GEONOVUM

TUSSEN WILLEN WETEN

EN WETTEN

Privacy op zijn plaats

Angélique van Oortmarssen, Marc de Vries
en Bastiaan van Loenen

Privacy op zijn plaats

Tussen willen weten en wetten

Witboek over de spanning tussen privacyregels

en het realiseren van het locatie-informatie potentieel

Including English management summary

Angélique van Oortmarssen, Marc de Vries

en Bastiaan van Loenen

Ten geleide

Dataficatie is de stoommachine van de 21e eeuw. De (potentiële) baten hiervan zijn ongekend: eeuwenoude marktbarrières worden geslecht, door praktisch iedere sector waait een innovatieve storm, consumentensurplus explodeert, wetenschappers zien verbanden die voorheen onzichtbaar waren, (verzamelingen) van burgers krijgen een krachtige stem en overheden kunnen hun taken veel beter, sneller en goedkoper verrichten. Tegelijkertijd worden daarbij traditionele relaties tussen en rollen van overheid, burgers en bedrijven overhoop gehaald.

Zo ook in de wereld van de geo-informatie. Geo-informatie vormt de basis voor het duiden, vastleggen, regelen, handhaven en sanctioneren van gebeurtenissen en gedragingen. Ontwikkelingen in en vooral de enorme verspreiding en onderlinge verbondenheid van digitale technologie leidt ertoe dat 'locatie' het koppelvlak is geworden van data uit een veelheid van bronnen. Geo-informatie is hierdoor veranderd van een 'plekje in de Bosatlas' tot een culminatiepunt van data, waaronder data die, zeker in onderling verband, in toenemende mate herleidbaar zijn tot een persoon. Dat plaatst gebruikers van geo-informatie – en hen die zich inzetten voor het goed gebruik daarvan – in een nieuw speelveld: dat van de bescherming van persoonsgegevens.

De spanning die hieruit voortkomt is evident: geo-informatie wil stromen, juist in het (grootschalig) gebruik zit de waarde. Privacybescherming is evenwel juist gericht is op het minder uitbundig delen van persoonsgegevens, waaronder dus ook locatie-informatie die te relateren is aan personen. Deze spanningen manifesteren zich inmiddels dan ook in de uitvoeringspraktijk van bedrijven en overheden en leiden steeds meer en vaker tot onzekerheden, kunstgrepen en suboptimale benutting van het (locatie-informatie) potentieel.

Daarnaast zijn er externe ontwikkelingen die het onderwerp enige urgentie geven. Zo heeft Commissievoorzitter Juncker het onderwerp ‘Rapidly concluding negotiations on common EU data protection rules’ bovenaan zijn actielijstje gezet ter realisatie van de ‘digital single market’. Het is zijn ambitie dit proces binnen zes maanden na aantreden af te ronden. Of er plaats is voor een fundamentele herziening valt te bezien. Het voorstel dat thans op tafel ligt, verdient echter nadere discussie. Onder meer daar waar het gebruik van locatie-informatie betreft.

Op nationaal niveau springt het initiatief voor een verkenning naar het opstellen van een kaderwet Gegevensuitwisseling in het oog. Deze verkenning beoogt vooralsnog het bevorderen van fraudebestrijding (onder meer door middel van profiling, maar heeft in potentie een bredere toepassing en kent ongetwijfeld precedentwerking voor de bescherming van privacy binnen het geo-domein. Ook hier zou het goed zijn de geo-belangen voor het voetlicht te brengen, vanuit een eigen visie op de oplossing van dit vraagstuk.

Reden waarom de Programmaraad van Geonovum opdracht heeft gegeven hierover een Witboek te schrijven: een stuk dat genoemde ontwikkelingen beschrijft, de spanningen – en de urgentie deze te adresseren – duidt en de onderwerpen agendeert in de juiste fora.

Dit Witboek wil een op feiten gebaseerde dialoog op gang te brengen tussen hen die verantwoordelijk zijn voor een goed gebruik van locatie-informatie en hen die de privacyregels maken en toezien op de naleving ervan. Daartoe schetst het de technologische ontwikkelingen en de rol die locatie-informatie hierin speelt (hoofdstuk 1) en de huidige wettelijke kaders waarbinnen dat moet gebeuren (hoofdstuk 2). Vervolgens beschrijft het de omgang in de praktijk met de technologische mogelijkheden en de regels die deze werelden aan elkaar proberen te knopen (hoofdstuk 3) om af te sluiten met enkele observaties rond de door de praktijk ervaren spanningen en het duiden van een mogelijk proces om te komen tot oplossingsrichtingen (hoofdstuk 4).

Denkend vanuit de missie van Geonovum – het bevorderen van het goed gebruik van geo-informatie binnen de publieke sector – staat het goed gebruik van locatie-informatie door de overheid centraal. Tevens gaat dit Witboek vooral over Nederland. Slechts daar waar het ‘buitenland’ het gebruik of de regels raakt – denk daarbij onder meer aan Europese regelgeving rond privacybescherming – kijken we over de grenzen heen.

Om dit Witboek te kunnen maken, is gesproken met een breed palet aan betrokkenen: naast overheidsorganisaties, zijn ook toezichthouders, bedrijven, civil society organisaties en domeinexperts geïnterviewd. Dit vertaalt zich door in de geformuleerde oplossingsrichtingen: bij het voeren van de dialoog en het vinden van de weg naar voren zullen ook andere belanghebbenden (dan de overheid) moeten aanschuiven. Hierbij valt te denken aan koepelorganisaties van de bedrijven die zich bezighouden met de productie en verwerking van geo-informatie (zoals Geo-Business) en de hoeders van de privacybelangen (zoals bijvoorbeeld Bits of Freedom het College Bescherming Persoonsgegevens).

Rob van de Velde
Directeur Geonovum

Amersfoort
Februari 2015

Inhoud

Managementsamenvatting

Dataficatie en locatie-informatie: een wereld die open gaat
Ons spectaculair toegenomen vermogen data te genereren, transporteren, analyseren en weer te distribueren luidt een nieuw tijdperk in. Geo-informatie – en locatie-informatie in het bijzonder – is daarbij het oliemannetje: het stelt ons in staat data uit verschillende bronnen aan elkaar te relateren. Dit schept ongekende mogelijkheden voor overheden, bedrijven en burgers, maar uiteraard creeërt het ook nieuwe uitdagingen. Een daarvan is dat met behulp van (het koppelen met) locatie-informatie een steeds gedetailleerder beeld valt te maken van personen. En dat breekt rechtstreeks in op een goed dat ons veel waard is: het recht op privacy.

