemak met zich mee brengt. De gemiddelde Nederlander is volstrekt onthand als hij per ongeluk een keer zonder mobiele telefoon de deur uit gegaan is.[116] Ook is het fijn dat de online platenwinkel, als u weer eens langs surft, aanbevelingen voor u heeft. Aanbevelingen die zijn bepaald op basis van uw eerdere aankopen en op die van andere kopers met een soortgelijk aankooppatroon als dat van u. En het is tevens fijn dat burgers zich veiliger voelen als zij weten dat er camera's hangen – hoewel de effecten van cameratoezicht niet eenduidig blijken te zijn[117] – los van de vraag of camera's een nuttige rol spelen bij het terugdringen van misdaad.[118] Er moet sprake zijn van (technische) vooruitgang én privacy, niet van vooruitgang of privacy. En als een vooruitgang een inperking van de privacy met zich mee zou brengen, dan zou de zelfbeschikking voorop moeten staan. Het is aan de persoon zelf om iets van zijn privacy in te leveren, in ruil voor een nieuwe (technologische) dienst.

Als gevolg van deze ontwikkelingen – camera's, verwerking gegevens via internet, opslag gegevens voor locatiegebonden diensten - neemt de redelijke verwachting van privacy af.[119] Een ontwikkeling die zich ook in het recht lijkt te manifesteren. In dat opzicht ontwikkelt het begrip privacy zich wel op basis van ontwikkelende technologie. Of die ontwikkeling een wenselijke kant op gaat is evenwel de vraag. De eerdergenoemde studie van het Rathenau Instituut *Van*

---

[114] Internetzoekmachines moeten privacy respecteren, CBP, 7 april 2008 (<www.cbpweb.nl> zoeken naar *zoekmachines*).
[115] Kilometerbeprijzing mag geen nationaal volgsysteem worden, CBP, september 2008 (beschikbaar via Recht.nl, <recht.nl/34300>).
[116] Nomofoob is nergens zonder mobiletje, Trouw, 11 april 2008 (Zoek via <www.google.nl> met het zoekwoord *nomofoob* voor de volledige tekst van dit artikel)
[117] De objectieve veiligheid is dankzij c.q. ondanks cameratoezicht in sommige gemeenten afgenomen en in andere gemeenten toegenomen. Zie S. Dekkers, 'Waakzame kijkers. Cameratoezicht op openbare plaatsen'. *Secondant* #5, oktober 2006. Op internet: http://www.hetccv.nl/binaries/ccv/dossiers/bestuurlijk-handhaven/cameratoezicht/secondant_5-06_cameratoezicht_openbare_plaatsen.pdf.
[118] CBP: Noodzaak en effectiviteit cameratoezicht onduidelijk, Recht.nl, 01/12/2004 (<recht.nl/25612>).
[119] Vgl. J. Nouwt, B.R. de Vries, J.E.J. Prins (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy.* The Hague: TMC Asser Press, 2005, p. 339.

privacyparadijs tot controlestaat, en het themanummer van de Groene Amsterdammer getiteld *De Gluurstaat* lijken deze vraag niet positief te beantwoorden.

3.5 Geo-informatie en privacy: een paar apart?

Speelt geo-informatie nu een bijzondere rol in relatie tot privacy? Nee, hetgeen gesteld is over contextuele privacy, privacy-by-design en transparantie geldt ook voor systemen waarbij geo-informatie geen rol speelt. Bovendien is geo-informatie sec niet privacy-gevoelig. Dat wordt deze informatie pas indien deze herleidbaar is tot identificeerbare personen, hetgeen veelal het geval zal zijn bij een opslag gecombineerd met andere gegevens. Indien dat echter het geval is, dan krijgt een ieder al snel visioenen van Big Brother. Opgeslagen persoonsgegevens leiden niet zo snel tot grote ongerustheid; als de overheid evenwel ook weet waar de burger wanneer geweest is, dan gaat dat toch een gevoel van ongemak en onvrijheid teweegbrengen. Men gaat zich ongemakkelijk voelen bij het bewegen in de openbare ruimte. Net zoals velen van ons nu nadenken over het gebruiken van zoekwoorden in Google, wetende dat deze worden opgeslagen. Of wat te denken van het plaatsen van persoonlijke gegevens in sociale netwerken.[120]

De privacy in de gewone en in de virtuele openbare ruimte lijkt dus in het geding te zijn.[121] De opslag van geo-informatie draagt daaraan bij en dient alleen al om die reden zo beperkt mogelijk gehouden te worden. Bovendien volgt uit de rechtspraak van het Europese hof voor de rechten van de mens dat de overheid ook in de publieke sector het grondrecht op privacy dient te respecteren.

3.6 Slot

Geografische informatiesystemen en locatiegebonden systemen bekeken hebbend vanuit privacy-perspectief moet gezegd worden dat privacy absoluut een rol speelt. Deze rol zou privacy al moeten spelen op de tekentafel (via privacy-by-design of via een Privacy Impact Assessment: PIA), zodat een ontwerp tot stand gebracht wordt dat rekening houdt met privacy, maar dat ook in zich herbergt dat zo weinig mogelijk gegevens worden verwerkt voor een zo optmaal mogelijk werkend systeem. Hiertoe zou een rol toebedicht moeten worden aan een privacyfunctionaris of FG.

Los hiervan dient bij gebruik van geografische informatiesystemen en locatiegebonden systemen waarbij privacy in het geding zou kunnen zijn, alle mogelijke transparantie in acht genomen dienen te worden. Hierbij dient de overheid een actieve rol te spelen. Indien de overheid aangeeft wie, welke gegevens over welke burgers bewaart, zal dat vertrouwen wekken bij de burgers, en zal dat diezelfde burgers bewust maken van het feit dat er gegevens verwerkt worden en hen wellicht manen tot een grotere voorzichtigheid omtrent die (persoons)gegevens. In dit kader is het wellicht interessant het rapport van de commissie Grondrechten in digitale tijdperk weer eens onder het stof vandaan te halen, waarin is voorgesteld een artikel aan de Grondwet toe te voegen dat stelt dat de overheid zorg moet dragen voor de toegankelijkheid van bij de overheid berustende informatie.[122] Een goede toegankelijke overheidsinformatievoorziening schept immers transparantie.

---

[120] Daniel J. Solove, Do Social Networks Bring the End of Privacy?, Scientific American, August 2008, <www.sciam.com/article.cfm?id=do-social-networks-bring>.
[121] Gluurstaat. De oorverdovende stilte rond privacy, Groene Amsterdammer, 13/2008.
[122] Rapport Commissie Grondrechten in het Digitale Tijdperk, Ministerie van BZK, 2001 (beschikbaar via Recht.nl, <recht.nl/1138>).

Voor wat betreft de toepasselijkheid van privacywet- en regelgeving is het duidelijk dat er een verschil is tussen het actief, vrijwillig aanmelden voor een dienst en de onvrijwillige confrontatie van de burger met een overheidsdienst. In het eerste geval zal een burger bereid zijn een stukje van zijn privacy op te geven in ruil voor deelname aan een systeem of dienst. De burger gebruikt de zelfbeschikking om zijn recht om met rust gelaten te worden in te perken. Daarbij speelt overigens de transparantie ook weer een belangrijke rol, omdat een burger immers pas inzicht heeft in de privacygevolgen van een systeem als dat klip en klaar wordt toegelicht door de (overheids)dienstverlener.

4. Arbeidsrecht

4.1 Recht op privacy op de (overheids)werkplek?

In het arrest van het Europese Hof voor de Rechten van de Mens (EHRM) inzake *Halford v. The United Kingdom* heeft het Hof uitdrukkelijk gezegd dat ook een werknemer op zijn werkplek een recht op privacy heeft. In de woorden van het Hof:

"*In the Court's view, it is clear from its case-law that telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 para. 1 (art. 8-1).*"

Het Hof verwijst in dit verband naar haar eerdere uitspraken in de zaken: *Klass and Others v. Germany* (judgment of 6 September 1978, Series A no. 28, p. 21, para. 41); *Malone v. the United Kingdom* (judgment of 2 August 1984, Series A no. 82, p. 30, para. 64); *Huvig v. France* (judgment of 24 April 1990, Series A no. 176-B, p. 41, para. 8, and p. 52, para. 25); en *Niemietz v. Germany* (judgment of 16 December 1992, Series A no. 251-B). Het is dus vaste rechtspraak van het EHRM dat een werknemer ook op zijn werkplek in beginsel een recht op privacy heeft. Dat geldt ook als de werkgever gebruik maakt van mogelijkheden om werknemers te lokaliseren, bijvoorbeeld door het wagenpark van het bedrijf uit te rusten met een GPS-systeem.

Het bestaan van een arbeidsverhouding brengt evenwel ook een beperking op de grondrechten van werknemers met zich mee. Deze beperking wordt veroorzaakt doordat er een gezagsverhouding bestaat tussen werknemer en werkgever. De werknemer is verplicht aanwijzingen van de werkgever op te volgen. Daardoor heeft de werknemer minder bewegings- en handelingsvrijheid en ook minder vrijheid van meningsuiting.[123] Dat geldt ook voor het recht op privacy. Door het betreden van de werkplek, verliest de werknemer een stukje van zijn privacy. Maar dat wil niet zeggen dat een werkgever de privacy van zijn werknemers helemaal niet hoeft te respecteren. Dat is immers bepaald in de bovengenoemde rechtspraak van het EHRM en volgt ook uit de algemene juridische (privaatrechtelijke) norm dat een werkgever zich als een goed werkgever dient te gedragen tegenover zijn werknemers (art. 7:611 Burgerlijk Wetboek (BW)).

In het rapport "Goed werken in netwerken" wijst het CBP er onder meer op dat wanneer een werkgever 'uiterlijke kenmerken' vastlegt van het communicatieverkeer van een werknemer, daar een *chilling effect* van uit gaat voor de communicatievrijheid van die werknemer.[124] Een zelfde *chilling effect*, maar dan voor de bewegingsvrijheid, kan het hebben als de werkgever de 'uiterlijke kenmerken' vastlegt van de verplaatsingen van een werknemer. Die 'uiterlijke kenmerken' hebben immers betrekking op de verkeersgegevens van de communicatie of de locatiegegevens van de eindapparatuur die in het bezit is van de werknemer.

4.2 Bescherming persoonsgegevens op de werkplek

Indien een werkgever persoonsgegevens van een werknemer verwerkt, waaronder locatiegegevens, dan is de werkgever eveneens gebonden aan de regels ter bescherming van persoonsgegevens. Dan gelden met name de voorwaarden van de WBP en van de Tw. Tevens kan de Wet op de ondernemingsraden van toepassing zijn.

---

[123] Goed werken in netwerken, College bescherming persoonsgegevens, Achtergrondstudies en verkenningen 21, 2002, p.20 (<www.cbpweb.nl> zoeken naar *netwerken*).
[124] Goed werken in netwerken, College bescherming persoonsgegevens, Achtergrondstudies en verkenningen 21, 2002, p.21 (<www.cbpweb.nl> zoeken naar *netwerken*).

Als locatiegegevens tevens persoonsgegevens zijn moet het verwerken daarvan voldoen aan de voorwaarden voor het mogen verwerken van persoonsgegevens. Deze voorwaarden zijn te vinden in de WBP en zijn beschreven in hoofdstuk 2.1.4.1.

Een van die voorwaarden, die bijvoorbeeld geldt wanneer een werkgever camera's op de werkplek wil inzetten, is dat de werknemers geïnformeerd moeten worden over (de mogelijkheid van) het gebruik van dergelijke middelen. Zo oordeelde de rechtbank Haarlem in 2006 dat een werkgever door middel van camera's zijn werknemers mag controleren als daartoe een noodzaak bestaat, zoals het doen stoppen van schadetoebrengend handelen (betalingen niet in de kassa gedeponeerd). In sommige gevallen is, aldus de rechtbank, zelfs het gebruik van verborgen camera's toegestaan, maar dan moeten de werknemers wel vooraf van in kennis zijn gesteld van deze mogelijkheid.[125] In dit geval had de werkgever aan deze voorwaarde voldaan door in de kassiersovereenkomst expliciet de mogelijkheid van controle via verborgen camera's op te nemen.

Een personeelsvolgsysteem waarbij bijvoorbeeld van GPS gebruik gemaakt wordt, kan door een werkgever voor diverse doeleinden worden ingezet.[126] Zo is het mogelijk om de dichtstbijzijnde werknemer te sturen naar een klant die een opdracht heeft. Maar het is ook mogelijk dat een werkgever de werknemer alleen maar wil controleren. Sommige werknemers zullen het een inbreuk op hun privacy vinden, anderen niet. Maar hoe dan ook, de werkgever zal zich aan de regels van de WBP moeten houden.

Voorts zal hij –indien van toepassing - rekening moeten houden met de Wet op de ondernemingsraden (WOR). Gezien het feit dat bij gebruik van een GPS-systeem om werknemers te volgen sprake is van een personeelsvolgsysteem, zal de ondernemingsraad daarmee moeten instemmen.

Een werkgever die een bedrijfsauto heeft uitgerust met een GPS-systeem kan daarmee controle uitoefenen op zijn werknemer. Dat geldt zeker als de werknemer weet dat er een GPS-systeem in de bedrijfsauto aanwezig is. Wanneer blijkt dat de uitdraaien van het GPS-systeem en de dagrapporten van de werknemer te zeer uiteenlopen, mag de werkgever de arbeidsovereenkomst met die werknemer zelfs ontbinden.[127]

Bij het gebruik van een GPS-systeem worden locatiegegevens verwerkt. Volgens de definitie in de Telecommunicatiewet (Tw) zijn dat: "gegevens die worden verwerkt in een elektronisch communicatienetwerk waarmee de geografische positie van de randapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven".[128] In het kader van de Telecommunicatiewet kan de werkgever worden beschouwd als de 'abonnee', die een elektronische communicatiedienst (het GPS-systeem) afneemt van een 'aanbieder' van een openbare elektronische communicatiedienst (netwerkoperator of dienstenleverancier).[129] De werknemer kan dan als de 'gebruiker' worden beschouwd. Een 'gebruiker' is: "een natuurlijke persoon die gebruik maakt van een openbare elektronische communicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd."[130]

Het verwerken van locatiegegevens over abonnees of gebruikers is slechts toegestaan als:

---

[125] Sector kanton Rechtbank Haarlem 24-05-2006 LJN: AX7687.
[126] Een voorbeeld van een systeem waarmee men voertuigen en dus mensen, kan volgen is GPS Buddy, <www.gps-buddy.com/site/NL/>.
[127] Exit-route via GPS?, D. Smits, Sprout Expertlog, 23 oktober 2006 (<www.expertlog.nl> zoeken naar *GPS*).
[128] Artikel 11.1, sub d, Telecommunicatiewet.
[129] Zie ook D. de Bot, S. Renette, Employee, where are thou? *Privacy & Informatie*, 2006/237, p. 212.
[130] Artikel 11.1, sub a, Tw.

- deze gegevens zijn geanonimiseerd; of
- de desbetreffende abonnee of gebruiker voor de verwerking van deze gegevens toestemming heeft gegeven ten behoeve van de levering van een dienst met toegevoegde waarde;[131]
- de abonnee of gebruiker voorafgaand aan het verkrijgen van die toestemming door de aanbieder is geïnformeerd over:
    - de soort locatiegegevens die zullen worden verwerkt;
    - de doeleinden waarvoor de locatiegegevens worden verwerkt;
    - de duur van de verwerking; en
    - of de gegevens aan een derde zullen worden verstrekt ten behoeve van de levering van de dienst met toegevoegde waarde;
- de verwerking van locatiegegevens noodzakelijk is voor de levering van de dienst met toegevoegde waarde;
- de aanbieder aan de abonnee of gebruiker wiens gegevens worden verwerkt de mogelijkheid aanbiedt om kosteloos en op eenvoudige wijze de verwerking van diens gegevens tijdelijk te beletten voor elke overbrenging van communicatie of elke verbinding met het openbare elektronische communicatienetwerk dat wordt gebruikt voor de levering van de dienst;
- de verwerking van de gegevens slechts plaats vindt door personen die werkzaam zijn onder het gezag van de aanbieder of de derde en is beperkt tot de gegevens die noodzakelijk zijn om de dienst te kunnen aanbieden.

Een abonnee of gebruiker heeft het recht om de verleende toestemming voor de verwerking van hem betreffende gegevens op elk moment weer in te trekken.[132] Dit recht bestaat voor persoonsgegevens ook op grond van art. 5, lid 2, WBP. Of de toestemming van de abonnee of van de gebruiker moet worden verkregen, hangt af van de te verwerken gegevens, van de aard van toegevoegde waarde dienst en van de technische procedurele en contractuele mogelijkheden om onderscheid te maken tussen de persoon die gebruik maakt van de dienst (de gebruiker) en degene die daarvoor de overeenkomst heeft afgesloten (de abonnee).[133]

Een 'dienst met toegevoegde waarde' is: "een dienst die de verwerking vereist van verkeersgegevens of locatiegegevens, niet zijnde verkeersgegevens, en die verder gaan dan hetgeen noodzakelijk is voor de overbrenging van een communicatie of de facturering daarvan."[134] Een aparte regeling voor locatiegegevens die geen verkeersgegevens zijn wordt wenselijk geacht omdat locatiegegevens veel nauwkeuriger iemands locatie kunnen bepalen dan verkeersgegevens. Verkeersgegevens worden verkregen uit netwerkcellen die veelal honderden meters bestrijken. GPS-systemen kunnen gebruikers met een nauwkeurigheid van een tiental meters vaststellen. Aldus geven locatiegegevens veel meer inzicht in de exacte locatie van (het randapparaat van) een gebruiker. Bovendien kan een gebruiker gemakkelijk 'in real time' worden gevolgd. Daarom worden aan de verwerking van locatiegegevens strengere eisen gesteld.[135]

Na toestemming van de abonnee of gebruiker, is de verwerking van locatiegegevens slechts toegestaan voor zover en voor zolang dat noodzakelijk is voor de levering van de toegevoegde waarde dienst. Daarna mogen de gegevens alleen nog worden gebruikt voor het opstellen van een factuur. In praktijk betekent dit ten hoogste 5 jaar, te weten tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden

[131] Artikel 11.5a, lid 1, Tw.
[132] Artikel 11.5a, lid 4, Tw.
[133] *Kamerstukken II* 2003/04, 28 851, nr. 3, p. 157 (MvT). Zie ook G.J. Zwenne 2005, (*T&C Telecommunicatierecht*), art. 11.5a Tw, aant. 2.
[134] Artikel 11.5, sub h, Tw.
[135] *Kamerstukken II* 2003/04, 28 851, nr. 3, p. 157 (MvT). Zie ook G.J. Zwenne 2005, (*T&C Telecommunicatierecht*), art. 11.5a Tw, aant. 1.

afgedwongen.[136] Zodra de factuur echter betaald is en er daarover geen geschillen ontstaan moeten de locatiegegevens (tevens verkeersgegevens) worden verwijderd of geanonimiseerd.[137]

De abonnee of gebruiker moet worden gewezen op de mogelijkheid om kosteloos en op eenvoudige wijze de verwerking van diens gegevens tijdelijk te beletten. Dit laat echter onverlet dat de gegevens altijd moeten worden verstrekt aan de aangewezen beheerders van een alarmnummer voor publieke diensten als er communicatie over een dergelijk alarmnummer wordt afgewikkeld. Dat geldt ook als de abonnee of gebruiker de verwerking van de locatiegegevens tijdelijk heeft belet.[138]