Bescherming van persoonsgegevens is een andere wereld
De wereld van de bescherming van de persoonsgegevens is een andere dan die van de dataficatie. Die eerste wordt vooral bewoond door juristen en is gericht op het onder strikte voorwaarden delen van locatie-informatie zodra deze onder het bereik van een van de wettelijke regelingen valt. Deze wettelijke regimes zijn evenwel niet gemakkelijk toe te passen, onder meer doordat de semantiek, die bepalend is voor de toepasselijkheid van de regels, verwarrend is, doordat de normen zeer abstract zijn en, wellicht nog wel het belangrijkste, doordat sommige gemaakte keuzes ingehaald lijken te zijn door de ontwikkelingen in de technologie.

De praktijk: voorzichtig proberen en experimenteren
Niettemin, op diverse plaatsen binnen de overheid – en ook daarbuiten uiteraard – wordt druk geëxperimenteerd met locatie-informatie. Dat men daarbij de regels rond bescherming van persoonsgegevens in acht moet nemen, is goed bekend. Evenwel is de concrete toepassing van de regels op het voorgenomen gebruik van de locatie-informatie voor velen een black box: men snapt de regels niet en vindt ze veel te abstract.

Zekerheden zijn moeilijk te vinden
De zoektocht naar meer zekerheid gaat niet over rozen: intern schiet de inhoudelijke kennis vaak tekort en bovendien is men dikwijls huiverig er (van meet af aan) een jurist bij te betrekken. Ook extern advies levert lang niet altijd de antwoorden op waar men naar op zoek is. Pogingen 'bij de officiële instanties' uitsluitsel te krijgen – zoals het College Bescherming Persoonsgegevens en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties – zijn meestal niet erg succesvol. Daarbij komt nog dat er weinig vertrouwen is in een open dialoog. Veel meer lijkt de relatie beheerst te worden door angst en wantrouwen. Deze dragen niet bij aan het realiseren van de beoogde doelen.

Spanningen vertalen zich in onderbenutting van mogelijkheden
Aldus roept de tegenstelling tussen de ongekende mogelijkheden die locatie-informatie biedt en het bestaande regelgevingskader spanningen op. Deze spanningen zitten op verschillende niveaus (inhoud en begrip van regelgeving, verschillen in perspectief, gebrek aan communicatie en regie) en leiden tot suboptimalisatie en kunstgrepen om gestelde doelen toch te realiseren: ook de geo-informatie community en hun afnemers hebben hier last van. Daarbij komt dat het in de huidige constellatie lijkt te ontbreken aan ventielen en informele probleemoplossers: processen en verantwoordelijkheden zijn geïnstitutionaliseerd en voeling met 'wat er leeft' vertaalt zich niet discussies over (laat staan verandering van) regels en toepassing ervan.

Oplossingen: combinatie van doen en praten op verschillende niveaus
De oplossingen zijn gelegen in het bijeenbrengen van de twee werelden door het scheppen van een dialoog, die leidt tot erkenning van wederzijdse belangen met het besef dat de voortzetting van de huidige praktijk op termijn geen (te verkiezen) optie is. Om de dialoog te laten werken moet een onderscheid gemaakt worden tussen de uitvoering – die dringend verlegen zit om concrete oplossingen – en het meer principiële, strategische, ja bijna ethische niveau, die op nationaal niveau en in Brussel gevoerd moet worden.

Management summary

Why and What?
This White Paper was prepared by Geonovum, a publicly funded organisation specialised in standardisation for the interoperability of geo-information. Its goal is to kick-start a fact-based dialogue between the agencies which are responsible for the proper production, management and use of spatial data within the public sector, and those responsible for, and involved in, the protection of personal data, including those engaged in enforcement. To that end, it describes the technological developments that have taken place over recent years and the profound role that location data has had in these developments; it also details the current legal framework applicable to the use of such data. Building on a large number of interviews and case studies which were conducted with local government agencies, companies, regulators, civil rights societies and various ministries, it describes the difficult situation that many organisations find themselves in as they grapple with the rules and, at the same time, try to use the new technological options available which rely on location data. The Paper concludes by proposing a number of ways forward on different playing fields.

The big movement: datafication, the steam engine of the 21st century
We are entering an era of datafication which enables us, for the first time, to generate, store, analyse and distribute huge amounts of data at the blink of an eye and at minimal cost. The technologies underpinning this development, however, are highly disruptive and the traditional roles and responsibilities of governments, companies and private citizens are being shaken up in such a way they can never return to the form they have taken over the last century. Barriers to markets are also disintegrating rapidly, the winds of rapid change are rushing through almost every sector, consumer surplus is exploding, unexpected correlations are surfacing,

every citizen has a voice reaching out to millions and governments' abilities to perform their tasks more effectively and efficiently are increasing day by day.

Role of location information: the 'grand glue'
This term is particularly applicable to the world of geo-information, being the basis for pointing at, tagging, organizing, enforcing and sanctioning events and behaviour. The enormous dispersal of sensors and their linkage to digital networks in combination with the associated massive storage, transmission and processing capabilities, convert location data – a place on earth, featuring an x and y (or even a z) coordinate – into the point of connection for data which comes from almost any source, (as 60-80% of all data sets hold such location data). Put differently, because of their 'grand glue characteristics', location data have changed from being a 'spot in the Time Atlas' into a data culmination point, including data which, when connected, increasingly allow for the identification of persons.

Protection of personal data: another world
Using this unprecedented linking potential, detailed pictures of real persons can be established quite easily and producers and users of geo-information are dragged into a new arena: the arena of data protection, an arena populated by a different species than those living in the geo-spatial world. Members of the data protection species are predominantly lawyers whose mission in life appears to be to limit the use of (location) data the moment these turn into personal data. Unfortunately, the abstract nature of the language used by these laws (and the lawyers) makes it quite difficult for people who are not species members to grasp. Furthermore, some argue that the choices made some 20 years ago when the laws were drawn up are no longer valid as technology and indeed life itself has changed so dramatically since then.

In practise: cautiously trying and experimenting
Nevertheless, attracted by the potential which is offered by new technologies, both public and private sector are experimenting with the use of location data to better perform their tasks and pursue their ambitions. Attempting to cope with the lack of clarity and the uncertainties, they proceed gingerly. As the case studies show, some organisations have tried knocking on official doors (like the Dutch data protection office), but with no luck. Others have tried to keep the lawyers out until the very last moment, not letting them 'spoil the show'. Overall, there appears to be a fundamental lack of mutual trust between both worlds which inhibits any development of a dialogue.

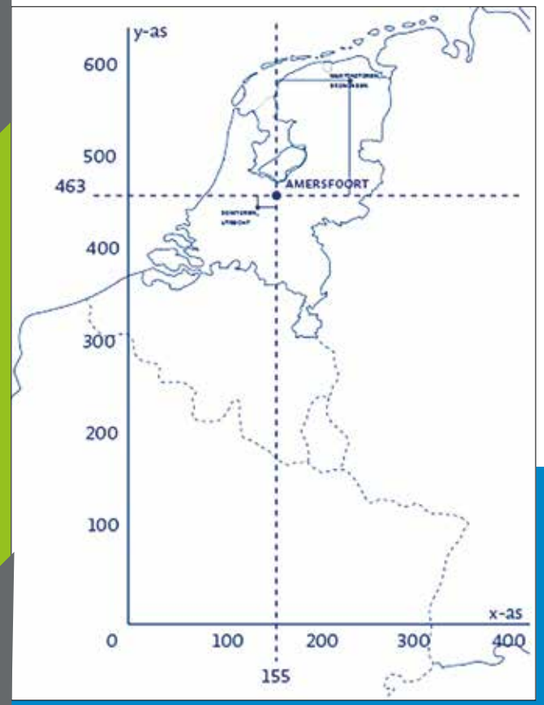
The outcome: tension and under usage of the potential
Clearly this creates tensions: location information requires the free flow of data where the large scale use creates and boosts its value. But the goal of those who would protect the use of personal data is to constrain and restrict this flow. When performing their (public) tasks, organisations are increasingly confronted with these tensions, as the technological developments allow for solutions which are on, or have even crossed over, the borderline of what is allowed. As a result, artificial and suboptimal solutions are sought, leading to the underuse of the location data's full potential, and to the geo community and its users not reaping the benefits at hand.

Current status: no quick fixes
These tensions surface not only in relation to the legal framework, but also in the different perspectives on governance and the ways of problem solving: geo-information communities tend to rely on bottom up consensual models (for instance in the process of setting standards), whereas privacy lawyers appear to put more trust in top down regulatory mechanisms. In addition, informal structures and processes to release pressure are not in place, but have been institutionalised in the form of regulators and official procedures separating them from those whose interests they are serving. Moreover, the mandate to regulate this matter at a fundamental level lies with Brussels.

Solutions: a combination of talking and acting
To stop these worlds continuing to grow apart, dialogues must first be constructed to connect them. We need to build on the growing mutual appreciation of the interests served and the understanding that the practice we have now is not an option for the future. To make these dialogues work, distinctions need to be made between the fundamental questions on the table – do the paradigms still work or do we need to rebalance and relocate interests? And what short term solutions do we need in practice now, today? This requires an open atmosphere where members of both worlds are willing to experiment, look beyond their own professional concerns and take a leap of faith.

Dataficatie en locatiegegevens – goede bedgenoten

Gedreven door ongekende informatietechnologische ontwikkelingen en de alom aanwezigheid van snelle infrastructuur en sensoren, is de wereld in rap tempo aan het 'dataficeren': patronen en ontwikkelingen worden zichtbaar die dat voorheen niet waren. Geografische informatie, locatie-informatie in het bijzonder, speelt daarin een cruciale rol als koppelaar.



Bron: www.kadaster.nl/web/Themas/Registraties/Rijksdriehoeksmeting/Rijksdriehoeksstelsel.htm

DE WERELD VAN DE GEO-INFORMATIE

Terminologie en basisprincipes

Geografische informatie, kortweg geo-informatie, is informatie over objecten of fenomenen die direct of indirect geassocieerd zijn met een locatie gerelateerd aan de aarde. Het verbindt dus een plek op aarde (een locatie) en kenmerken (attributen) van die plek met elkaar. Deze attributen komen in twee soorten: reële (wegen, woningen, leidingen) en virtuele attributen (landsgrenzen, bestuurlijke gebiedsindeling, eigendomsverhoudingen, bestemmingen etc.).[1] Een locatie kan worden vastgelegd in coördinaten. In Nederland wordt daarbij vaak gebruik gemaakt van het stelsel van de Rijksdriehoeksmeting (box 1).[2]

1 Loenen, B. van, Jong, J. de, e.a., *Recht en Locatie. Geo-informatie, wat is het en wat is de juridische context?*, Reeds Business, Den Haag, 2008, p. 12.

2 www.kadaster.nl/web/Themas/Registraties/Rijksdriehoeksmeting/Rijksdriehoeksstelsel.

Box 1 - Stelsel van Rijksdriehoeksmeting

Het stelsel van de Rijksdriehoeksmeting, bestaande uit ongeveer 5.600 coördinaatpunten (RD-punten), is het coördinatensysteem dat in Nederland gebruikt wordt voor het duiden van bijna alle geo-informatie. De coördinaatpunten bestaan uit een X- en een Y-coördinaat. X en Y geven de afstand aan tot twee loodrecht op elkaar staande assen.

Combineren we geo-informatie met thematische informatie in een ondersteunend gedigitaliseerd informatiesysteem, dan spreken we van een geografisch informatie systeem, kortweg GIS. Typische output van GIS is: de aanwezigheid van voetbalvelden in een gemeente, het aantal inbraken in een wijk, de soorten bomen langs een rijksweg, de ontwikkeling van de WOZ-opbrengsten in de afgelopen 10 jaar in een straat, de snelste route van A naar B, zonder gebruik van veerponten en de geluidseffecten bij aanleg van een spoorweg.