De aanbieders mogen de hier beschreven regels voor de locatiegegevens buiten toepassing laten als dat in het belang is van de nationale veiligheid of ter voorkoming, opsporing en vervolging van strafbare feiten. In dat geval kunnen de aanbieders desgevraagd voldoen aan de vorderingen van politie en justitie tot verstrekking van locatiegegevens op grond van art. 126n of 126u Sv. Tevens mogen de aanbieders locatiegegevens verwerken als dat nodig is voor een onderzoek naar hinderlijke en kwaadwillige oproepen, zoals bedoeld in artikel 11.11, lid 4 en 5, Tw.[139]

Omdat locatiegegevens, voor zover die niet zijn geanonimiseerd, tevens persoonsgegevens zijn, is naast de (bijzondere) Telecommunicatiewet ook de (algemene) Wet bescherming persoonsgegevens van toepassing op de verwerking daarvan. Voor zaken die niet in de Telecommunicatiewet zijn geregeld, zoals het inzagerecht, gelden de regels uit de WBP. Voorts dient de verwerking van locatiegegevens die tevens persoonsgegevens zijn in overeenstemming te zijn met de voorwaarden voor rechtmatige verwerking van persoonsgegevens uit de WBP. Een werkgever (abonnee) die een geolocalisatiedienst afneemt van een aanbieder (operator) moet nagaan of deze aanbieder de regels van de Telecommunicatiewet wel naleeft. Anders loopt de werkgever het risico dat de verwerking van persoonsgegevens onrechtmatig is en dan geldt dat ook voor de verdere verwerking (het gebruik) van die persoonsgegevens door de werkgever, bijvoorbeeld gericht op het treffen van maatregelen jegens een of meer werknemers.[140]

Locatiegegevens van werknemers kunnen worden verwerkt door de (netwerk)operator, de aanbieder van de toegevoegde waarde dienst en door de werkgever. Deze kunnen allen dezelfde locatiegegevens verwerken, maar dat kan telkens voor andere doeleinden zijn.
De netwerkoperator verwerkt locatiegegevens om de communicatie tot stand te brengen. Daartoe sluit hij een overeenkomst met de werkgever (abonnee) die vervolgens de eindapparatuur aan de werknemer (gebruiker) ter beschikking stelt. Vervolgens worden de locatiegegevens daarna gebruikt voor de plaatsbepaling van de werknemer. De locatiegebonden toegevoegde waarde dienst kan dan worden aangeboden door diezelfde operator of door een specifieke aanbieder van deze dienst, die daarbij gebruik maakt van de locatiegegevens die hem door de operator zijn verstrekt. Dezelfde gegevens kunnen door de werkgever van de operator of van de dienstenaanbieder worden ontvangen om de werknemer te kunnen volgen. De locatiegegevens kunnen dus worden verstrekt door de operator aan de werkgever, eventueel door tussenkomst van de dienstenaanbieder. Dergelijke verstrekkingen zijn verwerkingen van persoonsgegevens zoals bedoeld in de WBP en de Tw en zijn dus slechts toegestaan als de voorwaarden van beide wetten dat toelaten.[141]

[136] Artikel 3:307 e.v. BW.
[137] *Kamerstukken II* 2003/04, 28 851, nr. 3, p. 155 en 157-158 (MvT). Zie ook G.J. Zwenne 2005, (*T&C Telecommunicatierecht*), art. 11.5, aant. 3a en art. 11.5a Tw, aant. 4.
[138] G.J. Zwenne 2005, (*T&C Telecommunicatierecht*), art. 11.5a, aant. 6 en art. 11.10 Tw, aant. 3.
[139] G.J. Zwenne 2005, (*T&C Telecommunicatierecht*), art. 11.5a, aant. 8 en art. 11.13 Tw, aant. 2.
[140] D. de Bot, S. Renette, Employee, where are thou? *Privacy & Informatie*, 2006/237, p. 213.
[141] Vgl. D. de Bot, S. Renette, Employee, where are thou? *Privacy & Informatie*, 2006/237, p. 214.

4.3 Personeelsvolgsystemen, geo-informatie en privacy

Personeelsvolgsystemen – ook personeelsinformatiesystemen genoemd – kunnen worden gedefinieerd als "een doorgaans geautomatiseerd systeem waarin individuele en geaggregeerde gegevens van en over werknemers worden vastgelegd en dat als doel heeft 1) het ondersteunen van beslissingen ten aanzien van individuele werknemers en/of 2) het verschaffen van informatie met het oog op het voeren van een doelmatig en efficiënt personeelsbeleid en personeelsmanagement.[142]

Een voorbeeld van een dergelijk systeem is een zogenaamd voertuigvolgsysteem. In dit soort systemen kunnen de mogelijkheden van GPS, mobiele telefonie en het internet, gecombineerd worden waardoor een werkgever kan volgen waar zijn voertuigen zijn en/of waren. Vanzelfsprekend wordt bij dit soort toepassingen geo-informatie verwerkt. Het doel van dergelijke systemen is immers onder meer een werknemer, op basis van de locatie waar hij zich bevindt, naar een volgende werkplek te kunnen sturen.

Een ander soort volgsysteem dat in de toekomst wellicht gebruikt zou kunnen gaan worden is een systeem dat gebruik makend van radio frequency identification (RFID)[143] werknemers binnen een gebouw volgt. Het betreft hier dan als het ware lokale geo-informatie.

RFID is in dergelijke gevallen een technologie die gebruikt wordt in een personeelsvolgsysteem, dat verglijkbaar is met het gebruik van bewakingscamera´s in een gebouw. Het gebruik van RFID-technologie binnen een personeelsvolgsysteem vergemakkelijkt echter veelal het verzamelen en verwerken van gegevens over de werknemers. Het gebruik van RFID brengt daarmee een kwantitatief en – vanuit de optiek van de werkgever bezien ook - een kwalitatief verschil met zich mee ten opzichte van bewaking met camera´s. Zo kunnen met behulp van wat men noemt ‘active badge monitoring’ door middel van elektronische ogen (RFID-readers) en badges werknemers door het hele gebouw worden gevolgd en kunnen dus de tijdstippen waarop de werknemer een bepaalde reader passeert direct worden opgeslagen in een achterliggende database.[144]

In het geval van voertuigvolgsystemen en van RFID-systemen die werknemers kunnen volgen is sprake van geo-informatie. In het geval van voertuigvolgsystemen kunnen voertuigen, en dus werknemers, gevolgd worden die zich in een zekere regio (nationaal, internationaal) voortbewegen, in het geval van systemen waarbij gebruik gemaakt wordt van RFID kunnen dit personen zijn die zich binnen een gebouw of een gebouwenterrein verplaatsen. Beide systemen hebben een invloed op privacy.

Recht om met rust gelaten te worden
Bij personeelsvolgsystemen gaat het om arbeidsrechtelijke verhoudingen, om verhoudingen tussen private partijen. Daarbij dient de vraag aan de orde te komen of in die verhoudingen grondrechten zoals het recht op de persoonlijke levenssfeer (artikel 8 EVRM en artikel 10 Grondwet) van toepassing zijn, of er sprake is van de zogenaamde toepassingen van horizontale werking van grondrechten.[145] In het arrest waarin een Edamse bijstandsmoeder werd bespied door een buurman heeft de Hoge Raad bepaald dat dit het geval kan zijn.[146] Echter alleen indien een inbreuk van de ene burger op het grondrecht van de ander nodig is in een democratische samenleving ten behoeve van het algemeen belang. Burgerplicht en private

[142] Personeelsinformatiesystemen en privacybescherming, Drs. J.H.J. Terstegge <home.planet.nl/~privacy1/pis2107.htm>.
[143] Radio frequency identification, Wikipedia, <nl.wikipedia.org/wiki/RFID>.
[144] Werknemers en RFID, Jessica Verwer. In: Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen, NVvIR, 2005, <www.nvvir.nl/doc/rfid-tekst.pdf>.
[145] Grondrechten (Nederland), Wikipedia <nl.wikipedia.org/wiki/Grondrechten_(Nederland)>.
[146] HR 9 januari 1989, nr 12717, NJ, 1987, 928; AB, 1987, 231 (Edamse Bijstandsmoeder).

grondrechtenbescherming worden hiermee als het ware aan elkaar gekoppeld.[147] In het geval van de verhouding tussen werkgever en werknemer inzake een personeelsvolgsysteem zouden het genoemde grondrecht dus een rol kunnen spelen.[148]

Bescherming persoonsgegevens
Ook de WBP is van toepassing. Het gaat hier immers om identificeerbare personen. Een voertuig wordt gevolgd, maar de werkgever weet welke werknemer in een voertuig behoort te zitten. Net zoals een werkgever weet welke badge behoort bij welke werknemer. Met andere woorden het kost degene die verantwoordelijk is voor de persoonsgegevens geen moeite de identiteit van de betrokken werknemers te identificeren. Derhalve zijn de materiële normen van toepassing.

Een andere vraag die zich aandient in het kader van de WBP is of de verwerking van de gegevens in een personeelsvolgsysteem aangemeld dient te worden bij het College bescherming persoonsgegevens zoals gesteld in artikel 27 van de WBP. Een dergelijke melding heeft tot doel de transparantie van de gegevensverwerking te bevorderen en maakt dat de afweging van de belangen van verantwoordelijke en betrokkenen tot op zekere hoogte inzichtelijk en controleerbaar zijn.

Voor de werkgever-werknemerverhoudingen is vooral artikel 7 Vb van belang. Daarin staat de vrijstelling voor verwerkingen in het kader van de personeelsadministratie betreffende personen in dienst van of werkzaam ten behoeve van de verantwoordelijke,
voorzover de verwerking slechts geschiedt voor (onder andere) de interne controle en de bedrijfsbeveiliging. Van deze vrijstelling kan evenwel alleen gebruik worden gemaakt als er een betrekkelijk beperkt aantal soorten van gegevens worden verzameld en verwerkt. Als gevolg daarvan zal een personeelsvolgsysteem niet snel vallen onder de vrijstelling, zodat het zal moeten worden gemeld bij het College bescherming persoonsgegevens.[149]

4.4 Conclusie arbeidsrecht

Werknemers hebben volgens vaste rechtspraak een recht op privacy. Aan de andere kant brengt het bestaan van een arbeidsverhouding ook een beperking op de grondrechten van werknemers met zich mee. Deze beperking wordt veroorzaakt doordat er een gezagsverhouding bestaat tussen werknemer en werkgever.

Dat betekent dat er niet te pas en te onpas gebruik gemaakt mag worden van bijvoorbeeld personeelsvolgsystemen waarbij locatiegegevens – geo-informatie – over werknemers worden opgeslagen. Dat is al helemaal niet het geval indien de Wet op de ondernemingsraden van toepassing is. Dan zal namelijk de ondernemingsraad toestemming moeten geven tot het gebruik van het personeelsvolgsysteem.

In die gevallen dat personeelsvolgsystemen worden ingezet, waarbij gegevens als locatiegegevens – geo-informatie- verwerkt worden, kunnen bovendien de regels van Wet bescherming persoonsgegevens en de Telecommunicatiewet van toepassing zijn. Een werkgever

[147] Voetangels en klemmen: de horizontale werking van burger- en politieke rechten, Leonard F.M. Besselink. In: Cees Flinterman en Willem van Genugten (eds), Niet-statelijke actoren en de rechten van de mens; gevestigde waarden, nieuwe wegen, Den Haag: Boom juridische uitgevers, 2003.
[148] Werknemers en RFID, Jessica Verwer. In: Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen, NVvIR, 2005, p.74, <www.nvvir.nl/doc/rfid-tekst.pdf>.

[149] Werknemers en RFID, Jessica Verwer. In: Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen, NVvIR, 2005, p.76, <www.nvvir.nl/doc/rfid-tekst.pdf>.

die een geolocalisatiedienst afneemt van een aanbieder moet nagaan of deze aanbieder de regels naleeft. Anders loopt de werkgever het risico dat de verwerking van persoonsgegevens onrechtmatig is en dan geldt dat ook voor de verdere verwerking (het gebruik) van die persoonsgegevens door de werkgever, bijvoorbeeld gericht op het treffen van maatregelen jegens een of meer werknemers.

5. Openbaarheid / hergebruik

5.1 Inleiding[150]

Voor de ontwikkeling van met name geo-informatiesystemen is het vanzelfsprekend dat men over kaarten en aanverwante gegevens dient te beschikken. Veel van dit soort informatie wordt geproduceerd en beheerd door overheidsdiensten. Voor commerciële partijen is het dus van belang te weten of en waar deze informatie beschikbaar is, zodat zij met dat materiaal diensten kunnen ontwikkelen die vervolgens weer door de overheid, het bedrijfsleven of particulieren gebruikt kunnen worden.[151]

Er is een aantal mogelijkheden voor dienstenaanbieders om die ontsluiting te realiseren. In dit hoofdstuk wordt aandacht besteed aan de Richtlijn hergebruik overheidsinformatie, de (nieuwe) Wet openbaarheid bestuur (Wob), de mogelijkheid tot het sluiten van convenanten, en het voorontwerp Algemene wet overheidsinformatie. Daar waar relevant zal de Auteurswet aan de orde komen.

Alvorens deze regelingen de revue te laten passeren wordt kort een aantal notities besproken in het licht van de ontsluiting van geo-informatie.

5.2 Notities inzake de ontsluiting van overheidsinformatie

Naar toegankelijk van overheidsinformatie

Het begon eigenlijk allemaal in 1997 met de nota *Naar toegankelijk van overheidsinformatie*[152], een stuk van het ministerie van Binnenlandse Zaken (toen nog zonder Koninkrijksrelaties) waarin het beleidskader werd geschetst voor het vergroten van de toegankelijkheid van overheidsinformatie met informatie- en communicatietechnologie.[153] Vertrekpunt vormde het bestaande algemene kader voor de openbaarheid van overheidsinformatie en daarbij bevatte de nota twee hoofdpunten. Ten eerste de toepassing van ICT bij het verstrekken van openbare overheidsinformatie met het oog op het vergroten van de betrokkenheid van de burger bij het democratisch proces. Ten tweede de mogelijkheden tot exploitatie van elektronische gegevensbestanden door de particuliere sector om voor het bedrijfsleven nieuwe kansen te creëren. Het is duidelijk dat de ontsluiting van bestanden met geo-informatie voor dienstverleners betrekking heeft op het tweede punt.

Geo-informatie

Aan geo-informatie werd in de nota *Naar toegankelijkheid van overheidsinformatie* geen specifieke aandacht besteed. Er werd wel opgemerkt dat er overheidsorganen zijn die geografische gegevens verkopen. Tevens werd aangegeven dat inzake enkele geo-

---

[150] Zie voor informatie over hergebruik van geo-informatie: Leo van der Wees, Wees, Geo-infomatie, de WOB en hergebruik. In: Leo van der Wees, Sjaak Nouwt (red.), *Recht en locatie*, Nederlandse Vereniging voor Informatietechnologie en Recht, Den Haag: Elsevier Juridisch, 2008.

[151] Zie de eerder genoemde voorbeelden inzake het gebruik door de overheid van Google Maps bij klachten (Amsterdam, stadsdeel Geuzenveld-Slotermeer) en Procedures Online (Nijmegen). Bedrijfsleven en particulieren maken veelvuldig gebruik van navigatiesystemen als TomTom.

[152] *Kamerstukken II* 1996-1997, 20644, nr. 30, Informatievoorziening openbare sector; Brief staatssecretaris met nota 'Naar toegankelijkheid van overheidsinformatie'

[153] Tijdens een ePSIplus-bijeenkomst in Utrecht op 27 september 2007 is een overzicht gepresenteerd van beleidsinitiatieven inzake hergebruik van overheidsinformatie. Zie <www.epsiplus.net>, zoek naar *Netherlands National meeting presentations* en scroll naar die tekst op de dan getoonde pagina.

informatieverwerkende diensten, zoals het Kadaster en het KNMI, toestemming was gegeven nevenactiviteiten op de markt te verrichten. Daar bleef het evenwel bij.

Beleidslijn Naar optimale beschikbaarheid van overheidsinformatie[154]
Zo´n drie jaar na de hiervoor genoemde nota verscheen de Beleidslijn *Naar optimale beschikbaarheid van overheidsinformatie* van de Minister voor Grote Steden- en Integratiebeleid. Deze beleidslijn borduurt voort op de nota en noemt dan ook dezelfde twee hoofdpunten inzake de participatie van de burger aan het democratisch proces en de ontsluiting van overheidsbestanden om voor het bedrijfsleven nieuwe kansen te creëren.
Wel wordt in de beleidslijn – in tegenstelling tot in de eerder besproken nota – gewezen op het feit dat overheidsorganen, anders dan in de papieren situatie, massaal het auteursrecht en het databankenrecht op hun elektronische gegevensbestanden voorbehouden.[155] Dit wordt in twee opzichten onwenselijk geacht. Burgers en bedrijven kunnen daardoor de informatie wel krijgen maar mogen deze vervolgens zonder expliciete toestemming niet naar eigen inzicht hergebruiken, hetgeen volgens de beleidslijn in strijd lijkt met de geest van de Wob. Tevens zijn de voorbehouden ongewenst omdat in de kenniseconomie de maatschappelijke waarde van informatie groter wordt naarmate meer mensen deze gebruiken. De voorbehouden staan daaraan in de weg.

Geo-informatie
Het woord geo-informatie komt in de beleidslijn slechts één keer voor. Bijna aan het einde van beleidslijn wordt aangestipt dat vanuit de geo-informatiesector aandacht is gevraagd voor het risico dat bij een strakke wettelijke regeling van de prijs, negatieve gevolgen zouden kunnen optreden voor de kwaliteit van bestanden of de serviceverlening bij informatieverstrekking door de overheid. Dat is een interessante constatering en een terechte zorg.

Naar ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie[156]
In 2002 volgde het rapport *Naar ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie* gemaakt in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en reeds aangekondigd in de voornoemde beleidslijn. Dit rapport vormde de weerslag van een verkennend onderzoek naar de mogelijke inhoud van een Wet gebruiksrechten overheidsinformatie. Daarbij is gefocust op drie kernelementen: het doel, de normstelling en de reikwijdte.
De regeling zou tot doel moeten hebben het gebruik van overheidsinformatie door burgers, andere overheden en het bedrijfsleven te bevorderen. Daarbij zou de normstelling er primair op gericht moeten zijn dat overheden bij het beschikbaar stellen van informatie ten hoogste de *kosten van de verstrekking* in rekening zouden mogen brengen en dat zij als rechthebbende van informatie geen gebruiksbeperkingen meer aan derden zouden mogen opleggen, althans niet om hun informatie te kunnen exploiteren. Hooguit zouden aan het gebruik door derden nog voorwaarden mogen worden gesteld ter bescherming van publieke belangen. Zoveel was al min of meer duidelijk geworden uit de beleidslijn. Het onderzoek spitste zich dan ook vooral toe op de reikwijdte van een op te stellen regeling: op welke overheidsinformatie zou een Wet gebruiksrechten overheidsinformatie betrekking moeten hebben?
Dit leidde uiteindelijk tot het volgende: het verstrekkingskostenregime zou moeten gaan gelden voor aan derden verstrekte informatie die totstandgebracht wordt in het kader van de bestuurstaak, waarbij de vestrekking aan die derde niet voortvloeit uit die taak.