Basis geo-informatie gratis en alom beschikbaar

Productie en beheer van geo-informatie werd van oudsher vooral gezien als een overheidstaak, onder meer in het kader van defensie, landschapsbeheer en ruimtelijke ordening. Organisaties als het Ministerie van Infrastructuur en Milieu (beleid), het Kadaster (beheer), maar ook provincies en gemeentes (bronhouders) spelen hierbinnen een belangrijke rol. Nieuwe technologieën maken het echter mogelijk dat ook niet-publieke partijen in dit *metier* stappen. Denk aan bedrijven als Google, Cyclomedia, NavTeq – maar ook aan burgers die door middel van *crowdsourcing* – zoals Open Street Map – grootscheeps en systematisch inwinnen. Deze 'concurrentie' heeft er onder meer toe geleid dat in toenemende mate de basislagen geo-informatie – denk hierbij aan de basisregistratie topografie, het actueel hoogtebestand, maar ook Google Maps en Open Street Map – gratis en voor niets als Open Data beschikbaar komt voor gebruik door eenieder.

DATAFICATIE VAN ONZE SAMENLEVING

Dataficatie

Uiteraard vinden deze ontwikkelingen niet slechts in het geo-domein plaats. Sterker nog, velen menen dat we aan de vooravond staan van een nieuwe eeuw, die van de 'dataficatie'.[3] Dataficatie is het verschijnsel

3 Zie voor een 303-pagina's lange uitleg hierover: Mayer-Schonberger Viktor & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think,* Houghton Mifflin Harcourt, 2012.

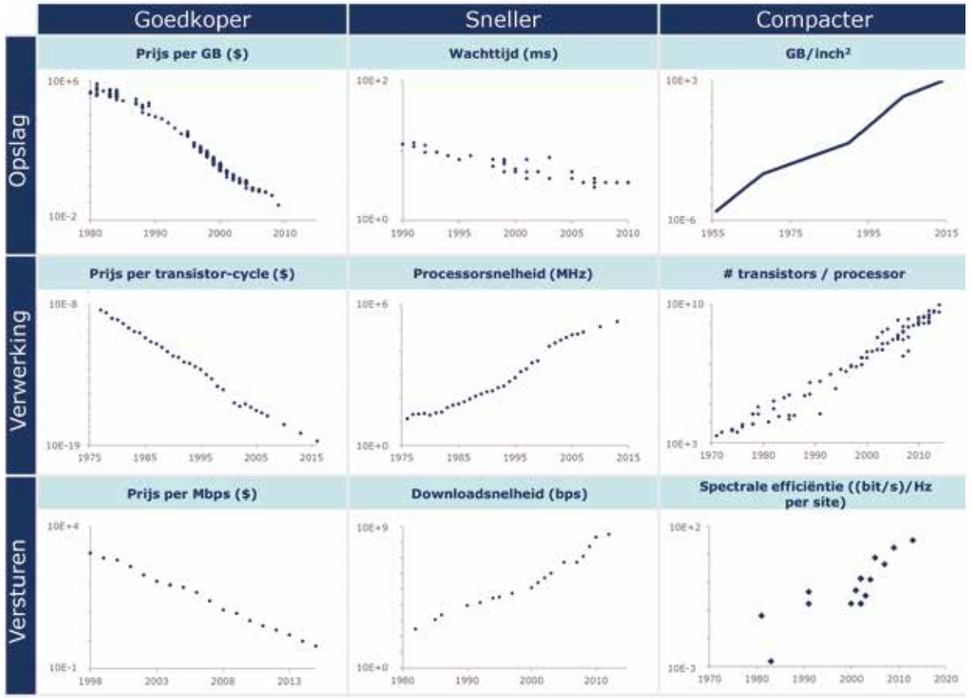
Box 2 –Duizelingwekkende cijfers

De hoeveelheid data die we thans naar schatting in twee dagen genereren – circa 5 quintillion bytes – is gelijk aan de opgetelde hoeveelheid data die de mensheid tot aan het jaar 2003 had geproduceerd. 90% van alle data is niet ouder dan twee jaar (IBM, *Bringing Big Data to the Enterprise,* augustus 2014).

De wereldmarktwaarde voor sensortechnologie – grotendeels verantwoordelijk voor de enorme stijging van inwincapaciteit van data – zal zich zal ontwikkelen van $56.3 miljard in 2010 tot $91.5 miljard in 2016 en zelfs $154 miljard in 2020 (Srinivasa Rajaram, *Global Markets and Technologies for Sensors,* BCC Research, juli 2014).

Bestedingen van eindgebruikers van cloud-technologie – de oplossing voor grootschalige opslag en decentrale toegankelijkheid – zullen naar verwachting in 2015 $180 miljard belopen en die voor cloud-hardware $79 miljard in 2018 (TJ McCue, *Cloud Computing: United States Businesses Will Spend $13 Billion On It, Forbes,* januari 2014).

Ook de markt voor de verwerking en analyse vertoont een gelijksoortig verloop: waar deze 5 jaar geleden nog non-existent was, bedraagt deze thans $3 miljard en naar verwachting $20 miljard in 2017 (Mark P. Mills, *The Next Great Growth Cycle, The American,* augustus 2012).



dat we aspecten van ons leven kunnen informatiseren, hetgeen voorheen onmogelijk was. Zo dataficeert Twitter onze fluistergedachtes, Facebook onze vriendschappen en Linkedin onze professionele context. Dit stelt ons in staat patronen te zien op bijna ieder denkbare schaal.

Exponentiële ontwikkelingen in datatechnologie

De impact daarvan is vergelijkbaar met die van de ontdekking van de stoommachine, de elektriciteit en de fossiele brandstoffen. In de kern wordt deze veroorzaakt door drie factoren: de spectaculaire toename van de capaciteit van opslag, distributie en verwerking van digitale data.

Zoals uit deze grafiek blijkt, vertonen de (daling van de) kosten, de snelheid en effectiviteit van deze drie de afgelopen jaar 20 jaar een exponentieel verloop. De verwachting is dat deze beweging zich versterkt zal doorzetten.[4] Zo zien we bijvoorbeeld dat de marktprijs voor 1 gigabyte opslagcapaciteit in 1980 $ 1.000.000 bedroeg. Nu is dat circa $ 0,01 en dus met een factor 100.000.000 afgenomen. Nota bene: de y-assen bevatten een logaritmische schaalverdeling.

Aanwezigheid van smartphones

Naast de spectaculaire toename in capaciteit en snelheid en afname van kosten, is er een nog factor van groot belang: de aanwezigheid van sensoren.[5] Door de enorme groei van *smartphones* en andere randapparatuur, gekoppeld aan alom aanwezigheid van snelle en goedkope digitale netwerken, is het mogelijk longitudinaal data te verzamelen. Dit gebeurt massaal, vaak ongemerkt en zonder dat gebruikers er een probleem van maken. Punt is wel dat weigeren mee te doen eigenlijk geen optie is. Dit impliceert namelijk het niet meer gebruikmaken van tal van essentiële voorzieningen, zoals het internet, mobiele telefoons, het openbaar vervoer, snelwegen, publieke ruimtes etc.

Dekking van massale distributieplatformen

Naast een sensor is de smartphone (en andere soorten randapparatuur) natuurlijk ook nog eens een ideaal distributieplatform: de interface met de eindgebruiker. Naar verwachting zal het niet lang meer duren voordat iedereen er eentje heeft: Ericsson schatte vorig jaar in dat tussen nu en 2019 het aantal smartphone-abonnementen zal verdrievoudigen tot 5,6 miljard stuks.[6] Anders gezegd, zal over 5 jaar zal bijna iedereen op aarde, gekoppeld aan 4G- en LTE-netwerken, continu data kunnen consumeren en genereren.

4 Velde, R. te, Dialogic BV, *De impact van ICT op de Nederlandse economie,* onderzoek in opdracht van het ministerie van Economische Zaken (nog niet gepubliceerd).

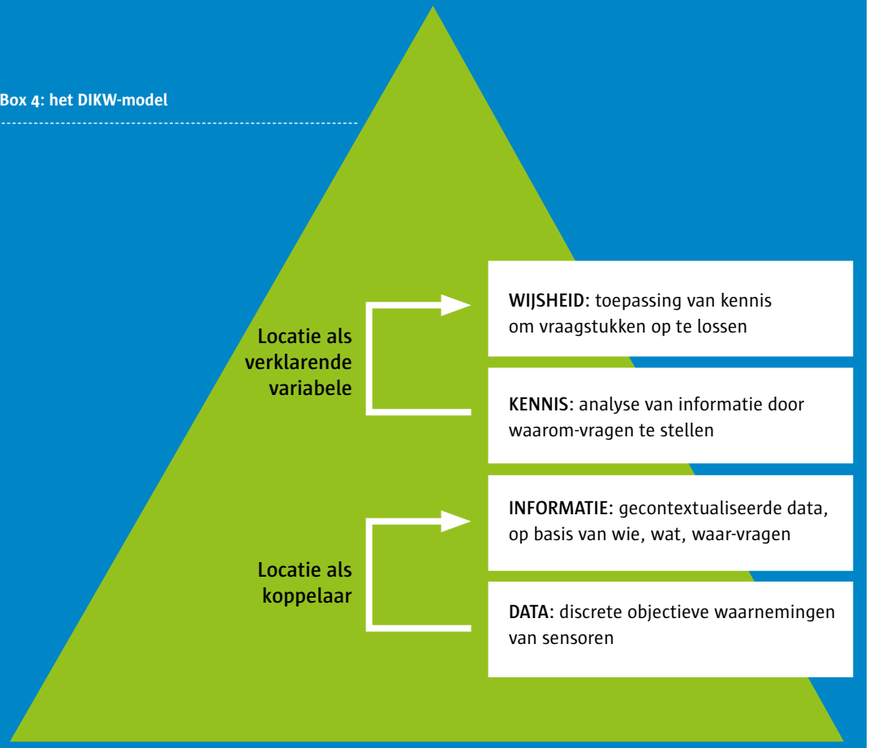
5 Een sensor is in feite een zintuig: het neemt de omgeving waar en verstuurt deze informatie in digitale vorm naar een verzamelpunt. Een sensor kan, mede omdat deze zo klein zijn geworden overal in of aangebracht worden (grond, water, gebouwen, machines, mobiele telefoons, dieren, mensen).

6 *On the pulse of the networked society,* Ericsson Mobility Report, November 2013. [www.ericsson.com/res/docs/2013/ericsson-mobility-report-november-2013.pdf]

Box 3: Wie allemaal weten waar we zijn?

Uit het in 2012 gepubliceerde rapport *'Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern'* blijkt dat er tenminste 13 (!) locatietechnologieën zijn die continu op de hoogte zijn waar wij – dan wel onze randapparatuur – ons bevinden. Zo zijn daar: satellietnavigatie (zoals GPS en Galileo), mobiele telefonie (o.a. via zendmasten), Internet (WLAN, WiFi, IP-adres), Ultra Wide Band, Bluetooth, Radio Frequency Identification, foto en videocamera's (door gezichtsherkenning/ NNgeotagging), Near Field Communication, ZigBee, Dedicated Short Range Communication. Het rapport signaleert een aantal duidelijke baten, maar waarschuwt toch vooral voor de privacyrisico's.

Box 4: het DIKW-model



Het is overigens niet alleen de smartphone die dit mogelijk maakt: een recent Zwitsers onderzoek stelde vast dat er nog 13 andere technologieën zijn die op dit moment grootschalig en continu locatiegegevens registreren (box 3).

Geo-informatie als *het* koppelpunt van digitale gegevens

Om de verbanden tussen al deze verschillende data te zien, moeten deze op een of andere manier gekoppeld worden. Dit koppelen kan op tal van manieren gebeuren (logisch, historisch, semantisch), maar dit heeft inherente tekortkomingen (verschil van interpretatie van zoek- en koppeltermen). De koppeling op basis van geografische coördinaten is daarentegen zeer accuraat: over de duiding bestaan wereldwijd geaccepteerde afspraken en het geografisch *'taggen'* van data impliceert dus dat deze gemakkelijk over elkaar heen gelegd kunnen worden.