---

[154] Beleidslijn 'Naar optimale beschikbaarheid van overheidsinformatie' + standpunt advies commissie auteursrecht, *Kamerstukken II* 1999-2000, 26387, nr. 7. De beleidslijn is ook toegankelijk op Recht.nl, <www.recht.nl/doc/kst26387-7.pdf>.
[155] Elektronische bestanden van het bestuur, BDO Consultants, Groningen 1998 in opdracht van het ministerie van Binnenlandse Zaken.
[156] Het rapport *Naar ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie* is beschikbaar op Recht.nl, <recht.nl/12166>.

Vervolgens hebben de onderzoekers met deze bevindingen in het achterhoofd de Wob geanalyseerd, met name met het oog op de verstrekking van de bovengenoemde informatie. Op basis hiervan kwamen zij tot de conclusie dat de regeling genoemd in de beleidslijn zou moeten worden opgenomen in de Wob, waarbij deze wel aangepast zou moeten worden. Was het doel van deze wet openheid en openbaarheid van het bestuur met het oog op "een goede en democratische bestuursvoering", na aanpassing zou deze ook gericht moeten op een vrij gebruik van informatie van bestuursorganen.

Geo-informatie
In dit rapport wordt, in tegenstelling tot de eerder besproken notities, iets meer aandacht besteed aan geo-informatie. Zo schrijven de onderzoekers dat het bedrijfsleven in het bijzonder interesse heeft voor geo-informatie en zij vinden dan ook dat de overheid in ieder geval systematisch bekend zou moeten maken welke geo-informatie beschikbaar is.[157] Dit zou dan ook een van de winstpunten van de verruimde Wob moeten zijn: eenmaal verstrekte gegevens moeten op internet geplaatst en actueel gehouden worden. Zo zou een ingenieursbureau dat incidenteel informatie nodig heeft over de bodemgesteldheid of een aannemer die snel wil nagaan waar kabels en leidingen liggen in de directe omgeving van een uit te voeren werk makkelijk en te allen tijde eenvoudig over actuele gegevens moeten kunnen beschikken.

De verruimde Wob heeft evenwel ook nadelen en een daarvan zou met name betrekking kunnen hebben op geo-informatie aldus de onderzoekers in het rapport. De vernieuwde wet zou namelijk wel eens financiële problemen kunnen veroorzaken voor bestuursorganen die bestanden zodanig intensief exploiteren dat de aanleg- en beheerskosten daarvan in belangrijke mate worden opgebracht door externe afnemers. Als nu deze afnemers in de toekomst slechts verstrekkingskosten moeten gaan betalen, dan zou het zou het wegvallen van de (substantiële) bijdragen van derden in de kosten er toe kunnen leiden dat de financiële basis aan deze bestanden ontvalt, zodat ze zouden verdwijnen. Dit zou zich hoofdzakelijk of zelfs uitsluitend voordoen bij geo-informatie.

Vraag die daarbij uiteraard aan de orde kwam, is wat de plaats zou worden van geo-informatie in de verruimde Wob. Was het geschetste gevaar inderdaad reëel? Dat leek inderdaad het geval, maar zou weggenomen kunnen worden door gegevensverstrekking uit de geografische (basis)registraties als een bestuurstaak aan te merken waardoor maximaal de integrale kosten van de informatie in rekening gebracht mogen gaan worden en de geo-informatie niet valt onder (het verstrekkingsregime van) de verruimde Wob.

Dit zou volgens de onderzoekers overigens niet betekenen dat een verruimde Wob helemaal geen betekenis meer zou kunnen hebben voor de beschikbaarheid van geografische bestanden. Bestanden van andere bestuursorganen die geheel of gedeeltelijk zijn gebaseerd op geografische (basis)registraties zouden mogelijk nog steeds onder een verruimde Wob opvraagbaar zijn.

Andere notities
Na *Naar ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie* is nog een aantal notities verschenen, maar deze zijn van minder belang of voegen niet veel relevante zaken toe om ook besproken te worden in het kader van dit onderzoek. De belangrijkste daarvan zijn:

- Wob & ICT. Onderzoek naar de gevolgen van toepassing van Informatie- en Communicatietechnologie voor de Wet openbaarheid van bestuur, J.P.R. Bergfeld, H.W.K. Kaspersen & A.R. Lodder, Vrije Universiteit Amsterdam in opdracht van het ministerie van BZK (beschikbaar op <www.minbzk.nl>, zoeken naar *Bergfeld*, en vervolgens klikken op *evaluatie wob ict).*

[157] De onderzoekers verwijzen daarbij als voorbeeld naar de website van het Britse Office of Public Sector Information, <www.opsi.gov.uk>.

- In dienst van de democratie: het rapport van de Commissie Toekomst Overheidscommunicatie (beschikbaar op <www.minaz.nl>, zoeken naar *In dienst van de democratie*, en vervolgens klikken op Commissie Wallage).
- Burger en overheid in de informatiesamenleving / De noodzaak van institutionele innovatie, Commissie Docters van Leeuwen (beschikbaar op <www.minbzk.nl>, zoeken naar *institutionele innovatie*, en klikken op Burger en overheid in de informatiesamenleving. De noodzaak van institutionele innovatie).
- Over wetten en praktische bezwaren. Een evaluatie en toekomstvisie op de Wet openbaarheid van bestuur, Universiteit van Tilburg in opdracht van het ministerie van BZK (beschikbaar op <recht.nl/17740>).

5.3 Richtlijn hergebruik overheidsinformatie

In het vorige hoofdstuk is in grote lijnen de ontwikkeling beschreven van de toegankelijkheid van overheidsinformatie. Drijfveer achter deze ontwikkeling waren niet alleen nationale gedachten over de ontsluiting van overheidsinformatie zoals hiervoor geschetst, maar tevens het Europese beleid inzake het hergebruik van dit soort informatie.

In 1999 is in de Europese Unie de toon gezet met de publicatie van een groenboek over overheidsinformatie in de informatiemaatschappij.[158] Een groenboek dat de voorbode was voor de richtlijn hergebruik overheidsinformatie, die in 2003 het licht zag. Een richtlijn waarin een minimumpakket aan voorschriften is vastgelegd voor het hergebruik en de concrete middelen ter vereenvoudiging van het hergebruik van bestaande documenten die in het bezit zijn van openbare lichamen van de lidstaten.

Over geo-informatie wordt in de richtlijn alleen vermeld dat deze door de overheid wordt verzameld, geproduceerd, vermenigvuldigd en verspreid. De richtlijn heeft dan ook niet geleid tot specifieke voor geo-informatie opgestelde bepalingen. De richtlijn heeft ook niets aan het plan gewijzigd dat reeds in het rapport *Naar ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie* werd aangekondigd om het hergebruik van overheidsinformatie te regelen in een verruimde Wob.

Een plan waar overigens niet iedereen even enthousiast over was. Zo stelde Marc de Vries in het Nederlands Juristenblad dat de keuze van de wetgever voor implementatie van de richtlijn in de Wet openbaarheid van bestuur (Wob) een verkeerde is. De richtlijn zou zich met name richten op overheidsinformatie die economisch potentieel heeft. De Wob zou evenwel niet van toepassing zijn op sommige van deze commercieel aantrekkelijke bestanden. Tevens stelde De Vries dat de Wob openbaarheid beoogt te scheppen ten behoeve van een goede en democratische bestuursvoering en dat deze dus geen economische doelen zou kennen. Hij concludeerde uiteindelijk zelfs dat doordat er was gekozen de richtlijn via de Wob te implementeren en het bereik van de Wob niet aan te passen, Nederland in feite niet aan haar verplichting tot implementatie voldoet, met alle mogelijke gevolgen van dien.[159]

Ook Mireille van Eechoud vond de keuze voor de Wob ter implementatie van de Richtlijn hergebruik overheidsinformatie een bijzondere. Zij stelde in Mediaforum dat herhaaldelijk is benadrukt dat de Richtlijn juist níet gaat over openbaarheid van overheidsinformatie, onder meer omdat het niet tot de competentie van de EU maar tot die van de lidstaten behoort. Door implementatie in de Wob, legt de regering een (te) nauw verband tussen toegang tot overheidsinformatie uit het oogpunt van democratische controle en ter exploitatie.

---

[158] Overheidsinformatie: een essentiële hulpbron voor Europa - Groenboek over overheidsinformatie in de informatiemaatschappij, COM(98) 585 (beschikbaar op <ftp.cordis.lu/pub/econtent/docs/gp_nl.pdf>).
[159] M. de Vries, Implementatie van de EU-Richtlijn hergebruik overheidsinformatie in de Wob, NJB, 2005/39.

Een andere reden waarom Van Eechoud vond dat implementatie van de richtlijn in de Wob niet voor de hand ligt, is dat de overheidsinformatie die voor het bedrijfsleven interessant is om te exploiteren, doorgaans berust bij overheidsorganen waarvoor de Wob (deels) niet geldt. Uit Europese en nationale onderzoeken zou blijken dat met name registerinformatie, meteorologische data, verkeersinformatie en allerhande digitale kaarten gewilde overheidsinformatie is. Voor het Kadaster, het KNMI, en dergelijke gelden echter aparte openbaarheidsregels. Wel stelde zij dat weliswaar de hergebruikprocedure ingevolge art. 1 van de nieuwe Wob ook zou gaan gelden voor informatie die openbaar is op grond van de Wob of een andere wet, maar of de hergebruikprocedure zoals die voor de Wob is geformuleerd ook past in de stelsels van al die bijzondere wetten heeft Van Eechoud niet kunnen achterhalen.[160]

Bastiaan van Loenen op zijn beurt stelde dat Marc de Vries gelijk heeft op het punt dat de Wob niet beoogt het hergebruik van overheidsinformatie te bevorderen. Maar dat door implementatie van de Richtlijn in de Wob juist bestanden met economisch potentieel niet worden bereikt, en daarmee suggererend dat ze niet zouden voldoen aan het bepaalde in de richtlijn, is onjuist volgens Van Loenen. Doordat sommige essentiële bepalingen van de richtlijn namelijk zo breed zijn geformuleerd, wordt daar in Nederland in zeer grote mate nu al aan voldaan. De gegevens van bijvoorbeeld het Kadaster zijn voor een ieder toegankelijk en mogen onder bepaalde voorwaarden worden hergebruikt. Het Kadaster zou slechts op details haar werkwijze moeten aanpassen om aan de bepalingen van de richtlijn te voldoen, aldus Van Loenen.

Daarnaast stelde hij dat de implementatie van de Europese richtlijn in de Wob of op een andere wijze irrelevant is voor de nationale discussie. De implementatie was al zo goed als rond. Wel wees Van Loenen op de evaluatie van de richtlijn in 2008 en achtte hij het van belang in dat kader de ontwikkelingen rond het hergebruik en het gebruik van de Wob daarbij, goed te blijven volgen.[161]

5.4 Wet openbaarheid bestuur

Gezien het feit dat implementatie van de richtlijn in de Wob inmiddels een feit is – de verruimde Wob is januari 2006 in werking getreden – zal ook hier op de juistheid van die keuze niet worden ingegaan. Wel zullen in het kort enkele opmerkingen over de nieuwe verruimde Wet openbaarheid van bestuur worden gemaakt en dan met name betreffende bepalingen die kwesties regelen die in het voorafgaande ook aan de orde zijn gekomen.

Hergebruik
In het eerder besproken rapport *Naar ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie* werd de keuze gemaakt voor de Wob om het hergebruik van overheidsinformatie wettelijk te regelen. De redenen daarvoor zijn terug te vinden in de memorie van toelichting bij de verruimde Wob. Zo is de Wob een wet waarin een algemeen openbaarheidsregime is neergelegd voor bestuursorganen en daarbij ligt de procedure voor hergebruik dicht tegen de openbaarheid van overheidsinformatie aan. En informatie kan slechts worden hergebruikt, indien het informatie betreft die openbaar is, en meestal zal dit gaan om informatie die openbaar is op grond van de Wob, aldus de memorie van toelichting.[162]
Voor de procedure voor hergebruik is dus aansluiting gezocht bij de procedure die reeds geldt voor een Wob-verzoek. Hiervoor is gekozen om de praktische afhandeling van een hergebruikverzoek zo eenvoudig mogelijk te maken en overheidsorganen niet op te zadelen met twee verschillende procedures met bijvoorbeeld verschillende behandelingstermijnen of wijzen

[160] M. van Eechoud, Vreemde bedgenoten: de Wob en de Richtlijn hergebruik overheidsinformatie, Mediaforum 2005-9, p. 291. Ook beschikbaar op <www.ivir.nl/publicaties/eechoud/mf_2005_9.html>.
[161] B. van Loenen, Implementatie van de EU-Richtlijn hergebruik overheidsinformatie, NJB, 2005/304.
[162] *Kamerstukken II* 2004-2005, 30188, nr. 3, p.5.

waarop een verzoek moet worden ingediend. Ook vanuit gebruikersoogpunt werd het wenselijk geacht dat de openbaarheidsprocedure en de hergebruikprocedure in dezelfde wet zijn neergelegd.
Geen vreemde gedachten, maar een wijziging van de naam van de wet in iets als *Wet openbaarheid en hergebruik van overheidsinformatie* zou mogelijk wel voor meer duidelijkheid hebben gezorgd. Verwarrend blijft dat de oorspronkelijke Wob betrekking had op bestuurlijke informatie en dat het hergebruik, zoals de memorie van toelichting ook aangeeft, ook betrekking heeft op informatie die geen bestuurlijke aangelegenheid is. Voordeel is weer dat doordat de procedures dicht tegen elkaar aan liggen, het zo kan zijn dat een niet-bestuursorgaan een verzoek om hergebruik kan doorsluizen naar een bestuursorgaan dat de gevraagde informatie ook heeft.[163] Aannemende dat zo´n bestuursorgaan vaker met Wobverzoeken te maken heeft, kan een dergelijk orgaan deze makkelijker en sneller afhandelen.
Interessant is dat in het onderdeel inzake hergebruik in artikel 11c wordt gesteld dat de artikelen 4 tot en met 7 van de Wob zijn van overeenkomstige toepassing zijn. Hiermee wordt naar de bekende Wob-procedure verwezen. Vreemd genoeg wordt in de memorie van toelichting gesproken over de artikelen 3 tot en met 7. Een niet onbelangrijk verschil omdat in dat artikel 3 wordt verwezen naar de artikelen 10 en 11 betreffende uitzonderingsgronden en beperkingen. Deze artikelen zijn hiermee buitenspel gezet voor de hergebruikprocedure. Dat lijkt echter een verschrijving in de memorie van toelichting. Het is immers zo dat wanneer het gaat om een orgaan dat onder de Wob valt en een verzoeker wil informatie hergebruiken die niet openbaar is, dat dan een openbaarheidsprocedure vooraf gaat aan een hergebruikprocedure. Er is dan dus sprake van een tweetrapsraket, eerst openbaarheid en dan hergebruik. Dat dan in de tweede procedure de artikelen 10 en 11 niet opnieuw een rol spelen is logisch. En als informatie al openbaar is en dus onmiddellijk een verzoek tot hergebruik ingediend kan worden, dan zijn de uitzonderingen en beperkingen niet relevant, omdat de informatie al beschikbaar is.
In artikel 1 van de verruimde Wob is aangegeven wat nu onder hergebruik verstaan dient te worden:

hergebruik: het gebruik van informatie die openbaar is op grond van deze of een andere wet en die is neergelegd in documenten berustend bij een overheidsorgaan, voor andere doeleinden dan het oorspronkelijke doel binnen de publieke taak waarvoor de informatie is geproduceerd.

Dit komt dus overeen met hetgeen in de hiervoor besproken beleidslijn is geschreven.

Bij hergebruik gaat het dus om informatie die al openbaar is. Indien een orgaan dat niet onder de Wob valt, informatie niet openbaar maakt en niet beschikbaar stelt voor hergebruik, dan lijkt het lastig, zo niet onmogelijk, deze informatie openbaar te krijgen en te mogen hergebruiken.

Vergoeding
De regeling inzake de vergoeding die een overheidsorgaan kan vragen voor hergebruik is terecht gekomen in artikel 11h in hoofdstuk V-A van de verruimde Wob:

Artikel 11h
1. De totale inkomsten uit het verstrekken en het verlenen van toestemming voor hergebruik zijn niet hoger dan de kosten van verzameling, productie, vermenigvuldiging en verspreiding van de informatie, vermeerderd met een redelijk rendement op investeringen.

2. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels gesteld worden met betrekking tot de totale inkomsten van het eerste lid.

Dit is dus wezenlijk anders geworden dan het verstrekkingskostenregime waarover in het rapport *Naar ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie* werd gesproken. De formulering lijkt het eerder geschetste gevaar van het verlies van kwaliteit of zelfs het verdwijnen van bestanden te hebben geëlimineerd. Organen kunnen immers de kosten voor hergebruik

[163] Een en ander is geregeld in artikel 4 van de Wob.

vermeerderen met een zogenaamd redelijk rendement op investeringen. De memorie van toelichting stelt hierover dat bij de reikwijdte van *redelijk rendement* in ieder geval de vereiste zelffinanciering van bestuursorganen in acht dient te worden genomen. In diezelfde memorie van toelichting wordt echter ook onderstreept dat dit artikel geen algemene bevoegdheid creëert voor bestuursorganen om kosten te berekenen voor hergebruik van hun informatie.

Verder geeft de memorie van toelichting nog aan dat de aanduiding *redelijk rendement op investeringen* dient te worden bezien in het licht van het doel van de richtlijn, namelijk het stimuleren van de interne markt van de Europese Unie door onder meer ondernemingen in staat te stellen optimaal gebruik te maken van overheidsinformatie en op die wijze bij te dragen tot economische groei en het scheppen van werkgelegenheid. Dit houdt in dat bestuursorganen buitensporige tarieven moeten voorkomen. Het gestelde betreft een bovengrens. Er wordt niet voor niets gesproken van een *redelijk* rendement. Overigens kunnen, zoals te lezen is in lid 1 van artikel 11h, bij of krachtens algemene maatregel van bestuur altijd nog nadere regels worden gesteld met betrekking tot de totale inkomsten voor hergebruik.

Met de implementatie van de Richtlijn hergebruik zijn dus nog geen stappen gezet om bij hergebruik slechts verstrekkingskosten te berekenen zoals in het rapport *Naar ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie* werd geopperd. Het plan is daaraan echter wel aandacht te besteden bij de evaluatie van Wob in 2008.

Geo-informatie
Vraag is nu natuurlijk of de verruimde Wob vruchten afwerpt. De geplande evaluatie van de wet in 2008 zal hopelijk duidelijkheid verschaffen. Tegen de tijd dat we daarvan resultaten zien, zal het waarschijnlijk 2009 zijn. Wat nu bekend is, is dat er begin december 2007 kamervragen gesteld zijn over de toegang tot overheidsdata, waarbij het met name geo-informatie betrof en waarbij uit de vraagstelling en de antwoorden op te maken was, dat het nog steeds is lastig de hand te leggen op bij de overheid beschikbare geo-informatie.[164] Het goede nieuws is evenwel dat de minister van BZK in het antwoord aangeeft dat de bestaande belemmeringen zoveel mogelijk weggenomen gaan worden. Zij geeft daarbij aan dat er met provincies een intentieverklaring gesloten gaat worden, waarin wordt geregeld dat geo-informatie die bij deze bestuurorganen rust, vrij toegankelijk en gratis beschikbaar wordt voor hergebruik. Iets dergelijks staat ook op stapel voor de waterschappen en de gemeenten.

De intentieverklaring van de provincies is er inmiddels.[165] Provincies gaan geo-informatie onder zo gunstig mogelijke voorwaarden beschikbaar stellen. Dat betekent dat geo-informatie tegen zo laag mogelijke kosten verstrekt en hergebruikt mag worden, maar ook dat beperkingen voor het hergebruik van de informatie worden weggenomen. Bovendien wordt inzicht gegeven in de kwaliteit van de geo-informatie en worden de mogelijkheden ervan verduidelijkt.

Wat via de verruimde Wob niet te verwezenlijken lijkt, is dus blijkbaar op andere wijzen wel mogelijk.

Desondanks zijn er ook al geschillen rondom het hergebruik van overheidsinformatie.[166] Zo was het bedrijf Landmark, dat gegevens over locaties van bodemonderzoeken heeft opgevraagd bij gemeenten om die te verwerken met andere data in commerciële producten, met de gemeente Amsterdam in een procedure verwikkeld over (onder meer) de prijs van hergebruik. Hierbij speelde het databankenrecht overigens een belangrijke rol. De rechtbank oordeelde namelijk dat

[164] Kamervragen over toegang tot overheidsdata, 05-12-07. Beschikbaar op <www.rgi.nl>, klik op Actueel onder de hoofdrubriek Nieuws.
[165] Geo-informatie provincies wordt beter beschikbaar, 10-12-07. Beschikbaar op <www.rgi.nl>, klik op Actueel onder de hoofdrubriek Nieuws. Onderaan het bericht staat een verwijzing naar de intentieverklaring.
[166] Zie bijvoorbeeld De overheid zit in de weg, Peter Mom, Digitaal Bestuur (<digitaalbestuur.nl/dossiers/de-overheid-zit-in-de-weg>).

de gemeente Amsterdam geen databankenrecht heeft op de databank met bodeminformatie, omdat niet aannemelijk is geworden dat zij daarin een risicodragende investering heeft gedaan. De gemeente werd dus niet gekwalificeerd als producent van de databank in de zin van de Databankenwet. Het gevolg daarvan is dat de hergebruikregeling van de Wob niet van toepassing is. Artikel 11a Wob stelt immers dat het hergebruikhoofdstuk niet van toepassing is op databanken in de zin van de Databankenwet waarvan een overheidsorgaan niet de maker is. De kostenregeling inzake hergebruik is om die reden dus ook niet van toepassing. Voor de verstrekking van de gegevens aan Landmark geldt zodoende het normale Wob-regime waarvoor slechts verstrekkingskosten in rekening mogen worden gebracht.[167]

Geschillen kunnen trouwens ook ontstaan bij het gratis en zonder voorwaarden beschikbaar stellen van informatie voor hergebruik. Daarvan getuigt de kwestie inzake het Nationaal Wegenbestand (NWB) van Rijkswaterstaat. Deze dienst wil het NWB, een digitaal bestand met vrijwel alle wegen van Nederland, vrijgeven voor hergebruik.[168] Dit heeft geleid tot protesten van bedrijven in de private sector die ook op het gebied van digitale wegenkaarten actief zijn. Zij vrezen namelijk dat hun investeringen in de eigen bestanden moeilijker zijn terug te verdienen als het NWB vrij beschikbaar is.

De richtlijn Hergebruik bepaalt wel dat de voorwaarden waaronder overheidsinformatie ter beschikking wordt gesteld niet gebruikt mogen worden 'om de mededinging aan banden te leggen' (art. 8(1)), maar geeft niet aan hoe om te gaan met situaties waarin het vrijgeven van informatie tot marktverstoring leidt.

Daarnaast gaan de Aanwijzingen voor het verrichten van Marktactiviteiten er vanuit dat als een onderdeel van de rijksoverheid door het leveren van bestanden in concurrentie treedt met de private sector (d.w.z. marktactiviteit verricht), dat alleen mag als die activiteit voortvloeit uit de wet, en de integrale kosten worden doorberekend. Het gaat daarbij om de aan de marktactiviteit toe te rekenen kosten.[169] Nu is de vraag of verstrekking op grond van de herziene Wob ook is aan te merken als een marktactiviteit; en als dat al zo is, welke kosten daaraan dan toegerekend moeten worden. Hoe laag/hoog moeten deze kosten zijn om niet marktverstorend te zijn. Een verstrekkingskostenregime zal hier overigens ook geen soelaas bieden, dat moge duidelijk zijn.[170]

5.5 Conclusie Openbaarheid / hergebruik

Via onder meer de notitie *Naar toegankelijkheid van overheidsinformatie* en het groenboek over overheidsinformatie in de informatiemaatschappij is uiteindelijk een richtlijn hergebruik overheidsinformatie tot stand gekomen. Een richtlijn die in Nederland heeft geleid tot de aanpassing van de Wob. Het hergebruik heeft onder meer betrekking op bestanden met geo-informatie in beheer bij (semi-)overheidsinstellingen.

Na bijna drie jaar 'ervaring' met de vernieuwde Wob is gebleken dat de praktijk weerbarstig is en dat de ontsluiting van overheidsinformatie te wensen overlaat. Dat heeft inmiddels tot een rechtszaak geleid in een poging geo-informatie bij de (gemeentellijke) overheid los te weken, maar ook tot hergebruik-convenanten die een beroep op de herziene Wob overbodig maken.

---

[167] Rechtbank Amsterdam 21 februari 2007. AWB 07/786 WET.
[168] WOB-verzoek Openbaarmaking van het Nationaal Wegen Bestand (NWB), ministerie van Verkeer en Waterstaat (<www.verkeerenwaterstaat.nl> klik op Actueel, vervolgens op WOB-verzoeken vul in bij Jaar/Maand: 2007/Mei)
[169] Aanwijzingen verrichten marktactiviteiten, ministerie van Economische Zaken (<www.minez.nl> zoeken naar *aanwijzingen verrichten marktactiviteiten*).
[170] Bron voor het laatste onderdeel over geschillen rond hergebruik overheidsinformatie is het artikel *Het hergebruik regime voor overheidsinformatie in de Wob, een tussenstand* van Mireille van Eechoud verschenen in Mediaforum 2008-1, p. 2-10.

Daarnaast ondervindt het hergebruik van overheidsinformatie hinder van (markt)situaties zoals die in de loop van vele jaren zijn ontstaan en die niet zomaar even zijn te veranderen dan wel terug te draaien door een regeling inzake hergebruik. Zo kan het vrijgeven van het Nationaal Wegenbestand de markt verstoren. Er zijn immers bedrijven die veel geld geïnvesteerd hebben in eigen wegenbestanden, op basis daarvan producten maken en hun investeringen proberen terug te verdienen. Als vervolgens door de overheid een Nationaal Wegenbestand gratis ter beschikking gesteld gaat worden, dan wordt de concurrentie wel heel makkelijk in het zadel geholpen.

Hiernaast zijn er overheidsinstellingen voor wie de verkoop van (geo-) informatieproducten een belangrijke bron van inkomsten is geworden. Indien als gevolg van een nieuwe hergebruikregeling deze informatie tegen lagere tarieven moeten vrijgeven, kan dat tot problemen leiden.

Dit alles gezegd hebbend, lijkt het niet vreemd dat het hergebruik van overheidsinformatie nog niet op grote schaal plaatsvindt. Vooral niet het hergebruik van geo-informatie, waarbij vaak sprake is geweest van substantiële investeringen om de informatie te verzamelen, op te slaan en te ontsluiten. Indien daar ook nog eens bepaalde kosten-modellen voor de beherende organisatie op toegepast zijn, spreekt het voor zich dat overheidsinstanties niet van de ene op de andere dag in staat zijn (dure) geo-informatie tegen kostprijs van de hand te doen.

Wellicht dat een grondwettelijk duwtje in de rug zou helpen, zoals eerder voorgesteld door de commissie Grondrechten in het digitale tijdperk. Deze commissie stelde voor een nieuw artikel toe te voegen aan de Grondwet waarin staat dat een ieder recht heeft op toegang tot bij de overheid berustende informatie, en waarin tevens wordt vermeld dat de overheid dient te dragen voor toegankelijkheid van bij de overheid berustende informatie. Het lijkt er echter op dat het rapport van deze commissie geen prioriteit (meer) heeft. Er is al een tijd lang weinig of niets meer over vernomen. Datzelfde geldt voor een vervolgonderzoek naar *constitutional rights and new technologies*[171] uitgevoerd in opdracht van dezelfde commissie.[172]

Punt van aandacht en zorg is nog het feit dat niets bekend is van een meting van de effecten van de hergebruikprocedure, zowel wat betreft de doelstelling als de administratieve lasten. Nederland is daartoe namelijk verplicht; in artikel 13 van de richtlijn hergebruik overheidsinformatie is opgenomen dat de toepassing van de richtlijn uiterlijk op 1 juli 2008 geëvalueerd zal worden door de Commissie. Dat laatste gaat wat Nederland betreft in ieder geval niet meer lukken.

[171] Zie voor het rapport van de commissie Grondrechten in het digitale tijdperk en het vervolgonderzoek naar constitutional rights and new technologies, Recht.nl, <recht.nl/1138>.
[172] *Kamerstukken II* 2006-2007, 27460, nr. 5

6. Intellectuele eigendomsrechten

In dit hoofdstuk wordt aandacht besteed aan de intellectuele eigendomsrechten op geo-informatie.[173] In dat kader komen het auteursrecht en het databankenrecht aan de orde. Daarnaast zullen soms tevens de Wet openbaarheid bestuur (Wob) en de Richtlijn hergebruik overheidsinformatie de revue passeren, maar deze zullen slechts summier worden toegelicht omdat deze hiervoor al besproken zijn.

6.1 Auteursrecht

Het auteursrecht is het uitsluitende recht van de maker van een letterkundig werk, wetenschappelijk werk of kunstwerk om dat werk openbaar te maken en te verveelvoudigen (art. 1 Auteurswet 1912). Auteursrecht kan rusten op een werk, zoals een kaart of foto of de selectie of ordening van gegevens. Om voor auteursrechtelijke bescherming in aanmerking te komen moet het werk een eigen, oorspronkelijk karakter vertonen en het persoonlijk stempel van de maker (HR 4 januari 1991, NJ 1991,608, *Van Dale/Romme*). Ook een selectie of combinatie van gegevens op basis van technische of wetenschappelijke expertise en kennis, die een persoonlijke keuze inhoudt uit een (groot) aantal mogelijkheden kan aan deze eis voldoen (HR 24 februari 2006, IER 2006, 39, BIE 2007, 23, *Technip/Goossens*).

Auteursrecht kan niet rusten op een idee of methode en evenmin op feiten of gegevens. Spoor, Verkade en Visser maken in dit verband onderscheid tussen de objectieve (feitelijke) en de subjectieve (persoonlijke) trekken van een werk.[174]

6.2 Databankenrecht

Het geëigende middel voor bescherming van investeringen in gegevens – zoals geografische informatie - is het *sui generis* databankenrecht, neergelegd in artikel 7 e.v. van Richtlijn 96/9/EG. Zoals bepaald in overweging 39 heeft de richtlijn ten doel "*de bescherming van de fabrikanten van databanken tegen onrechtmatige toeëigening van de resultaten van de financiële en professionele investeringen die zijn gedaan om de inhoud te verkrijgen en te verzamelen*". Deze richtlijn is in Nederland uitgewerkt in de Databankenwet.

Het databankenrecht rust op een systematisch of methodisch geordende verzameling gegevens of werken, die afzonderlijk toegankelijk zijn, in de verkrijging, controle of presentatie waarvan een substantiële investering is gedaan (artikel 1, eerste lid, sub a Databankenwet). Afzonderlijke gegevens zijn niet door een databankenrecht beschermd. Het staat ieder vrij om dezelfde gegevens te verzamelen en in een databank onder te brengen (en dus: om een soortgelijke investering te doen).

In zijn arrest van 9 november 2004 inzake *British Horseracing Board* heeft het Hof van Justitie van de EG bepaald dat:

het begrip investering in de verkrijging van de inhoud van een databank in de zin van artikel 7, lid 1, van richtlijn 96/9 betreffende de rechtsbescherming van databanken [artikel 1, eerste lid sub a Databankenwet] *aldus* [moet] *worden opgevat dat het betrekking heeft op de investering ten*

[173] Dit hoofdstuk is een bewerking van H.W. Wefers Bettink, Intellectuele eigendomsrechten op geo-informatie, eerder gepubliceerd in Leo van der Wees, Sjaak Nouwt (red.), *Recht en locatie*. Nederlandse Vereniging voor Informatietechnologie en Recht, Den Haag: Elsevier Juridisch, 2008. Met dank aan de auteur Wolter Wefers Bettink, advocaat bij Houthoff Buruma.
[174] Spoor/Verkade/Visser, Auteursrecht, Naburige rechten en Databankenrecht, Deventer: Kluwer, 2005, p. 67.

behoeve van het aanleggen van deze databank. Het duidt dus op de middelen die worden aangewend om bestaande elementen te verkrijgen en in deze databank te verzamelen, maar omvat niet de middelen die worden aangewend voor het creëren van de elementen die de inhoud van een databank vormen.[175]

In *British Horseracing Board* bestond het creëren van de gegevens volgens het HvJ EG onder meer uit het vaststellen van datum en tijd, plaats en naam van de race en de namen van de deelnemende paarden. Ook het controleren van de identiteit van degene die een paard voor een race inschreef en de karakteristieken van het paard, alsmede het verifiëren van diens classificatie en van eigenaar en jockey behoren volgens het Hof tot de fase van het creëren van de informatie. Alle investeringen daarin worden *niet* door het databankenrecht beschermd.

Onder investering in de verkrijging, controle of presentatie van de inhoud van een databank valt de investering in het opzetten van de databank *als zodanig*. In dat verband verwijst het HvJ EG naar de overwegingen 9, 10 en 12 van de Richtlijn waaruit blijkt dat het doel van de Richtlijn is het bevorderen en beschermen van investeringen in systemen voor de opslag en verwerking van gegevens die bijdragen aan de ontwikkeling van een marktinformatie.[176]

6.2.1 Exclusieve rechten

De rechthebbende kan zich verzetten tegen het '*opvragen of hergebruiken van het geheel of van een in kwalitatief of kwantitatief opzicht substantieel deel van de inhoud van de databank*' (art. 2 lid 1 onder a Databankenwet). Een gedeelte van een databank kan volgens de memorie van toelichting als 'substantieel' aangemerkt worden indien door de overname ervan '*een normale exploitatie voor de producent niet mogelijk is of indien de producent ongerechtvaardigde schade aan zijn rechtmatige belangen lijdt*'.[177] Hiervan kan bijvoorbeeld sprake zijn indien een groot deel van de databank wordt overgenomen, of een gedeelte dat weliswaar klein is, maar in de verkrijging, controle of presentatie waarvan substantieel is geïnvesteerd.[178]

Voorts kan de databankrechthebbende zich verzetten tegen het '*herhaald en systematisch opvragen of hergebruiken van in kwalitatief of in kwantitatief opzicht niet-substantiële delen van de inhoud van een databank, voor zover dit in strijd is met de normale exploitatie van die databank of ongerechtvaardigde schade toebrengt aan de rechtmatige belangen van de producent van de databank*' (art. 2 lid 1 onder a Databankenwet). Doel van deze bepaling is te voorkomen dat degene die herhaald en systematisch kleine gedeelten opvraagt of hergebruikt daardoor de databank geheel of grotendeels kan reconstrueren.[179] De databankrechthebbende wordt door dit 'uitmelken' van de databank immers in zijn rechtmatige belangen geschaad.

6.3 Geo-informatie bij de overheid

Veel geo-informatie wordt door of in opdracht van de overheid verzameld, doorgaans op basis of in het kader van een wettelijke regeling, zoals de Kadasterwet. Volgens de Kadasterwet heeft de 'Dienst voor het kadaster en de openbare registers' (doorgaans aangeduid als het Kadaster) onder andere tot taak de bevordering van de rechtszekerheid ten aanzien van registergoederen.

Een ander voorbeeld van de rol van de overheid bij het creëren van geo-informatie is de in het kader van de Wet bodembescherming aan overheidsorganen gegeven opdracht informatie over

[175] Zaak C203-02, Arrest van het Hof (grote kamer) van 9 november 2004, The British Horseracing Board Ltd en anderen tegen William Hill Organization Ltd. Jurisprudentie 2004 bladzijde I-10415.
[176] British Horseracing Board, r.o. 30.
[177] *Kamerstukken II* 1997/1998, 26108, nr. 3, p. 10.
[178] British Horseracing Board, r.o.71.
[179] British Horseracing Board, r.o. 87.

de kwaliteit van de bodem in het door hen bestuurde gebied te verzamelen. De informatie over (potentieel) ernstig verontreinigde locaties is neergelegd in de bodemkwaliteitskaarten en verzameld in het Landsdekkend Beeld Bodemverontreiniging.

6.3.1 Wet openbaarheid van bestuur

Geo-informatie afkomstig van een overheidsorgaan mag in beginsel vrij worden gebruikt. Dit sluit aan bij de Wet openbaarheid van bestuur (Wob) op grond waarvan een bestuursorgaan op verzoek openbare informatie ter beschikking moet stellen aan burgers en bedrijfsleven. Het begrip 'bestuursorgaan' ziet op een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld, of een ander persoon of college, met enig openbaar gezag bekleed, zoals de Ministers, het College van Gedeputeerde Staten en het College van Burgemeester en Wethouders. De Dienst voor het kadaster en de openbare registers valt eveneens onder dit begrip, aangezien de Dienst is ingesteld krachtens de Organisatiewet Kadaster.[180]

Met "openbare informatie" is bedoeld informatie die is neergelegd in documenten over een bestuurlijke aangelegenheid (artikel 3 Wob). Het gaat hier om informatie over aangelegenheden die betrekking hebben op het beleid van een bestuursorgaan, met inbegrip van de voorbereiding en de uitvoering van dat beleid (artikel 1 Wob).[181]

6.3.2 Hergebruik

Geo-informatie zal in het algemeen niet onder een van de uitzonderingsgronden van artikel 10 Wob vallen en wordt door de overheid in steeds ruimere mate uit eigen beweging ter beschikking gesteld. Voorbeelden zijn de kaarten van de Topografische Dienst Kadaster, leidingkaarten en bodemkwaliteitskaarten.

Voor het (commerciële) hergebruik van overheidsinformatie gelden bijzondere regels, die zijn opgenomen in hoofdstuk V-A van de Wob. Deze bepalingen zijn gebaseerd op Richtlijn 2003/98/EG inzake het hergebruik van overheidsinformatie.[182] In overweging 5 van de Richtlijn is bepaald dat overheidsinformatie een belangrijke grondstof vormt voor digitale informatieproducten en -diensten en dat ruimere mogelijkheden voor het hergebruik van overheidsinformatie Europese ondernemingen in staat zullen stellen om bij te dragen aan economische groei en het scheppen van werkgelegenheid.

Het uitgangspunt van de Richtlijn, uitgewerkt in artikel 11b Wob, is dat eenieder een overheidsorgaan kan vragen om verstrekking van informatie die hij wenst te hergebruiken. Op grond van artikel 11h kan het overheidsorgaan een vergoeding voor het hergebruik in rekening brengen. De totale inkomsten uit het verstrekken en het verlenen van toestemming van hergebruik mogen niet hoger zijn dan de kosten van verzameling, productie, vermenigvuldiging en verspreiding van de informatie, vermeerderd met een redelijk rendement op investeringen. In de memorie van toelichting bij de Invoeringswet van de Hergebruikregeling in de Wob is bepaald dat de regeling alleen van toepassing is wanneer een overheidsorgaan informatie openbaar

[180] Artikel 2 van deze wet bepaalt: "*Er is een Dienst voor het kadaster en de openbare registers. Hij bezit rechtspersoonlijkheid en is gevestigd te Apeldoorn*." Volgens hetzelfde artikel is de Dienst belast met de taken die hem bij of krachtens de Kadasterwet of andere wetten worden opgedragen.