Er wordt geschat dat tussen de 60 en 80% van alle data een geo-component (een locatie) in zich heeft. Deze schattingen dateren van (ver) voor de dataficatie.[7] Verwacht mag worden dat dit percentage snel zal toenemen, vooral omdat genoemde sensoren bijna standaard de locatiegegevens verzamelen die bij de waarnemingen horen. Dus doordat data – gestructureerd, maar ook ongestructureerd – zo vaak een digitale geografische component heeft, kan deze gemakkelijk op basis van dat gemeenschappelijke element – de locatie – gekoppeld worden met andere data. Daarvoor is geen aparte administratieve koppelentiteit nodig (zoals een persoon, een bedrijf, een dier, een voertuig). De aanwezigheid van locatie-informatie maakt dus de transitie van data naar informatie mogelijk en dat stelt ons weer in staat om de informatie om te zetten in kennis en wijsheid (zie het Data-Informatie-Kennis-Wijsheid model in box 4).[8]

7 Zie voor een leuke beschrijving van de zoektocht naar de grondslagen van deze percentages: Caitlin Dempsey Morais, *Where is the Phrase '80% of Data is Geographic' From?* in GIS Lounge, 2012. [www.gislounge.com/80-percent-data-is-geographic]

8 en.wikipedia.org/wiki/DIKW_Pyramid?

OM MEE TE NEMEN NAAR HET VOLGENDE HOOFDSTUK

Ons spectaculair toegenomen vermogen data te genereren, transporteren, analyseren en weer te distribueren, luidt een nieuw tijdperk in. Locatie-informatie is daarbij het oliemannetje: het stelt ons in staat data uit verschillende bronnen aan elkaar te relateren. Het schept ongekende mogelijkheden voor overheden bedrijven en burgers, maar uiteraard ook nieuwe uitdagingen. Een daarvan is dat met behulp van (het koppelen met) locatie-informatie een steeds gedetailleerder beeld valt te maken van personen. En dat breekt rechtsreeks in op een goed dat ons veel waard is: het recht op privacy. Dat brengt ons bij die andere wereld, die van de bescherming van de persoonsgegevens en deze ziet er heel anders uit zoals we in het volgende hoofdstuk zullen zien.

De andere wereld van de bescherming van persoonsgegevens

Locatie-informatie, zeker als deze wordt gekoppeld met andere databronnen, kan een persoonsgegeven of zelfs een zogenaamd 'locatiegegeven' zijn[9]. In dat geval gaat er een wereld van regels open bij het verwerken van die locatie-informatie. Hoe ziet de wereld eruit, hoe functioneert die, wie wonen daar, en vooral ook, hoe passen de regels van die wereld op het gebruik van locatie-informatie dat we in die andere wereld van hoofdstuk 1 hebben leren kennen? Dat zijn de vragen die in dit tweede hoofdstuk aan de orde komen.

BESCHRIJVING VAN HET JURIDISCH KADER

Complexe materie

De wereld van de bescherming van persoonsgegevens wordt met name bewoond door juristen. Privacyrecht kenmerkt zich door een hoog abstract karakter en is dan ook een echt specialisme geworden, dat voor de buitenstaander – zelfs het juridische soort daarvan – niet altijd gemakkelijk te doorgronden en toe te passen is. Dit gezegd zijnde, doen we hieronder niettemin een poging het recht rond bescherming van persoonsgegevens inzichtelijk te maken. Om de snelheid erin te houden doen we dat in een zeer gecomprimeerde vorm. Bijlage III bevat meer details.

Verankering bescherming persoonsgegevens

Bescherming van persoonsgegevens behoort tot de zogenaamde 'informationele privacy': het recht te bepalen welke informatie over iemand aan anderen bekend is.[10] Het recht op bescherming van persoonsgegevens ligt vast in de Grondwet[11], het Handvest van de Grondrechten van

9 Zie Bijlage III voor de gehanteerde (en nauw luisterende) semantiek.

10 S. Nouwt, *Privacy voor doe-het-zelvers.* Over zelfregulering en het verwerken van persoonsgegevens via internet, SDU Uitgevers, Den Haag, 2005, p. 19.

11 Artikel 10 lid 2 en 3 Grondwet, Hierin is verankerd dat nadere wetgeving regels stelt 'ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens en inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens'.

de Europese Unie[12] en het Verdrag betreffende de werking van de Europese Unie[13]. De Europese wetgever heeft voorts nadere regels gemaakt met betrekking tot de bescherming van locatie- en persoonsgegevens en wel in de ePrivacy Richtlijn (uit 2002[14], aangepast in 2009[15]) en de algemene Privacy Richtlijn.[16] Deze regels zijn grotendeels geïmplementeerd in de Telecommunicatiewet (Tw)[17] en de Wet bescherming persoonsgegevens (Wbp)[18]. De ePrivacy Richtlijn is een sectorspecifieke richtlijn die voorgaat op de algemene regels van de Privacyrichtlijn. Waar de ePrivacy Richtlijn niet voorziet, is de Privacy Richtlijn van toepassing, bij wijze van vangnet[19].

Privacyrichtlijn (Wbp)

De Privacy Richtlijn beoogt gegevensbeschermingsregels in de Europese Lidstaten te harmoniseren. Het geeft een algemeen kader voor verwerking van persoonsgegevens, dus ongeacht de sector waarin dit plaatsvindt. Het bevat een aantal kernbegrippen die vrij abstract van karakter zijn, zoals 'persoonsgegevens' en 'verwerking'. Dit geldt ook voor de personae dramatis waarop de Richtlijn ziet – de verantwoordelijke, de bewaarder, de betrokkene – waaraan dan weer specifieke verantwoordelijkheden en plichten, respectievelijk rechten verbonden zijn.

Box 5: De achtereenvolgende Wbp-verplichtingen op een rijtje als men persoonsgegevens wil verwerken

- *Verwerking* moet in overeenstemming met de wet en behoorlijk en zorgvuldig (artikel 6);
- *Verzameling* mag alleen voor welbepaalde, uitdrukkelijk omschreven gerechtvaardigde doeleinden (artikel 7);
- *Verwerking* mag alleen als het rust op tenminste 1 van de rechtvaardigingsgronden (artikel 8);
- *Verdere* verwerking mag alleen als het niet onverenigbaar is met oorspronkelijke doel (artikel 9);
- *De gegevens* moeten steeds voldoende kwaliteit hebben (artikel 11) afdoende beveiligd zijn (artikel 12, 13 en 14) en niet langer dan nodig bewaard worden.