[181] Volgens Spoor/Verkade/Visser, Auteursrecht, Naburige Rechten en Databankenrecht, p.141 zouden onder dit begrip ook vallen privaatrechtelijke rechtspersonen aan wie de openbare macht de uitoefening van een deel van de publieke taak heeft opgedragen. Zij ontlenen dit aan HR 14 juni 1968, NJ 276 m.nt. HB (Bankbiljetten), waarin overigens werd vastgesteld dat De Nederlandsche Bank N.V. niet onder het begrip "openbare macht" van artikel 15b Auteurswet valt.

[182] PbEU 2003, L 345/90.

maakt en daarbij aangeeft dat zij op die informatie een auteursrecht, databankenrecht of naburig recht voorbehoudt.[183] Daarbij wordt aangetekend dat de regering met de hergebruikregeling wil stimuleren dat zoveel mogelijk informatie uit eigen beweging door overheidsorganen openbaar wordt gemaakt en daarbij zo min mogelijk voorbehouden worden gemaakt.

Is geen auteursrecht of databankenrecht voorbehouden, dan zal het overheidsorgaan verstrekking van de gevraagde informatie niet mogen weigeren (tenzij een van de weigeringsgronden van artikel 10 Wob van toepassing is), ook als duidelijk is dat de verzoeker die informatie (commercieel) zal hergebruiken. In dat geval mogen alleen de feitelijke verstrekkingskosten in rekening worden gebracht, zoals dat ook gebeurt wanneer een gewoon verzoek tot verstrekking van informatie op basis van de Wob wordt ingediend.

6.3.2.1 Voorbehoud auteursrecht of databankenrecht

Is wel een voorbehoud gemaakt dan zal aan het betreffende overheidsorgaan toestemming moeten worden gevraagd voor hergebruik. Die toestemming kan worden geweigerd of aan voorwaarden worden gebonden, zoals het betalen van een vergoeding al dan niet tegen kostprijs. Uit de in de memorie van toelichting genoemde voorbeelden van weigering van toestemming – hergebruik van politielogo's, paspoorten en diskettes van de Belastingdienst – blijkt dat alleen in uitzonderingsgevallen, wanneer een legitiem gebruik van de informatie niet goed denkbaar is en misbruik dus op de loer ligt, het verzoek tot hergebruik zal mogen worden geweigerd.

Hoewel de overheid in beginsel een discretionaire bevoegdheid heeft bij het bepalen van de voorwaarden voor hergebruik is in de memorie van toelichting nadrukkelijk bepaald dat deze voorwaarden het hergebruik niet nodeloos mogen beperken en evenmin mogen worden gebruikt om de mededinging aan banden te leggen. In het algemeen zullen overheidsorganen de voorwaarden waaronder hergebruik mogelijk is inzichtelijk moeten maken, bij voorkeur via het internet. Ook het zoeken naar voor hergebruik beschikbare documenten zal zo eenvoudig mogelijk moeten worden gemaakt, waartoe overheidsorganen worden aangespoord de beschikbare informatie en de voorwaarden voor hergebruik op hun website beschikbaar te stellen.

6.3.2.2 Modelverordening en wet

De Vereniging van Nederlandse Gemeenten heeft een tekst vastgesteld voor een modelverordening om auteursrecht en databankenrecht voor te behouden. Daarin is in zijn algemeenheid bepaald dat een gemeente zich het auteursrecht en databankenrecht uitdrukkelijk voorbehoudt en dat burgemeester en wethouders toestemming kunnen verlenen voor het verveelvoudigen en openbaar maken van gemeentelijke databanken, waaraan voorwaarden kunnen worden verbonden. Een aantal gemeenten heeft een dergelijke verordening vastgesteld, ingegeven door de gedachte dat geld kan worden verdiend aan hergebruik van overheidsinformatie.

Een ander voorbeeld van een dergelijk voorbehoud biedt artikel 7 van het wetsvoorstel tot wijziging van de Kadasterwet. [184] Het artikel bepaalt dat het databankenrecht ten aanzien van (ondere andere) de 'basisregistratie kadaster' (kadastrale registratie en kadastrale kaart) en de 'basisregistratie topografie' (digitale topografische kaarten van Nederland) is voorbehouden aan het Kadaster.

6.3.2.3 Voorbehoud nader bekeken

[183] *Kamerstukken II* 2004-2005, 30188, nr.3, p.8.
[184] Wet basisregistraties kadaster en topografie, 5 maart 2007, Stb. 105, 5 maart 2007.

Het is de vraag of een in algemene bewoordingen gestelde verordening voldoet aan de uitgangspunten van de Richtlijn overheidsinformatie en de hergebruikregeling van de Wob. Een algemeen geformuleerd voorbehoud van auteursrecht of databankenrecht, waarbij niet is aangegeven op welke databanken het betrekking heeft, lijkt haaks te staan op het in de memorie van toelichting bij de Wob verwoorde uitgangspunt dat zoveel mogelijk overheidsinformatie voor hergebruik ter beschikking wordt gesteld en dat sporadisch gebruik wordt gemaakt van de mogelijkheid een voorbehoud te maken. Bovendien komt een dergelijk algemeen voorbehoud de transparantie van bestuur en de rechtszekerheid niet ten goede. Onduidelijk is immers op welke auteursrechtelijk beschermde werken en databanken het betrekking heeft, terwijl in de meeste gevallen de betreffende verordening geen voorwaarden voor hergebruik bevat.

In praktijk blijkt de modelverordening een belangrijk obstakel te zijn voor het hergebruik van overheidsinformatie. Bestuursorganen gaan pas na ontvangst van een verzoek tot hergebruik nadenken over de vraag of de verordening van toepassing is op de gevraagde informatie en, zo ja, op welke voorwaarden de informatie mag worden hergebruikt. Daarbij lijken bestuursorganen zich niet te realiseren dat het maken van een voorbehoud nog niet betekent dat men een auteursrecht of databankrecht *heeft*. Het werk of de databank moet immers voldoen aan de vereisten voor bescherming onder de Auteurswet 1912 respectievelijk de Databankenwet.

6.3.3 Auteursrecht op overheidsinformatie

Zoals hierboven aangegeven is de drempel voor auteursrechtelijke bescherming laag, zodat bijvoorbeeld kaarten – ook als deze door een computer zijn gegenereerd – doorgaans wel voor auteursrechtelijke bescherming in aanmerking zullen komen. Bij databanken (verzamelingen van gegevens) zal dat echter meestal niet het geval zijn. Een databank kan als werk onder de Auteurswet vallen als de selectie en ordening van de daarin opgenomen gegevens getuigt van een persoonlijke visie van de maker. Het uitgangspunt van de meeste databanken met overheidsinformatie is echter dat deze *alle* relevante gegevens bevat, zoals de coördinaten van een perceel en de ligging van leidingen en kabels. Van een op subjectieve inzichten en voorkeuren gebaseerde selectie zal zelden of nooit sprake zijn. Ook de ordening van een databank met overheidsinformatie vindt doorgaans plaats op basis van objectieve gegevens, zoals de locatie, alfabetische volgorde van de betreffende straatnamen of het tijdstip van onderzoek. Overheidsdatabanken komen derhalve doorgaans niet voor auteursrechtelijke bescherming in aanmerking. Wel kunnen zij beschermd zijn op grond van de Databankenwet, indien een geldig voorbehoud is gemaakt conform artikel 8, tweede lid, Databankenwet.

6.3.4 Databankenrecht op overheidsinformatie

Op grond van artikel 2 van de Databankenwet heeft de producent van een databank het uitsluitend recht hergebruik van de inhoud daarvan toe te staan en aan toestemming voorwaarden te verbinden. Artikel 1, eerste lid, onder b Databankenwet bepaalt dat de producent van een databank degene is die "*het risico draagt van de voor de databank te maken investering*".

Het gebruik van de terminologie "*risico dragen*" en "*investering*" roept de vraag op of de overheid risico draagt en of het besteden van overheidsgelden kan worden gezien als een investering. Uit de memorie van toelichting bij de Databankenwet blijkt dat met "*risico dragen*" is bedoeld dat degene die een investering heeft gedaan het risico loopt dat hij deze niet uit de exploitatie van de databank zal terugverdienen.[185] Tenzij de overheid een databank met het oog op de commerciële exploitatie daarvan heeft opgezet zal bij databanken van een overheidsorgaan niet snel sprake zijn van een dergelijk risico. Doorgaans worden overheidsdatabanken opgezet om te voorzien in of ter ondersteuning bij de uitoefening van de publieke taak van de overheid. Zo is de databank

[185] *Kamerstukken II* 1997-1998, 26108, nr. 3, p.9.

met informatie over bodemverontreiniging van bepaalde locaties opgezet als onderdeel van de taak van gemeenten als bevoegd gezag in het kader van de Wet bodembescherming.

Uit de memorie van toelichting bij de Wet basisregistraties kadaster en topografie valt op te maken dat de overheid zich op twee gronden beroept om het voorbehoud van databankrechten van het Kadaster te rechtvaardigen. Het eerste argument is gelegen in de tarieffinanciering van het Kadaster, "*dat zich moet bedruipen uit vergoedingen voor (her)gebruik van de databanken (de registraties)*". Het Kadaster is een zelfstandig bestuursorgaan en moet, net als een groot aantal andere zelfstandige bestuursorganen, haar publieke taak kostendekkend uitvoeren. De tweede grond voor het Kadaster om databankrechten voor te houden is uit vrees voor schaduwregistraties, "*vanwege de daarmee gepaarde gaande onduidelijkheid en (rechts)onzekerheid in het maatschappelijke en rechtsverkeer*".[186]

Deze argumentatie moge politiek sluitend zijn, hij sluit niet aan bij de omschrijving van 'producent van een databank' in de Databankenwet. Daarmee staat immers niet vast dat het Kadaster 'producent van de databank' is, in die zin dat hij investeringen doet, waarvan hij het risico draagt dat hij deze niet kan terugverdienen. Uit het feit dat het Kadaster kennelijk 'self-supporting' moet zijn kan worden afgeleid dat het Kadaster niet wordt gefinancierd uit overheidsgelden, zodat wellicht toch sprake is van het lopen van risico voor de gedane investeringen.

6.4 Definitie databank

Ook als een overheidsorgaan ten aanzien van een bepaalde databank kan worden beschouwd als de producent daarvan, is de databank nog niet beschermd onder de Databankenwet. Deze zal moeten voldoen aan de definitie van databank in de Databankenwet, met name dat de verkrijging, de controle of de presentatie van de inhoud in kwalitatief of kwantitatief opzicht getuigt van een substantiële investering.

In het genoemde arrest van het Hof van Justitie van de EG van 9 november 2004 inzake de British Horseracing Board[187] is bepaald dat het begrip investering:

> *"duidt op de middelen die worden aangewend om bestaande elementen te verkrijgen en in deze databank te verzamelen, met uitsluiting van de middelen die worden aangewend voor het creëren van die elementen."*

Onder het creëren van informatie moet niet alleen het opstellen en vervaardigen van gegevens worden verstaan, maar ook het omzetten daarvan in digitale gegevens en de controle van die gegevens. Daartegenover ziet het verkrijgen van informatie op het verzamelen van gegevens met het oog op de aanleg van een databank en het omzetten van die gegevens in een digitaal bestand.

Zoals aangegeven is dit onderscheid minder scherp dan het op het eerste gezicht lijkt. Het roept onder meer de vraag op of het invoeren in een databank van gegevens die afkomstig zijn uit papieren rapportages, moet worden gezien als het creëren of als het verkrijgen van gegevens. In dat verband is de zogenaamde spin-off theorie van belang die in de Nederlandse jurisprudentie is ontwikkeld.

6.5 Spin off

Het Gerechtshof Arnhem heeft in zijn arrest 4 juli 2006 in de zaak Zoekallehuizen.nl bepaald:

---

[186] *Kamerstukken II* 2005-2006, 30544, nr. 3, p.36.
[187] Zie noot 9.

> *"Naar het voorlopig oordeel van het Hof hebben de makelaars ook in hoger beroep niet voldoende aannemelijk gemaakt dat zij in verband met het verkrijgen, controleren of presenteren van de gegevens op de website aanzienlijke investeringen hebben moeten doen die zij anders niet zouden hebben gedaan."*

Het Gerechtshof doelt daarmee op het feit dat de betreffende databank met informatie over te koop staande huizen in het kader van de reguliere dienstverlening van makelaars is opgezet. Een investering die zij in het kader van hun hoofdactiviteit tóch moesten doen om als makelaar hun beroep goed te kunnen uitoefenen telt niet als investering in de databank zelf.

Deze overweging volgt op een beschouwing van het Gerechtshof over het *British Horseracing Board* arrest van het HvJ EG, waarbij het Gerechtshof benadrukt dat het feit dat een databank een spin-off is van een hoofdactiviteit op zich nog niet betekent dat die databank niet beschermd kan zijn. Immers, indien *daarnaast* is geïnvesteerd in het aanleggen van de databank als zodanig (het verkrijgen, controleren of presenteren van de inhoud) zal de databank – mits het om een substantiële investering gaat – beschermd zijn onder de Databankenwet. Kennelijk is het Gerechtshof van mening dat de investeringen in de website de hoofdactiviteiten van de betrokken makelaars betreffen en niet de databank als zodanig.

6.5.1 Overheidsinformatie als spin-off

Ook bij een databank die door een overheidsorgaan wordt samengesteld zal steeds moeten worden beoordeeld of de daaraan bestede gelden de hoofdactiviteit (publieke taak) betreffen. Is dat het geval, dan zijn de investeringen gericht op het (beter) vervullen van die hoofdactiviteit en betreffen niet de databank *als zodanig*. Los daarvan zal een overheidsorgaan subsidie, die het voor het inrichten van databanken heeft ontvangen, in mindering moeten brengen op de gelden die als 'investering' worden aangemerkt. Zo is voor het opzetten van databanken met informatie over bodemverontreiniging in het kader van het Landsdekkend Beeld Bodemverontreiniging door het ministerie van VROM subsidie verstrekt, waarbij het opstellen en inrichten van de databank bovendien een voorwaarde was om in een later stadium subsidie bij het uitvoeren van bodemsaneringsoperaties te krijgen. De vraag is dan of het overgebleven bedrag (na aftrek van de subsidie) kan gelden als substantiële investering, zoals de definitie van databank vereist.

6.6 Landmark vonnis

De rechtbank Amsterdam heeft in zijn vonnis van 11 februari 2008 het spin-off beginsel op een dergelijke databank toegepast [188]. Het bedrijf Landmark, dat onder meer rapportages levert over de percelen en de omgeving van te koop staande huizen, had de gemeente Amsterdam gevraagd om een lijst met adressen waar bodemonderzoek was verricht. Landmark deed dat verzoek in het kader van de Wob. De gemeente beriep zich, na een aanvankelijke weigering de gegevens te leveren, op een databankenrecht op de betreffende gegevens en stelde dat de hergebruikregeling van de Wob van toepassing was op het verzoek van Landmark. De gemeente berekende een (haars inziens kostendekkende) vergoeding van aanvankelijk €94.000, en later ca. €10.000 en stelde beperkende voorwaarden aan het gebruik van de gegevens door Landmark. In de procedure stelde Landmark zich op het standpunt dat de gemeente geen databankenrechten heeft, omdat zij niet voldoet aan de definitie van producent van een databank in de Databankenwet. Zij had immers geen risicodragende investering gedaan in het verkrijgen, de controle of de presentatie van de inhoud van de databank. De rechtbank nam dit standpunt over en deelde:

[188] Landmark Nederland B.V. tegen College van B&W Amsterdam, zaak AWB 07/786 WET.

> *"De rechtbank stelt vast dat verweerder voor het aanleggen van de databank waarin de door eiseres gevraagde gegevens zijn neergelegd, publieke middelen ter beschikking heeft, die gedeeltelijk komen uit eigen middelen en gedeeltelijk uit een speciale rijksbijdrage. Van een risicodragende investering is daarom geen sprake. Dat voor het opzetten van de databank mogelijk (hoge) kosten moeten worden gemaakt, maakt dat niet anders."*

De rechtbank deelt het standpunt van eiseres dat de databank in het geval van verweerder in de eerste en voornaamste plaats een publieke taak dient.

> *"Naar het oordeel van de rechtbank heeft verweerder niet voldoende aannemelijk gemaakt dat hij in verband met de databank aanzienlijke investeringen heeft moeten doen die hij anders niet zou hebben gedaan in de zin van de Databankenwet."*

De rechtbank was daarnaast van mening dat, gezien het arrest van het Gerechtshof Arnhem in het arrest Zoekallehuizen.nl, een databank niet in aanmerking komt voor een databankenrecht als deze een nevenproduct is van de hoofdactiviteit van de producent: Naar het oordeel van de rechtbank deed die situatie zich eveneens voor.

Tenslotte bevestigde de rechtbank dat, bij gebreke van een databankenrecht, de hergebruikregeling uit de Wob niet van toepassing is.

De rechtbank concludeerde:

> *"Het vorenstaande leidt tot het oordeel dat verweerder geen bevoegdheid had om op grond van artikel 2, eerste lid, onder a, van de Databankenwet aan het hergebruik van de door eiseres gevraagde gegevens voorwaarden te verbinden."*

6.7 Conclusie intellectuele eigendomsrechten

Auteursrecht
Ten aanzien van (overheids)werken waarin geo-informatie is vastgelegd, zoals kadastrale kaarten, leidingkaarten en bodemverontreinigingskaarten, kan worden geconcludeerd dat zij allemaal zijn gemaakt met als doel het zo nauwkeurig mogelijk weergeven van de werkelijkheid. Daarbij is slechts beperkt plaats voor subjectieve keuzes van de auteur, omdat de kaarten vooral duidelijk en compleet moeten zijn, en dan is het auteursrecht niet van toepassing.

Databankenrecht
Op grond van de hergebruikregeling van de Wob zal een overheidsorgaan op verzoek geografische informatie voor hergebruik ter beschikking moeten stellen. Indien het overheidsorgaan een databankenrecht op die informatie heeft en zich dat uitdrukkelijk heeft voorbehouden, kan hij voor het verstrekken van die informatie een kostendekkende vergoeding vragen.
Geografische informatie kan beschermd zijn met een databankenrecht, maar dan moet wel aan de materiële vereisten die de Databankenwet daar aan stelt zijn voldaan. In veel gevallen zal de overheid, niet over een databankenrecht beschikken, omdat zij niet kwalificeert als producent van een databank, dan wel omdat de databank zelf niet voldoet aan de vereisten van de Databankenwet.

Het Landmark vonnis bevestigt deze gedachtegang. Daarmee wordt recht gedaan aan het uitgangspunt van de hergebruikregeling in de Wob om ruimhartig overheidsinformatie aan burgers en bedrijfsleven ter beschikking te stellen. Doel daarvan is het bevorderen van

economische activiteiten en, daarmee, de werkgelegenheid. Het vragen van een kostendekkende vergoeding op basis van de hergebruikregeling – waarmee het overheidsorgaan in feite de uitgaven voor de publieke taken terugverdient – staat daarmee op gespannen voet. Een overheidsorgaan zal alleen in uitzonderingsgevallen, waarin het los van zijn hoofdactiviteit heeft geïnvesteerd in de databank als zodanig, een dergelijke vergoeding kunnen vragen. In alle andere gevallen zal de informatie op grond van de Wob tegen verstrekkingskosten beschikbaar moeten worden gesteld – ongeacht het doel waarvoor de informatie is opgevraagd.