12 Artikel 7 van dit Handvest bepaalt dat eenieder recht heeft op bescherming van de hem betreffende persoonsgegevens en geeft hiervoor ook een aantal spelregels, namelijk: (a) eerlijke verwerking, (b) voor bepaalde doeleinden, (c) met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet, (d) met een recht van inzage en rectificatie (e) allemaal onder toezicht van een onafhankelijke autoriteit.

13 Artikel 16 van dit verdrag bepaalt dat eenieder recht heeft op bescherming van de hem betreffende persoonsgegevens en bepaalt voorts dat het stellen van regels over de verwerking van persoonsgegevens en het vrij verkeer daarvan een Brusselse competentie is.

14 Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie.

15 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming.

16 Richtlijn 1995/46/EG van het Europese Parlement en de Raad van betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

17 Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie.

18 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens.

19 Art. 2 aanhef, ePrivacy Richtlijn.

Kernbegrippen Wbp

De Wbp is van toepassing op verwerking van persoonsgegevens door een (vestiging van een) verantwoordelijke in Nederland. Daarmee hebben we direct de kernbegrippen te pakken:

- Persoonsgegevens: gegevens die direct of indirect herleidbaar zijn tot een natuurlijk persoon.[20] Hieronder vallen ook gegevens *'die mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld'*;[21]
- Betrokkene: de natuurlijke persoon op wie persoonsgegevens betrekking hebben[22];
- Verwerken: alle handelingen van creatie tot vernietiging van persoonsgegevens;[23]
- Verantwoordelijke: degene die het doel van en de middelen voor de verwerking vaststelt.[24]

Belangrijkste voorwaarden en verplichtingen van de Wbp

Artikel 6 van de Wbp bevat de essentie van de hele regeling: als er sprake is van verwerking van persoonsgegevens, moet dit behoorlijk en zorgvuldig gebeuren overeenkomstig de regels van de Wbp. Voor een rechtmatige – dat wil zeggen, conform de regels van de Wbp – verwerking, moeten de persoonsgegevens eerst en vooral *verzameld* zijn voor een gerechtvaardigd, duidelijk bepaald en goed omschreven doel (artikel 7). Dat doel vormt steeds het toetsingskader. Ook bij verdere

20 Art. 1 sub a Wbp.

21 TK 25892, nr. 3 , blz. 46.

22 Art. 1 sub f Wbp.

23 Art. 1 sub b Wbp. Zie in dit kader ook Cuijpers C.,e.a., *Bestuursrecht en ICT,* SDU Uitgevers, Den Haag, 2012, p. 62 en SDU Commentaar, Wet Bescherming Persoonsgegevens, SDU Uitgevers, Den Haag, 2013, p. 19.

24 Art. 1 sub d Wbp.

verwerking. Anders gezegd: verdere verwerking mag, mits verenigbaar met het oorspronkelijke doel; ongeacht of dit plaatsvindt binnen of buiten de organisatie van de verantwoordelijke. De Wbp concretiseert niet nader wat nog wel en niet meer verenigbaar is met het oorspronkelijke doel, maar geeft in artikel 9 wel een aantal factoren die bij die afweging meegewogen moeten worden (zoals de aard van de gegevens en de impact van de gevolgen (voor de betrokkene) bij dit volgend gebruik).

Daarnaast moet iedere verwerking gebaseerd zijn op tenminste één van de in artikel 8 Wbp limitatief omschreven verwerkingsgronden, waaronder: een wettelijke taak, toestemming betrokkene en een gerechtvaardigd belang prevalerend boven die van de betrokkene. Daar komt bij, nog steeds op grond van artikel 8, dat de verwerking ook moet voldoen aan de beginselen van proportionaliteit en subsidiariteit: de inbreuk moet in verhouding staan tot het met de verwerking te dienen doel en er moet geen andere, voor de betrokkene minder nadelige weg, bestaan. Verder heeft de verantwoordelijke tal van informatieplichten[25] en moeten de door hem verwerkte gegevens ook aan bepaalde kwaliteitseisen voldoen, afdoende beveiligd zijn en zorgvuldig bewaard worden.[26] Betrokkenen hebben inzage- en correctierechten[27] en een beroep op de rechter is mogelijk bij (vermeende) inbreuk.

CBP

Het College bescherming persoonsgegevens (CBP) is belast met het toezicht op de naleving van de regels in de Wbp.[28] In het kader van de toezichtstaak kan het, ook uit eigen beweging, onderzoek doen naar overtredingen van de Wbp en sancties (bestuursdwang of bestuurlijke boetes) opleggen, waartegen overigens rechtsbescherming bestaat). Bij handhaving legt het CBP de nadruk op ernstige overtredingen die structureel van aard zijn en veel mensen raken. Bij het CBP werkten in 2013 circa 80 fte's en had het een budget van in totaal € 7.586.000,-.[29]

25 Zie artikelen 33 en 34 Wbp.
26 Zie onder andere artikelen 13 en 14 Wbp.
27 Zie artikelen 33 tot en met 42 Wbp.
28 Artikel 51 lid 1 Wbp.
29 Jaarverslag CBP 2013, p. 66.

Box 6: Waakhonden en aanverwante organisaties

- *Het College bescherming persoonsgegevens (CBP):* is belast met het toezicht op de naleving van de regels Privacy Richtlijn.
- *De functionaris voor de gegevensbescherming (FG):* facultatief in te stellen en ziet toe op naleving van de Wbp
- *De 'Artikel 29 Werkgroep':* Europees samenwerkingsverband van waakhonden rond Privacy Richtlijn, geeft gevraagd en ongevraagd opinies over uitleg Privacy Richtlijn.
- *Autoriteit Commerciële Markt (ACM):* houdt toezicht op naleving regels ePrivacy Richtlijn.