Het moge duidelijk zijn dat de geschetste situatie betreffende intellectuele eigendom niet specifiek van toepassing is op geo-informatie, maar op hergebruik van overheidsinformatie in zijn algemeenheid, waarbij duidelijkheid en volledigheid van de informatie vereist is.

7. Samenvatting en conclusie

Dit rapport is het resultaat van een onderzoek naar de juridische (on)mogelijkheden van het gebruik van geo-informatie bij overheidsdiensten. Die geo-informatie kan gebruikt worden in locatiegebonden diensten en geografische informatiesystemen.

Er is in dit kader een juridische analyse gedaan waarbij vier rechtsgebieden aan de orde zijn gekomen: privacy, arbeidsrecht, openbaarheid/hergebruik, intellectuele eigendom. Per rechtsgebied zijn, indien relevant, toepasssing beschreven, waarna deze tegen het juridische licht gehouden zijn.

Privacy
In systemen waarbij geo-informatie een rol speelt en deze informatie (vaak) in combinatie met andere gegevens te herleiden is tot een identificeerbare persoon hebben we de aandacht willen vestigen op het begrip contextuele privacy. Dit betekent dat binnen de context waarin een systeem gebruikt wordt of gaat worden, dit beoordeeld dient te worden op de gevolgen voor privacy (recht om rust gelaten te worden én gegevensbescherming).

Daarbij zou wat ons betreft de leidraad moeten zijn dat zo weinig mogelijk gegevens verwerkt dienen te worden, maar vanzelfsprekend genoeg om een systeem naar behoren te kunnen laten functioneren: het principe *less is more* zoals vaak vermeld in relatie tot privacy enhancing technologies (PET).

Bij de beoordeling van de context van het gebruik van privacy-gevoelige gegevens en de toepasbaarheid van het principe *less is more* zou een privacyfunctionaris ingeschakeld kunnen worden, of een EDP-auditor die tevens een oordeel – een privacy-audit – velt over het ontwerp van te gebruiken of te ontwikkelen systeem.

Daarnaast is en blijft transparantie een groot goed. Het moet een burger te allen tijde duidelijk zijn wie welke gegevens over an hem verzameld en hij moet eenvoudige middelen hebben om zijn gegevens te kunnen aanpassen, verwijderen of anderszins. Hierbij past een actief overheidsbeleid. Het moet niet de burger zijn die op zoek moet gaan naar plekken waar zijn gegevens opgeslagen kunnen zijn; de overheid moet actief – op eigen initiatief – aangeven bij wie welke gegevens voor hoe lang zijn opgeslagen.

Het gebruik van geo-informatie bij verschillende overheidsdiensten kan niet anders dan gevolgen hebben voor de privacy in de publieke ruimte en de mate waarin burgers bescherming van hun privacy mogen verwachten. Zeker als we bedenken dat naast geografische informatiesystemen en locatiegebonden diensten er in de publieke ruimte tegenwoordig steeds vaker camera's aanwezig zijn die opnames maken van passerende burgers. Om nog maar niet te spreken van de digitale openbare ruimte, het internet.

Maar natuurlijk moeten we ook niet vergeten dat technologie gemak met zich mee brengt. Er moet sprake zijn van (technische) vooruitgang én privacy, niet van vooruitgang of privacy. En als een vooruitgang een inperking van de privacy met zich mee zou brengen, dan zou de zelfbeschikking voorop moeten staan. Het is aan de persoon zelf om iets van zijn privacy in te leveren, in ruil voor een nieuwe (technologische) dienst.

Arbeidsrecht
Op het terrein van het arbeidsrecht speelt, naast de Wet bescherming persoonsgegevens en de grondrechten, de Wet op de ondernemingsraden een rol.

Werknemers hebben volgens vaste rechtspraak een recht op privacy. Aan de andere kant brengt het bestaan van een arbeidsverhouding ook een beperking op de grondrechten van werknemers met zich mee. Deze beperking wordt veroorzaakt doordat er een gezagsverhouding bestaat tussen werknemer en werkgever.

Dat betekent dat er niet te pas en te onpas gebruik gemaakt mag worden van bijvoorbeeld personeelsvolgsystemen waarbij locatiegegevens – geo-informatie – over werknemers wordt opgeslagen.

Het gestelde over personeelsvolgsystemen geldt overigens ook als er geen geo-informatie aan de orde is, of geen geo-informatie wordt verwerkt in een personeelsvolgsysteem. Het toevoegen van geo-informatie aan personeelsvolgsystemen geeft deze naar onze mening echter wel een extra (Big Brother-)dimensie. Voor de werknemer kan het ongemakkelijk zijn als de werkgever hem gedurende werktijd tot op de meter nauwkeurig kan volgen. Het recht om ook als werknemer met rust te gelaten te worden, zal aan het gebruik van dat soort systemen grenzen kunnen en moeten stellen.

Openbaarheid / Hergebruik
Openbaarheid en hergebruik van overheidsinformatie lijken na aanpassing van Wet openbaarheid van bestuur nog wat moeizaam op gang te komen. Dat geldt ook voor het hergebruik van geo-informatie. Het is vooralsnog niet de Wob die zorgt voor een toename van hergebruik en toegankelijkheid van overheidsinformatie, maar het zijn initiatieven van bijvoorbeeld provincies, die geo-informatie onder gunstige voorwaarden beschikbaar stellen.

Marktverstorende elementen die een verder hergebruik van overheidsinformatie in de weg staan, zullen uit de weg geruimd dienen te worden. Kosten-modellen van overheidsinstanties die geo-informatie verstrekken zullen daartoe wellicht aangepast moeten worden.

In navolging van de commissie Grondrechten in het digitale tijdperk kan worden gesteld dat de toegang tot bij de overheid berustende informatie van cruciaal belang is geworden voor de politieke, juridische en sociale positie van burgers. Misschien dat de evaluatie van de vernieuwde Wet openbaarheid van bestuur mede uitgevoerd kan worden in het licht van deze opvatting, waarbij de voorstellen van de commissie om een nieuw artikel toe te voegen aan de Grondwet inzake de toegang en ontsluiting van overheidsinformatie nog eens tegen het licht gehouden kunnen worden. Hierbij zal ook een zekere balans gevonden moeten worden in de toegang en ontsluiting. Immers, alvorens informatie te ontsluiten voor het publiek, dient de overheid de gelegenheid te hebben de informatie de vorm en inhoud te geven op basis waarvan bijvoorbeeld met de burgers gediscussieerd kan worden.

Intellectuele eigendomsrechten
Het auteursrecht zal niet snel een rol spelen bij de ontsluiting van geo-informatie door de overheid, mits die informatie zo duidelijk en volledig moet zijn. Er is dan geen ruimte voor een persoonlijk stempel van de maker.

Geografische (overheids)informatie kan beschermd zijn met een databankenrecht, maar dan moet wel aan de materiële vereisten zijn voldaan die de Databankenwet daar aan stelt. In veel gevallen zal de overheid niet over een databankenrecht beschikken, omdat zij niet kwalificeert als producent van een databank, dan wel omdat de databank zelf niet voldoet aan de vereisten van de Databankenwet.

In een uitspraak van de Amsterdamse rechter is bevestigd dat een overheidsorgaan alleen in uitzonderingsgevallen, waarin het los van zijn hoofdactiviteit heeft geïnvesteerd in een databank, een kostendekkende vergoeding kan vragen. In alle andere gevallen dient de informatie op grond van de Wob tegen verstrekkingskosten beschikbaar te worden gesteld – ongeacht het doel waarvoor de informatie is opgevraagd.

Bijlage 1: Rubricering geo-diensten

De in dit rapport vermelde geo-diensten verschillen elk in hun werkwijze. De ene dienst kan alleen gebruikt worden als iemand actief toestemming geeft, zich heeft aangemeld of iets heeft aangeschaft, terwijl men bij andere diensten er simpelweg mee geconfronteerd wordt. In het eerste geval heeft een gebruiker zelf bewust iets van zijn privacy ingeleverd en staat dat in een ander juridisch daglicht dan wanneer iemand een sms-bericht ontvangt van de politie omdat hij op een zeker moment in de buurt was bij een misdrijf.

Tevens kunnen burgers een beroep doen op de overheid om bepaalde (overheids)geo-informatie te verstrekken, waarbij de privacy minder een rol speelt, maar meer de rechten op de geo-informatie van belang zijn.

Daarnaast is het van belang te weten welke juridische regimes van toepassing zijn op de gebruikte systemen, zodat duidelijk is hoe dan moet worden omgegaan met bijvoorbeeld bewaartermijnen of, zoals bij het toezenden van elektronische berichten, dat een abonnee altijd gewezen moet worden op de mogelijkheid een dienst te beëindigen.

Tevens is het belang te weten in welk domein een dienst wordt ingezet, omdat dat weer een aanwijzing kan zijn voor de toepasselijkheid van bepaalde regels, zoals bijvoorbeeld de Wet politiegegevens indien sprake is van verwerking van (persoons)gegevens in het kader van de politietaak.

Dit heeft geleid tot het onderstaande lijstje van criteria die toegepast op de in deze studie genoemde systemen de onderstaande tabel tot gevolg hebben gehad.

Passief of actief
Bij actieve geo-diensten is het de gebruiker zelf die gelokaliseerd of benaderd wenst te worden (bijvoorbeeld een chronische patiënt als houder van een toestel die daarmee medische hulp kan inroepen). Bij passieve locatiediensten wordt de gebruiker gelokaliseerd op verzoek van een derde (bijvoorbeeld het benaderen van personen die in de buurt waren van een misdrijf).

Verplicht of vrijwillig
In bepaalde gevallen kan de burger verplicht worden om diensten af te nemen bij de overheid (bijvoorbeeld bij rampenbestrijding). In andere gevallen heeft de burger een vrije keuze om een dienst af te nemen (bijvoorbeeld assistentie van de politie via sms-alert).

Beleidssector
Voorts zal ook de beleidssector waarbinnen de overheid relaties heeft met burgers mede bepalend zijn voor enerzijds het lokaliseren, classificeren en informeren van burgers (bijvoorbeeld rampenbestrijding door politie, brandweer, GGD, etc., waarbij gebruik wordt gemaakt van cell broadcast).

Maatschappelijk probleem
Geo-diensten kunnen worden ingezet voor het oplossen van tal verschillende maatschappelijke problemen (bijvoorbeeld een verbetering van de uitvoering van taken door de politie en als gevolg daarvan een grotere veiligheid in buurten door gebruik van SMS-alert).

Gegevens
Ten behoeve van een geo-dienst kunnen bepaalde soorten gegevens worden verwerkt, zoals persoonsgegevens, politiegegevens, locatiegegevens en verkeersgegevens. Het soort gegeven bepaalt welk gegevensbeschermingsregime van toepassing is (bijvoorbeeld: Wet bescherming persoonsgegevens, Wet politiegegevens, Telecommunicatiewet).

Geo-dienst	LBS / GIS	Actief / Passief	Verplicht / Vrijwillig	Beleidssector	Maatschappelijk probleem	Gegevens
SMS-alert	LBS	Actief	Vrijwillig	Strafvordering, OO&V	Voorkomen en opsporen strafbare feiten	Persoonsgegevens + politiegegevens
Groeps-SMS	LBS	Passief	Verplicht	Strafvordering, OO&V	Opsporen misdrijven	Politiegegevens + verkeersgegevens
SMS-bom	LBS	Passief	Verplicht	Strafvordering	Opsporen gestolen goederen	Geen
Cell broadcast	LBS	Actief	Vrijwillig	OO&V	Rampenbestrijding, bescherming bevolking	Geen
Kilometerprijs	LBS	Passief	Verplicht	Verkeer, belasting, milieu	Mobiliteit	Persoonsgegevens
Locatiebepaling GSM bij 112	LBS	Actief	Verplicht	OO&V	Commerciële dienstverlening, lokaliseren beller 112	Locatiegegevens + persoonsgegevens
OV-chipkaart	LBS	Passief	Verplicht	Vervoer	Eén vervoersbewijs door heel NL	Persoonsgegevens
Burgernet	LBS	Actief	Vrijwillig	Strafvordering, OO&V	Voorkomen en opsporen strafbare feiten	Persoonsgegevens + politiegegevens
Verlof TBS'er	LBS	Passief	Verplicht	Strafvordering, OO&V	Voorkomen ontsnapping, voorkomen strafbare feiten	Politiegegevens
Noodhulp ouderen GPS	LBS	Actief	Vrijwillig	Zorg	Hulpverlening aan ouderen	Locatiegegevens
GPS locator voertuigen	GIS	Actief	Vrijwillig	Verkeer, strafvordering	Diefstalpreventie, opsporing	Politiegegevens
Google Maps / Google Earth	GIS	Actief	Verplicht	Ruimtelijke ordening	Ondersteuning vraagstukken ruimtelijke ordening	Persoonsgegevens

Bijlage 2: Overzicht privacy/gegevensbescherming geo-toepassingen

Geo-dienst	Inbreuk op rust/privacy (ongevraagd)?	Gegevensbescherming?
Sms-alert	NEE (opt-in)	WBP (verkrijgen) en Wpolg (verwerken)
Groeps-sms	JA	Sv, Wpolg
Sms-bom	JA	Geen persoonsgegevens
Cell broadcast	JA	Geen persoonsgegevens
Km prijs	JA	WBP
Locatiebepaling 112	JA	Tw, Sv
OV-chipkaart	JA, mits anoniem of wegwerpkaart (ook bij betalen via GSM)	WBP, Tw (indien via GSM)
Burgernet	NEE (opt-in)	WBP (verkrijgen) en Wpolg (verwerken)
Verlof Tbs-ers	JA	Sv, Wpolg
Noodhulp ouderen GPS	NEE (opt-in)	Tw, WGBO (medische gegevens)
GPS-locator in auto	JA (indien verplicht)	Wpolg
Geografische info-systemen	JA (bijv Google Street View)	WBP, Kadasterwet

Toelichting:

Bovenstaande tabel geeft per in dit onderzoek behandelde geo-dienst aan of die wel of geen inbreuk maakt op het recht om met rust te worden gelaten (privacy). In het algemeen is geen sprake van een inbreuk daarop als deelname aan de geo-dienst op vrijwillige basis geschiedt. Als wel sprake is van een inbreuk moeten de criteria van art. 8 lid 2 EVRM daarop worden toegepast. Dat betekent dat men zich het volgende dient af te vragen:

- Is de inbreuk bij wet voorzien?
- Is de inbreuk noodzakelijk in een democratische samenleving (in het licht van proportionaliteit en subsidiariteit)?
- Welk belang dient de inbreuk: nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of de bescherming van de rechten en vrijheden van anderen?

Naast de vraag of de inbreuk die op de privacy wordt gemaakt in overeenstemming is met art. 8 EVRM, is een minstens even belangrijke en praktische vraag welke wet(ten) van toepassing is/zijn op de verwerking van gegevens in het kader van de geo-dienst. In de tabel in Bijlage 1 is per geo-dienst aangegeven welke gegevens er worden verwerkt. De soort gegevens is vervolgens van invloed op de gegevensbeschermingswetgeving die van toepassing is op de betreffende geo-dienst.

Bijlage 3: Case study (SMS bij opsporing)

Computerrecht
Aflevering 2008-4
Artikel

Computerrecht 2008, 100. Sms, opsporing en privacy (P.J.A. De Hert, J. Nouwt, I. Voets en J.G.L. van der Wees* [1])

Analyse van de privacyaspecten bij het gebruik van sms voor opsporingsactiviteiten en een pleidooi voor meer transparantie.

In de Rathenau-studie 'Van privacyparadijs tot controlestaat' wordt duidelijk dat politie en justitie steeds meer mogelijkheden hebben om technische middelen in te zetten in het kader van de opsporing van strafbare feiten. Dat leidt tot een steeds grotere druk op het privacygrondrecht.* [2] De in de studie genoemde optelsom van maatregelen heeft destijds wel enig stof doen opwaaien; inmiddels is het ruim een jaar na publicatie van het rapport - ondanks andere, latere, zorgwekkende signalen* [3] - weer stil aan het privacyfront. Oorverdovend stil volgens De Groene Amsterdammer in een themanummer over privacy.* [4]

1 Inleiding

Intussen gaat de technologische ontwikkeling gewoon door en lijken overheidsorganisaties op dit moment erg gecharmeerd te zijn van mobiele technologie. De ene na de andere prachtige toepassing wordt bedacht: sms-alert, sms-bom, kilometerprijs, locatiebepaling van ons mobieltje bij noodhulpdiensten, een anti-diefstal apparaat in onze auto, ov-chipkaart, enz. Nieuwe technologische ontwikkelingen waarbij mobiele apparaten een rol spelen en die ieder voor zich wellicht bijdragen aan een mooiere, betere, veiligere maatschappij, maar opnieuw ten koste van onze privacy? Dat laatste is de vraag en voor ons reden om de oorverdovende stilte rond privacy (en technologie) toch maar weer eens te doorbreken.
In dit artikel zouden wij overigens graag een overzicht hebben gegeven van alle mobiele ontwikkelingen bij de overheid en de daarbij relevante regels inzake de bescherming van de persoonlijke levenssfeer. Gezien het feit dat dit er veel zijn - te veel - hebben wij een keuze gemaakt. Bij het maken van die keuze is het gebruik in de praktijk doorslaggevend geweest. Natuurlijk is het interessant om - bijvoorbeeld - vooruit te lopen op kastjes in onze auto waarin ons rijgedrag wordt vastgelegd, maar misschien komen die kastjes er wel nooit.* [5] Wat wel al in de praktijk gebruikt wordt zijn sms-diensten, zoals sms-alert en groeps-sms. Deze toepassingen worden onder andere ingezet bij opsporing en dit artikel gaat dan ook over sms, opsporing en privacy.
Hierna volgt allereerst een korte beschrijving van sms-alert en groeps-sms. Vervolgens worden, na een korte uiteenzetting over de verschillende gedaanten van privacy, per dienst de privacyaspecten toegelicht. Zoals zal blijken leveren deze sms-diensten niet zozeer privacyproblemen op, als wel problemen met het recht op bescherming van persoonsgegevens. Het gegevensbeschermingsrecht is in dit verband onder meer te vinden in de Wet bescherming persoonsgegevens (Wbp), de Wet politiegegevens (Wpolg) en het Wetboek van Strafvordering (Sv). Deze regelgeving wordt daar waar relevant dan ook nader toegelicht in het kader van sms en opsporing. Het verhaal wordt vervolgens afgesloten met enkele aanbevelingen over privacy, opsporing en het gebruik van sms-diensten.

2 Sms-alert

Sms-alert is een dienst die in politiekringen voor het eerst is gebruikt door het korps Midden en West Brabant. Het is een dienst die dit korps in staat stelt om bewoners te informeren over allerlei zaken die met veiligheid in de wijk te maken hebben. Zo kan de politie via een sms-bericht informatie geven over bijvoorbeeld een inbreker die in de buurt is gesignaleerd of over een buurtbewoner die vermist wordt. Door de burgers erbij te betrekken hoopt de politie dat dit zal leiden tot een snelle aanhouding van de inbreker of tot het vinden van de vermiste persoon. Daarnaast kan de politie via sms-alert preventieberichten versturen. Indien er bijvoorbeeld personen in een buurt actief zijn die met babbeltrucs mensen proberen geld afhandig te maken, kunnen bewoners door middel van een alert daarvoor gewaarschuwd worden.
Behalve voor burgers is er ook een soortgelijke dienst voor winkeliers. In Brabant hebben winkeliers zich aangemeld voor een sms-dienst waarbij berichten verstuurd worden indien de veiligheid van de winkels in het geding is of ander gevaar dreigt. Zo heeft de politie deze winkeliers enige tijd geleden gewaarschuwd dat een man in een winkel had geprobeerd met een vals biljet van €□100 af te rekenen. Omdat de politie vermoedde dat de man dit bij andere winkels ook zou proberen, is een sms-alert verstuurd om de andere winkeliers te waarschuwen.* [6]

3 Groeps-sms

Het zojuist besproken sms-alert wordt ingezet voor opsporing en preventie in bepaalde postcodegebieden. Het is echter heel goed denkbaar dat een incident zich voordoet in een zeker postcodegebied, en dat er op het moment dat het incident plaatsvindt ook mensen in het gebied zijn, die niet wonen in het betreffende gebied. Dan is het wenselijk dat de politie ook die personen zou kunnen benaderen. Het gaat dan eigenlijk om een sms-alert die verzonden wordt naar personen die op een zeker moment op een bepaalde plek aanwezig waren. Ter onderscheid van de sms-alert die in ons land vooral wordt ingezet voor buurtpreventie, noemen wij een dergelijk bericht een groeps-sms. Dit betreft een bericht naar een bepaalde groep mensen, die onafhankelijk van hun woonplaats op een zeker moment iets gemeen hadden, zoals het in de nabijheid zijn van een bepaalde gebeurtenis.
De groeps-sms is door de politie ingezet in een aantal geruchtmakende zaken. Zo heeft de politie een groeps-sms gestuurd naar zo'n drieduizend personen die op 15 november 2005 rond 21.00 uur, de avond dat Louis Sévèke werd vermoord, in het centrum van Nijmegen waren. De politie verzocht in het bericht deze personen 's avonds te kijken naar de uitzending van AVRO's Opsporing Verzocht.
Ook in het kader van het onderzoek naar de moord op Anneke van der Stap heeft de politie een groeps-sms gestuurd, tot twee keer toe zelfs.* [7]
Het middel wordt niet alleen in moordzaken ingezet. De allereerste keer dat het middel in Nederland gebruikt werd, was kort na de rellen die plaatsvonden bij de Rotterdamse Kuip na de wedstrijd Feyenoord-Ajax enige tijd geleden. De politie stuurde destijds een sms naar 17□000 telefoons op zoek naar getuigen.* [8]
In de beschreven gevallen was het doel van het bericht hetzelfde als bij de sms-alert, namelijk assistentie vragen aan burgers. Belangrijk verschil is gelegen in het feit dat een sms-alert alleen ontvangen wordt door een burger die zich daarvoor vrijwillig heeft opgegeven, terwijl bij de groeps-sms zoals beschreven, iedere bezitter van een geactiveerde mobiele telefoon en in de buurt bij een incident, een bericht kan ontvangen.

4 De verschillende gedaanten van privacy

Alvorens in te gaan op de privacyaspecten van sms-alert en groeps-sms besteden we kort aandacht aan de verschillende gedaanten van privacy.
Privacy is in de eerste plaats een recht om met rust gelaten te worden. 'The right to be left alone', zoals Warren en Brandeis dat meer dan honderd jaar geleden al beschreven in hun beroemde artikel 'The Right to Privacy'.* [9] Dat is de kern, maar overigens niet de sluitende definitie. Die is namelijk tot op heden niet gegeven, bewust niet. Althans, niet door het Europees Hof van de Rechten voor de Mens (EHRM) dat in 1992 stelde: 'The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of '*private life*'.'
Wel staat vast dat het Hof vandaag de dag een ruime invulling hanteert van het privacybegrip en daaraan gerelateerde begrippen zoals communicatie en correspondentie.* [10] Zo stelde het Hof in het arrest *Niemietz** [11] over het privacybegrip dat werknemers een gerechtvaardigd belang hebben om ook gedurende het uitvoeren van bedrijfsmatige activiteiten relaties met andere mensen aan te kunnen gaan. Een zekere mate van vrijheid om met anderen al dan niet persoonlijk te kunnen communiceren zonder inmenging door de werkgever is in dat kader onontbeerlijk. Art. 8 EVRM beschermt het individu dus niet alleen tegen inbreuken door de overheid, maar ook tegen inbreuken door particulieren, zoals werkgevers. In het arrest *Halford* maakte het Hof duidelijk dat ook telefoongesprekken, gevoerd met een zakelijk toestel, of onder een zakelijk nummer, onder de bescherming van art. 8 vallen.* [12]
Hiernaast blijkt uit het arrest *P.G. en J.H. vs. het Verenigd Koninkrijk* dat het voortaan denkbaar is om niet alleen in de privé- of professionele sfeer, maar ook in de publieke sfeer een beroep te doen op de bescherming geboden door het privacygrondrecht.* [13] Deze principiële erkenning van het concept *publieke privacy* gebeurde een jaar eerder in het arrest *Rotaru vs. Roemenië*.* [14] Steunend op eerdere arresten zoals *Amann vs. Zwitserland* en verwijzend naar de beginselen van het *data protection*-recht (zie hierna), verklaarde het Hof, in deze zaak over door de overheid opgeslagen persoonsgegevens, dat 'publieke informatie' over een persoon onder de werking van art. 8 EVRM valt, wanneer deze systematisch wordt verzameld of blijvend wordt opgeslagen in overheidsbestanden.* [15]
In het arrest *P.G. en J.H. vs. het Verenigd Koninkrijk* wordt naar deze passage uit *Rotaru* verwezen, maar gaat het Europees Hof verder. Het Hof stelt voorop dat het begrip 'privéleven' een ruim begrip is dat moeilijk te definiëren is. Het begrip omvat in ieder geval het recht op identiteit, op persoonlijke ontwikkeling en het recht op het ontwikkelen en onderhouden van relaties met anderen en de buitenwereld. Deze relaties kunnen ook een zakelijk karakter hebben. Dit betekent dat de bescherming van het privéleven zich tot het publieke domein kan uitstrekken.* [16]
Hiermee is weliswaar geen definitie gegeven, maar is wel duidelijk dat het recht om met rust gelaten te worden verder gaat dan eigen lichaam, huis en tuin. Er is ruimte om uiteenlopende waarden te beschermen.* [17]
Het aantal beschermde waarden is nog toegenomen met het recht op bescherming van persoonlijke gegevens. Dit recht, dat recentelijk als nieuw grondrecht is opgenomen in art. 8 van het Handvest van de Grondrechten van de Europese Unie, overlapt slechts ten dele met het privacyrecht. Het focust tevens op aspecten van procedurele rechtvaardigheid en gelijkheid die aan de orde komen bij het verwerken van persoonsgegevens. Het recht op bescherming van persoonsgegevens legt om die reden ook andere klemtonen dan het privacyrecht. Zo is het bijvoorbeeld verre van evident om een telefoonnummer in alle gevallen te laten vallen onder de bescherming van het privacyrecht, terwijl over de toepassing van het gegevensbeschermingsrecht op telefoonnummers geen enkele

twijfel bestaat. Telefoonnummers zijn immers bijna altijd persoonsgegevens zoals de Registratiekamer in 1993 al aanduidde.
Het (ruime) recht om met rust gelaten te worden en het gegevensbeschermingsrecht spelen een rol bij diensten als sms-alert en de groeps-sms. Deze worden in de volgende paragrafen toegelicht.

5 Sms-alert bekeken vanuit het privacyperspectief

De sms-alert die door verschillende politiediensten wordt gebruikt, is een dienst waarvoor gebruikers (burgers, winkeliers) zich vrijwillig aanmelden. Daarbij verstrekt de aanmelder niet meer gegevens dan het mobiele telefoonnummer, de postcode en het huisnummer. De gegevens die bij sms-alert dus een rol spelen zijn de (statische) adresgegevens van een aanmelder. Natuurlijk heeft men een mobiel telefoonnummer nodig om berichten te kunnen versturen naar de aangemelde personen, maar waar deze personen zich bevinden op het moment dat het bericht verstuurd wordt, is niet relevant. Zo kan iemand die de dienst niet tijdelijk op pauze zet als hij op vakantie gaat, een sms-alert ontvangen, terwijl hij bijvoorbeeld in Italië zit.
Met de aanmelding voor een sms-alert-dienst van de politie levert iemand iets in van zijn privacy. Men geeft als het ware aan dat de politie zijn rust mag verstoren als er iets gebeurt in de buurt van zijn woonadres, waarvan de politie het nodig vindt dat hij daarvan op de hoogte wordt gebracht. Dat kan iets betreffen waarbij de politie assistentie nodig heeft, of het kan een bericht zijn ter voorkoming van een misdrijf. In het eerste geval kan men denken aan het zoeken naar een vermiste burger, in het tweede aan bijvoorbeeld een waarschuwing dat er in de buurt iemand gesignaleerd is die door middel van een babbeltruc mensen probeert op te lichten.
Het is in dergelijke gevallen de burger die van zijn zelfbeschikkingsrecht gebruikmaakt en er daarbij dus voor kiest iets van zijn privacy in te leveren. Het ontvangen van een sms-bericht in het kader van de dienst waar men zich vrijwillig voor opgegeven heeft, is dus overduidelijk geen inbreuk op de privacy van de aanmelder.

6 Sms-alert bekeken vanuit het gegevensbeschermingsrecht

Iets anders betreft de gegevens van de personen (abonnees) die zich hebben aangemeld. Deze abonnees overleggen het nummer van hun mobiele telefoon, hun postcode en het huisnummer. Zijn dit nu persoonsgegevens of politiegegevens? Zijn het gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (art. 1 Wbp) óf zijn het gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon die in het kader van de uitoefening van de politietaak worden verwerkt (art. 1 Wpolg)? Is dus de Wet bescherming persoonsgegevens van toepassing of de Wet politiegegevens?
Volgens de Registratiekamer vormen combinaties van postcode en huisnummer samen persoonsgegevens.* [18]
Het gaat immers om gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Vraag is nu of de gegevens van personen die zich hebben aangemeld voor een alert worden verkregen en verwerkt in het kader van een politietaak.
Er is iets te zeggen voor een positief antwoord op deze vraag. Ook binnen de politiewereld gaat men daarvan uit.* [19] Bestudering van de Wet politiegegevens en de bijbehorende memorie van toelichting maakt evenwel duidelijk dat de wet niet is geschreven voor iets als de verkrijging van gegevens van mensen die zich vrijwillig hebben aangemeld bij een sms-alert. Het gaat in die wet om de verwerking van gegevens bij een politietaak.
In de memorie van toelichting staat onder meer:
Bij de uitvoering van de dagelijkse politietaak komt de politie in contact met veel burgers ter zake van zeer diverse gebeurtenissen. Het gaat bijvoorbeeld om burgers die zich om hulp tot de politie wenden, betrokken zijn bij verstoringen van de openbare orde, meldingen van overlast doen, aangifte doen of slachtoffer, getuige of verdachte zijn van een strafbaar feit.
* [20]
Een burger komt dus naar aanleiding van een gebeurtenis in aanraking met de politie en op grond daarvan worden gegevens verwerkt. In het geval van aanmelding voor een sms-alert is er geen gebeurtenis, maar geeft men vrijwillig aan bereid te zijn de politie te helpen en/of dat men op de hoogte gehouden wil worden van bepaalde zaken die zich in de woonomgeving afspelen. Als er vervolgens een gebeurtenis plaatsvindt, dan worden de gegevens verwerkt en wordt een nader bepaalde groep aangemelde burgers om assistentie gevraagd of gewaarschuwd, maar dat is een fase verder. De gegevens van de deelnemers aan de alert-dienst staan daartoe klaar. De verkrijging van de gegevens vindt dus niet plaats in het kader van de politietaak, die volgens art. 2 van de Politiewet zowel de daadwerkelijke handhaving van de rechtsorde betreft als het verlenen van hulp aan die deze behoeven. Er is bij verkrijging nog geen sprake van een concrete taak waarbij de gegevens ingezet en verwerkt gaan worden.
Hierbij komt dat de Wpolg geen betrekking heeft op de *verkrijging* van politiegegevens.* [21] De wet geeft regels voor de *verwerking* van persoonsgegevens die in het kader van de uitvoering van de politietaak zijn verkregen. Hoe gegevens verkregen zijn, stoelt op een andere basis; op vrijwilligheid in het geval van de aanmelding voor een alert, op basis van bijvoorbeeld de Wet vorderen gegevens telecommunicatie indien de politie mobiele telefoonnummers voor een groeps-sms wil gebruiken. Dus de gegevens van de vrijwillig bij een alert aangesloten personen worden politiegegevens op het moment van verwerking voor het inzetten bij een alert. Het *verkrijgen* van de gegevens van de betreffende personen valt niet onder de Wpolg.
Los van het bovenstaande zou het ook niet echt praktisch zijn als de verkrijging van abonneegegevens voor sms-alert onder de Wpolg zou vallen. Politiegegevens dienen namelijk uiterlijk vijf jaar na de eerste verwerking

verwijderd te worden uit de politiebestanden, aldus art. 8 lid 6 Wpolg. Bovendien zijn politiegegevens een jaar na de eerste verwerking al niet meer vrij toegankelijk (art. 8 lid 1 Wpolg). Ze verdwijnen dan 'achter een schot' aldus de MvT.
Moeten dan jaarlijks of vijfjaarlijks de abonneegegevens opnieuw toegestuurd worden door de personen die zich vrijwillig hebben aangemeld, omdat de politie hun gegevens anders niet meer (zomaar) kan inzetten? De vraag is bovendien of het dan wel weer mag, want het zijn immers dezelfde persoonsgegevens die dan weer ingezet worden.
Is dan het regime van de Wbp van toepassing op de (vrijwillige) *verkrijging* van gegevens in het kader van een sms-alert? De vraag die dan aan de orde dient te komen is of er sprake is van een verwerking van die gegevens in het kader van Wbp. De Wbp beschrijft de verwerking van persoonsgegevens als elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Volgens de memorie van toelichting bij de Wbp is het verkrijgen van gegevens een vorm van verwerken van gegevens. Dit betekent naar onze mening dat het verkrijgen van gegevens van personen die zich vrijwillig aanmelden voor sms-alert een verwerking is in de zin van de Wbp.
Dit brengt de volgende interessante vraag naar voren: is de verwerking van de gegevens van personen die zich hebben aangemeld voor sms-alerts bij de verschillende korpsen volgens de regels van de Wet bescherming persoonsgegevens aangemeld bij het CBP (art. 27 e.v. Wbp)? Raadpleging van het openbare meldingenregister en navraag bij de korpsen heeft geleerd dat dat niet het geval is.
Er dient dus onderscheid gemaakt te worden tussen de verkrijging van de gegevens door de politie en de verwerking van de gegevens bij een politietaak. Op het eerste is de Wbp van toepassing, op het tweede de Wpolg.
Los van de kwestie of de Wbp, de Wpolg of beide een rol spelen bij sms-alert, is het niet echt duidelijk wat er nu precies gebeurt met de gegevens van de personen die zich hebben aangemeld bij een alert-dienst. Wordt bijvoorbeeld het mobiele nummer (wellicht met postcode en huisnummer) doorgegeven aan een telecomprovider ter versturing van een sms-alert of voert de politie de verzending van de sms zelf uit? Worden gegevens bij opzegging onmiddellijk verwijderd? En hoe zit dat met gegevens die zijn ingezet bij een alert en als gevolg daarvan onder het regime van de Wpolg vallen?
Daarnaast is er sprake van dat de politie behalve het 06-nummer, de postcode en het huisnummer andere gegevens, zoals het bezit van een hond, zou willen gaan opslaan van de personen die meedoen aan de alert. Is het dan zo dat de politie in het geval van een incident met een persoon en een hond in een bepaalde buurt, even de databank van de alert raadpleegt om snel te bekijken wie mogelijk bij het incident betrokken zou kunnen zijn? Een dergelijk gebruik is vanzelfsprekend zeer ongepast, schaadt het vertrouwen van de burger, en is absoluut niet in overeenstemming met het doel van de verzamelde gegevens. Ter bevordering van de transparantie is het dan ook het overwegen waard het proces van opslag en verwerking van de gegevens, en wat er wel en niet mee gedaan zal worden op te nemen in een gedragscode. Het zou duidelijkheid verschaffen en vertrouwen in alert-diensten doen toenemen.

7 Groeps-sms bekeken vanuit het privacyperspectief

Eerdergenoemde praktijkvoorbeelden geven aan dat iemand die in het bezit van een mobiele telefoon in de buurt is geweest van een ernstig incident de kans loopt dat hij een sms-bericht ontvangt van de politie. Uiteraard moet de mobiele telefoon dan wel aangestaan hebben. Als dat niet het geval is, zendt de telefoon immers geen signaal uit.
De ontvangst van het bericht, verstuurd in het kader van een groeps-sms, verstoort overduidelijk iemands rust. Gezien het feit dat het middel (vooralsnog) slechts wordt ingezet bij ernstige incidenten, zou dat echter tot de overweging kunnen leiden dat die toch wel minimale verstoring van de rust, niet opweegt tegen het belang van de opsporing van de dader(s) en het om die reden is toegestaan.
In dit kader is het van belang te weten dat art. 10 van onze Grondwet in lid 2 vermeldt dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. En om iemand die in de buurt is geweest van een ernstig incident een bericht te kunnen sturen, heeft de politie een persoonsgegeven nodig: het nummer van de mobiele telefoon.* [22] Vraag is nu of er wetgeving is die het toestaat in bepaalde gevallen persoonsgegevens op te vragen en de rust van een persoon te verstoren. In de volgende paragraaf wordt daar nader op ingegaan.

8 Groeps-sms bekeken vanuit het gegevensbeschermingsrecht

Zoals gezegd, de politie heeft de nummers nodig van de mobiele telefoons van de personen die in de buurt waren van een ernstig incident om deze te kunnen benaderen. Eerder werd opgemerkt dat het CBP reeds in 1993 heeft gesteld dat telefoonnummers (bijna altijd) persoonsgegevens zijn. Daar kunnen we nog een CBP-onderzoek van recenter datum aan toevoegen waarin het college stelt dat een telefoonnummer een persoonsgegeven is, omdat het onder meer bedoeld is als middel tot toegang en als middel tot identificatie van gebruikers. Als een nummer zonder onevenredige inspanning kan leiden tot identificatie van een persoon, wordt dit nummer als een persoonsgegeven beschouwd, aldus het CBP. Waarna het vervolgt dat bij telefoonnummers gevorderd door

opsporende instanties waarbij er nog geen NAW-gegevens zijn opgevraagd, sprake is van persoonsgegevens omdat het voor opsporende instanties relatief weinig inspanning kost de bijbehorende NAW-gegevens alsnog te achterhalen.* [23]
Vraag is nu op basis van welke regels opsporende instanties telefoonnummers - en dus persoonsgegevens - mogen opvragen, om vervolgens met behulp van die telefoonnummers de rust te verstoren van de personen die in de buurt waren van een ernstig incident. De wet die deze mogelijkheid schept is te vinden in het Wetboek van Strafvordering. Sinds september 2004 is dit wetboek aangepast waardoor nauwkeurig bepaald kan worden welke *telecommunicatieverkeersgegevens* van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst (telefoon, fax, internet en e-mailverkeer) gevorderd kunnen worden.* [24] Met deze wet zijn naast de verkeersgegevens, gegevens over de gevoerde of nog te voeren communicatie, de zogenaamde *gebruikersgegevens* (naam, adres, postcode, woonplaats, nummer en soort dienst waarvan personen gebruikmaken) geïntroduceerd als gegevens die ten behoeve van de strafvordering en door de inlichtingen- en veiligheidsdiensten kunnen worden opgevraagd.
Biedt deze wet nu de mogelijkheid aan de politie om in een geval als dat van Louis Sévèke de telefoonnummers op te vragen van de personen die ten tijde van de moord in de buurt waren? Nummers dus van personen die (nog) niet als verdachte zijn aangemerkt zijn, maar die slechts in de buurt waren en de politie dus mogelijk van nuttige informatie zouden kunnen voorzien?
Art. 126na van het Wetboek van Strafvordering (Sv) stelt dat in geval van verdenking van een misdrijf een opsporingsambtenaar in het belang van het onderzoek een vordering kan doen gegevens te verstrekken ter zake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst. Moeten we uit dit artikel nu opmaken dat alle personen die ge-sms't zijn na de moord op Sévèke, maar ook na de voetbalrellen en de moord op Anneke van der Stap - zo'n 50□000 in totaal - verdacht waren van een misdrijf? Of was dat wellicht helemaal niet noodzakelijk om de gegevens te mogen opvragen?
Art. 126na Sv spreekt weliswaar over verdenking van een misdrijf, maar er staat niet met zoveel woorden dat de verdenking moet slaan op een verdachte gebruiker. Degene wiens gegevens in het kader van art. 126na Sv afgetapt mogen worden, lijkt dus niet dezelfde te hoeven zijn als de verdachte. De memorie van toelichting beaamt dit ook. Daarin staat dat de bevoegdheid tot het vorderen van telecommunicatiegegevens door de Wet vorderen gegevens telecommunicatie in vijf opzichten wordt gewijzigd. Een van deze opzichten betreft de eis dat de vordering alleen betrekking kan hebben op gegevens betreffende de verdachte. Deze eis is door deze wet komen te vervallen. De memorie van toelichting stelt daarover dat het vorderen van gegevens jegens andere personen dan de verdachte kan bijdragen aan de opsporing. Het kan bijvoorbeeld nodig zijn na te gaan met welke personen een slachtoffer van een misdrijf contacten heeft gehad vlak voordat het misdrijf werd gepleegd. Op die manier kan men op het spoor van de verdachte komen. Dit kan er dan weer aan bijdragen dat weloverwogen kan worden besloten tot het op een selectieve en effectieve wijze aftappen van telecommunicatie, aldus de memorie van toelichting.* [25]
Het feit dat er een misdrijf heeft plaatsgevonden kan er dus toe leiden dat telecommunicatiegegevens opgevraagd worden van gebruikers niet zijnde de verdachte. De hierboven staande argumentatie waarom dat moet kunnen, lijkt echter wel aan te geven dat de personen van wie de gegevens gevorderd worden dicht bij de daad, dicht bij het slachtoffer moeten staan.
Dit is ook in overeenstemming met het vereiste dat de toepassing van de bevoegdheid tot het vorderen van verkeersgegevens dient plaats te vinden 'in het belang van het onderzoek'. Temeer daar het een bevoegdheid betreft tot het vorderen van gegevens van derden die door particulieren voor specifieke doeleinden zijn vergaard en die dan dus aangewend gaan worden voor andere doeleinden. Een goede afweging van enerzijds het belang dat zorgvuldig wordt omgegaan met persoonsgegevens en anderzijds het opsporingsbelang is dan ook vereist.* [26] Daarbij speelt onder meer een rol dat de bevoegdheid inzake gebruikersgegevens betrekking heeft op een beperkte categorie gegevens: naam, adres, woonplaats, nummer en soort dienst. De memorie van toelichting stelt hierover dat het vorderen van de gebruikersgegevens niet leidt tot een min of meer volledig beeld van bepaalde aspecten van iemands leven. Met andere woorden, aan het vorderen van dit soort (persoons)gegevens moet niet zo zwaar getild worden.
Gezien het feit echter dat er sprake is van gegevens die voor een ander doel worden gebruikt dan waartoe ze verzameld zijn, dient er wel een toetsing plaats te vinden met het oog op de omgang met persoonsgegevens in relatie tot het opsporingsbelang.
In dit kader wordt in de memorie van toelichting verwezen naar het Databeschermingsverdrag van de Raad van Europa.* [27] Art. 9 van het verdrag bepaalt namelijk dat doelafwijkend gebruik mogelijk is, indien dit bij wet is voorzien en noodzakelijk is in een democratische samenleving in het belang van het bestrijden van strafbare feiten. Er dient dus voldaan te worden aan het noodzakelijkheidscriterium. Bovendien dient de vergaring van gegevens rechtmatig te zijn en dient zij niet bovenmatig te zijn.
Over het noodzakelijkheidscriterium in relatie tot het vorderen van gebruikersgegevens wordt vervolgens in de memorie van toelichting gesteld dat dit soort gegevens een opsporingsambtenaar in staat stelt te weten met welke persoon hij te maken heeft, als hij een bepaald nummer of adres heeft, dan wel welk nummer een bepaalde persoon heeft. Dit zou een onmisbaar onderdeel van veel strafrechtelijke onderzoeken zijn. Men heeft dan namelijk bij de start van een onderzoek kennis van enkele feiten en personen en men kan door het vergaren van aanvullende gegevens verbanden leggen. Daarnaast zijn de gebruikersgegevens ook nodig alvorens andere bevoegdheden kunnen worden toegepast, bijvoorbeeld de bevoegdheid tot het vorderen van verkeersgegevens en de bevoegdheid tot het opnemen van telecommunicatie. Deze bevoegdheden kunnen namelijk pas worden toegepast wanneer de gebruiker in samenhang met het nummer van telecommunicatie kan worden

geïdentificeerd. Het belang dat de opsporingsinstanties bij deze categorie gegevens hebben is dus groot. Er wordt daarom voldaan aan het noodzakelijkheidscriterium, aldus de memorie van toelichting.
Men kan zich nu afvragen of hetgeen in de memorie van toelichting gesteld wordt, geschreven is met een toepassing als groeps-sms in het achterhoofd. Het lijkt veel meer te wijzen op een beperkte kring rond een verdachte of een slachtoffer, maar niet op willekeurige passanten. Wij stellen dan ook dat terughoudendheid in acht genomen moet worden bij het inzetten van het middel van de groeps-sms en de daaraan gekoppelde eis daarvoor eerst gebruikersgegevens te moeten opvragen. Het dient niet te pas en te onpas ingezet te worden. Het opsporingsbelang dient het niet altijd zomaar te winnen van het privacybelang. Met andere woorden, de eisen van subsidiariteit en proportionaliteit zijn van groot belang bij de afweging tot het vorderen van gebruikersgegevens over te gaan. Overigens wijst het aantal keren dat groeps-sms is ingezet erop dat de opsporingsautoriteiten daarbij zorgvuldig te werk gaan.
Mocht men na zorgvuldige overweging hebben besloten gebruikersgegevens op te vragen en te gebruiken voor een groeps-sms, dan zijn dit gegevens die worden verwerkt in het kader van de uitoefening van een politietaak en zijn het dus politiegegevens in het kader van de Wet politiegegevens. Gegevens die in die gevallen dus ingevolge art. 8 van Wpolg gedurende een periode van één jaar na de datum van de eerste verwerking verwerkt mogen worden en die uiterlijk vijf jaar na de datum van eerste verwerking verwijderd moeten worden. Het feit dat deze gegevens dus nog aan nadere verwerking onderworpen kunnen worden en vijf jaar lang bewaard mogen blijven, zijn redenen temeer zorgvuldig met het middel van groeps-sms om te gaan, daar waar het willekeurige passanten betreft.
Het laatste lijkt ons een reden om *ook* voor de groeps-sms een gedragscode op te stellen.

9 Conclusie: een gedragscode?

Van de nieuwe overheidsdiensten waarbij gebruikgemaakt wordt van mobiele technologieën hebben wij een tweetal sms-diensten toegelicht die een rol spelen bij de opsporing: sms-alert en groeps-sms.
In het geval van sms-alert lijkt met name onduidelijkheid te bestaan over het regime waaronder de vrijwillige verkrijging van de persoonsgegevens valt, Wbp of Wpolg. Op basis van de memorie van toelichting van de Wpolg kan gesteld worden dat de *verkrijging* niet onder deze wet valt. Bij verkrijging is er geen sprake van een concrete politietaak en de Wpolg betreft de verwerking van gegevens, niet de verkrijging. De Wbp daarentegen lijkt wel op deze *verkrijging* van toepassing en dat betekent dat deze aan de eisen van de Wet bescherming persoonsgegevens dient te voldoen. Dit punt verdient dan ook aandacht voor de korpsen die sms-alert aanbieden. Op het moment dat gegevens van deelnemers daadwerkelijk ingezet worden bij een sms-alert vindt de *verwerking* wel plaats in het kader van een politietaak en is dus de Wpolg van toepassing. Hierover lijkt geen misverstand te bestaan.
Bij de groeps-sms heeft het er alle schijn van dat deze weloverwogen wordt ingezet bij schokkende gebeurtenissen waarbij de opsporing lastig is of dreigt vast te lopen. Hier blijft echter het gevaar van disproportioneel gebruik op de loer liggen. Met name omdat de persoonlijke levenssfeer van willekeurige burgers - niet zijnde verdachten - met dit instrument gemakkelijk geraakt kan worden als gevolg van de intrede van de Wet vorderen telecommunicatiegegevens.
Welke wet wanneer van toepassing moge zijn, het is voor personen van wie de gegevens op vrijwillige basis of op basis van bijvoorbeeld de Wet vorderen gegevens telecommunicatie worden gebruikt, bij respectievelijk sms-alert en groeps-sms, onduidelijk wat er door wie en voor welke periode met hun gegevens wordt gedaan. Het lijkt ons om die reden verstandig dat er een gedragscode komt voor het gebruik van sms-diensten door de overheid. En wellicht ook een specifieke code voor het gebruik van dit soort diensten door politie en justitie. Burgers zullen immers een ander gevoel hebben over hun opgeslagen gegevens bij de politie, dan over de opslag van diezelfde gegevens bij bijvoorbeeld een waterbedrijf. Het dient een code te zijn waarin, in tegenstelling tot de sms-gedragscode van commerciële partijen* [28] , onder meer is opgenomen wat er gebeurt met de opgeslagen gegevens. In feite dus een gedragscode annex *privacy statement*. Zo kan inzake de alert-dienst bij aanmelding duidelijk gemaakt worden dat gegevens onder het regime van de Wbp vallen en als gevolg daarvan aan bepaalde eisen voldoen en dat bij daadwerkelijke inzet bij een alert de gegevens gaan vallen onder de Wpolg met verschillende gebruiksvoorwaarden en termijnen als gevolg. Dat het laatste ook het geval is in geval van inzet bij een groeps-sms zou door middel van een code ook duidelijk gemaakt kunnen worden aan de personen die in het kader van een groeps-sms benaderd worden. Dat kan bijvoorbeeld door middel van een simpele verwijzing naar een webadres van de code tegelijkertijd met de verzending het sms-bericht. Het zal de broodnodige transparantie vergroten en leiden tot een *privacy compliant*-inzet van een mobiele technologie als sms bij opsporing.

---

*[1] Dr. Paul De Hert, dr. mr. Sjaak Nouwt, mevr. Irene Voets en mr. Leo van der Wees zijn werkzaam bij het Tilburg Institute for Law, Technology, and Society (TILT) van de Universiteit van Tilburg als respectievelijk universitair hoofddocent, universitair docent, student-assistent en onderzoeker.

*[2] 'Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw', Anton Vedder, Leo van der Wees, Bert-Jaap Koops en Paul de Hert, Rathenau Instituut, 2007. In te zien via *www.rathenau.nl*.

*[3] Zie bijvoorbeeld Voorzitter CBP: 'Nederland hard op weg controlestaat te worden', 12 mei 2007, *www.recht.nl/28620* en 'Vrijwillig op weg naar de politiestaat', *NRC Handelsblad* 2 april 2008,

www.recht.nl/32180.

*[4] 'Gluurstaat. De oorverdovende stilte rond privacy', *De Groene Amsterdammer* 2008, nr. 13.

*[5] 'Kastje voor volgend kabinet', *NRC Handelsblad* 7 februari 2008.

*[6] 'Politie stuurt groeps-sms over vals geld', *Zibb.nl* 21 juli 2006 (www.zibb.nl, vul 'groeps-sms' in in het zoekveld).

*[7] 'Tweede SMS actie in zaak Anneke van der Stap', *Rijksrecherche.nl* 11 september 2006 (www.rijksrecherche.nl, vul 'anneke' in in het zoekveld).

*[8] 'Politie spoort hooligans op met sms', *Webwereld* 31 augustus 2005 (www.webwereld.nl vul 'hooligans' in in het zoekveld).

*[9] Samuel Warren & Louis Brandeis, 'The Right to Privacy', *Harvard Law Review*, No. 5, 1890. Dit artikel is onder meer beschikbaar op de website van de Lawrence University, Appleton, Wisconsin, www.lawrence.edu.

*[10] In *Klass* bepaalde het EHRM dat ook telefoonverkeer onder de bescherming van art. 8 valt. Het Hof kiest daarbij niet voor een extensieve interpretatie van het begrip 'correspondentie' maar voor een combinatie van privéleven en correspondentie. In *Malone* gaf het Hof aan dat ook *metering records* en in het bijzonder het gekozen telefoonnummer integraal deel uitmaken van de beschermde communicatie. Zie EHRM 2 augustus 1884, NJ 1988, 534 (*Malone*). In het arrest *P.G. en J.H. vs. het Verenigd Koninkrijk* (*infra*) is het EHRM van mening dat de opname van het stemgeluid aangemerkt dient te worden als een registratie van een persoonsgegeven (§ 59) en onder de werking van art. 8 EVRM valt (§ 60). Tevens wordt het opvragen van de nummers die gedraaid waren met de telefoon eveneens gezien als een handeling die onder toepassing van het privacygrondrecht valt. Over nieuwere toezichttechnieken zijn nog geen uitspraken. Over het algemeen wordt echter aangenomen dat het EHRM te zijner tijd door een verdragsdynamische interpretatie ook e-mail onder art. 8 zal brengen. Zie H.H. de Vries, 'Vertrouwelijkheid van e-mail in arbeidsverhoudingen', in: H.W.K Kaspersen & C. Stuurman, *Juridische aspecten van e-mail*, Deventer: Kluwer 2001, p. 111-139, m.n. p. 116-117; L. Ascher & W. Steenbruggen, 'Het Emailgeheim op de werkplek. Over de toelaatbaarheid van inbreuken op het communicatiegeheim van de werknemer in het digitale tijdperk', NJB 2001, 37, p. 1788.

*[11] EHRM 16 december 1992, NJ 1993, 400 (*Niemietz*).

*[12] EHRM 25 juni 1997, NJ 1998, 506 (*Halford*). Mevrouw Halford was Assistant Chief Constable bij een Engels politiekorps. In verband met een rechtszaak tegen haar werkgever wegens ongelijke behandeling had zij de beschikking over een tweede telefoon die was uitgezonderd van de standaardcontrole van de telefoons van het politiebureau. Uit het bewijs dat in de rechtszaak was overlegd, kon worden afgeleid dat de werkgever waarschijnlijk de gesprekken die via de speciale telefoon waren gevoerd, had afgeluisterd. Het Hof overwoog dat 'the right to private life and correspondence' zich ook uitstrekt tot de werkplek. Omdat er geen waarschuwing was gegeven dat de telefoongesprekken werden opgenomen, had zij een 'reasonable expectation of privacy', hetgeen werd versterkt door bijkomende factoren waaronder het feit dat de telefoon specifiek ter beschikking was gesteld voor privégebruik. Het enkele bekend zijn van de mogelijkheid tot meeluisteren of opnemen rechtvaardigt op zichzelf het gebruik daarvan evenwel niet. Kenbaarheid van de (mogelijkheid tot) controle is niet meer dan een basisvoorwaarde voor de rechtmatigheid ervan.

*[13] EHRM 25 september 2001 (*P.G. en J.H. vs. Verenigd Koninkrijk*). Zie P. De Hert, 'Het Europees Hof Rechten van de Mens erkent publieke privacy. De legaliteitseis en het politioneel optreden in het licht van art. 8 EVRM', *Nieuw Juridisch Weekblad* 2002, vol. 1/4, 9 oktober, p. 116-122.

*[14] EHRM 4 mei 2000 (*Rotaru vs. Roemenië*), *ECHR* 2000-V. Het arrest is tevens opgenomen in *Revue trimesterielle des droits de l'homme* 2001, p. 138-183, m.nt. O. De Schutter.

*[15] EHRM (*Rotaru vs. Roemenië*), *l.c.*, § 43.

*[16] Zie EHRM 25 september 2001 (*P.G. en J.H. vs. het Verenigd Koninkrijk*), § 56. Ten aanzien van het antwoord op de vraag wanneer zich een inmenging in het privéleven voordoet ingeval een persoon zich in het publieke domein bevindt, is volgens het Hof een aantal factoren relevant. In een situatie waarin iemand weet dat hij gefilmd wordt of anderszins wordt waargenomen, zijn *reasonable expectations of privacy* van belang, maar niet doorslaggevend. Het privéleven komt in het geding wanneer het (opgenomen) materiaal systematisch of blijvend wordt opgeslagen. Het is daarom dat het EHRM eerder heeft uitgemaakt (in de zaak *Rotaru* vs. *Roemenië*) dat een dossier met daarin de door de veiligheidsdienst verzamelde gegevens over een persoon onder de werking van art. 8 EVRM valt, ook in geval de gegevens niet op een heimelijke of slinkse wijze zijn verkregen. Het Hof wijst verder nog op de zaak *Amann vs. Zwitserland*, waarin het aannam dat een kaartsysteem met gegevens over de klager een inbreuk op zijn privéleven vormde, ook al betrof het geen gevoelige gegevens en ook al waren deze waarschijnlijk nooit geraadpleegd.

*[17] Zie ook A. Vedder, 'Huidige bescherming privacy loopt ver achter', *Trouw* 23 oktober 2007. Een verwijzing naar het artikel staat op *Recht.nl*, www.recht.nl/30387.

*[18] Registratiekamer 21 juni 1996, 95.O.043.

*[19] Zoals blijkt uit de notitie 'SMS-Alert en de privacywetgeving', van Vts-Politie Nederland.

*[20] *Kamerstukken II* 2005/06, 30□327, nr. 3, p. 10.

*[21] *Kamerstukken II* 2005/06, 30□327, nr. 3, p. 25.

*[22] Registratiekamer 8 juli 1993, 93.A.002.

*[23] Onderzoek fotopublicaties op internet, CBP 23 februari 2006, *www.cbpweb.nl*.

*[24] Eerste Kamer stemt in met wetsvoorstel Vorderen gegevens telecommunicatie, 17 maart 2004, *www.recht.nl/16884*.

*[25] *Kamerstukken II* 2001/02, 28□059, nr. 3, p. 9.

*[26] *Kamerstukken II* 2001/02, 28□059, nr. 3, p. 3-6.

*[27] 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. CETS No. 108', *Trb*. 1988, 7 of zie *www.conventions.coe.int*, klik op 'Full list' en zoek 'verdrag 108'.

*[28] 'Vernieuwde SMS-gedragscode', *Recht.nl*, 4 maart 2008, *www.recht.nl/31864*.