FG en Artikel 29 Werkgroep

In het krachtenveld rond de Wbp zijn nog twee andere instituties van belang: de functionaris voor de gegevensbescherming en de Artikel 29 Werkgroep. Organisaties kunnen ervoor kiezen binnen hun eigen muren een toezichthouder in te stellen, een zogenaamde functionaris voor de gegevensbescherming, kortweg 'een FG'.[30] Deze FG heeft op grond van de Wbp een onafhankelijke positie en als taak ervoor te zorgen dat de Wbp netjes wordt nageleefd. Circa 400 organisaties in Nederland hebben inmiddels een FG.[31] Verder voorziet Artikel 29 van de Privacy Richtlijn in de oprichting van een onafhankelijk advies -en overlegorgaan van Europese privacytoezichthouders, die men dan ook de 'Artikel 29 Werkgroep' heeft genoemd. Hierin zitten alle Lidstaatwaakhonden zoals het CBP. Strevend naar een uniforme toepassing van de principes uit de Privacy Richtlijn kan zij, gevraagd en ongevraagd, hierover uitleg geven. Dit doet zij veelvuldig in de vorm van werkdocumenten en opinies. Daarnaast coördineert zij de gezamenlijke handhaving van de nationale toezichthouders.[32]

ePrivacy Richtlijn (Tw)

De ePrivacy Richtlijn richt zich specifiek op gegevensverwerking in de telecommunicatiesector, waaronder de verwerking van zogenaamde 'locatiegegevens'.[33] Deze Richtlijn is dus slechts van toepassing op aanbieders van elektronische-communicatiediensten, waaronder mobiele randapparatuur, die communiceren via openbare netwerken. Het legt hen specifieke verantwoordelijkheden en verplichtingen op (onder meer ter zake van opslag, beveiliging, vertrouwelijkheidsgaranties, spamming en het gebruik van cookies).[34]

De ePrivacy Richtlijn definieert locatiegegevens als gegevens *'die worden verwerkt in een elektronische-communicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker van een*

30 Artikelen 62 tot en met 64 Wbp.
31 www.ngfg.nl.
32 Op de website van het CBP is meer te vinden over deze Artikel 29 Werkgroep.
33 Artikel 1 sub b en c jo. artikelen 6 en 9 ePrivacy Richtlijn.
34 Zie o.a. artikel 4 ePrivacy Richtlijn.

algemeen beschikbaar elektronische-communicatiedienst wordt aangegeven'.[35] Deze locatiegegevens mogen volgens artikel 9 van de ePrivacy Richtlijn slechts worden verwerkt als (a) deze anoniem zijn gemaakt of (b) als deze verwerking nodig is voor de levering van een dienst met toegevoegde waarde[36] en gebruikers hiervoor ook hun expliciete toestemming hebben gegeven. Voorts moet de verwerking noodzakelijk zijn voor het te bereiken doel en dient de verwerking onder bevoegd gezag plaats te vinden.[37] Daarnaast rusten er nog tal van informatieverplichtingen op de dienstaanbieder.

ACM

Toezicht op deze regels is neergelegd bij de Autoriteit Commerciële Markt (ACM). Bij overtreding van de regels kan de ACM een dwangsom opleggen. In 2005 hebben de OPTA, de voorloper van de ACM, en het CBP een samenwerkingsprotocol opgesteld waarin afspraken zijn gemaakt over mogelijke samenloop van bevoegdheden. De ACM bestond in 2013 uit ongeveer 500 fte's en het budget voor 2013 was €771.000.[38] Daarbij moet wel opgemerkt worden dat de ACM veel meer taken heeft dan toezicht op de naleving van de regels van de ePrivacy Richtlijn.

LOCATIE-INFORMATIE: EEN LOCATIEGEGEVEN OF PERSOONSGEGEVEN OF…?

Hoe nu deze regels toe te passen op het gebruik van locatie-informatie? Dit is van groot belang want als deze regelingen van toepassing zijn, gelden plots allerlei voorwaarden en verplichtingen rond het gebruik van deze gegevens. Voor de beantwoording van deze vraag moeten we

35 Artikel 2 sub c ePrivacy Richtlijn. We laten de situatie dat een locatiegegeven een 'verkeersgegeven' (artikel 2 sub b) kan zijn verder buiten beschouwing.

36 Zoals adviezen over de voordeligste tariefpakketten, routegeleiding, verkeersinformatie, weerberichten en toeristische informatie. Zie overweging 18 bij richtlijn 2002/58.

37 Onder het gezag de aanbieder van het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst, of de derde die de dienst met de toegevoegde waarde levert.

38 Jaarverslag ACM 2013, p. 21.

een allereerst een onderscheid maken tussen 'locatiegegevens' in de strikte zin van de ePrivacy Richtlijn en andere locatiegegevens.

Locatiegegevens vallend onder de ePrivacy Richtlijn

Artikel 3 lid 1 van de ePrivacy Richtlijn luidt: *'Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische-communicatiediensten over openbare communicatienetwerken in de Gemeenschap'*. In de praktijk is dit inmiddels een lastig criterium: het zijn niet slechts openbare elektronische-communicatiediensten over openbare communicatienetwerken die locatiegegevens genereren en verwerken. Anderen, waaronder overheden en private partijen, doen dit ook massaal. Daarmee is dus ook het onderscheid tussen private en publieke diensten niet langer gerechtvaardigd. De verwarring die hierdoor ontstaat over de toepasselijkheid van ePrivacy regels moge blijken uit het onderstaande schema waarin bovengenoemde criteria op enkele bekende (plaatsbepalings) technologieën zijn gelegd.[39]

Bereikbepaler ePrivacy Richtlijn	**GPS**	**Sensoren**	**RFID, WIFI, Blue-tooth**	**Op cellen gebaseerde mobiele netwerken**	**Op pin gebaseerde betalingen**
Elektronisch communicatie netwerk?	Ja	Waarschijnlijk niet	Ja	Ja	Waarschijnlijk niet
Elektronische-communicatiediensten?	Ja	Waarschijnlijk niet	Ja	Ja	Waarschijnlijk niet
Publiek?	Ja, maar technische beperking mogelijk	Onduidelijk	Mogelijk	Ja, maar technische beperking mogelijk	Ja
ePrivacy Richtlijn van toepassing?	Ja, waarschijnlijk	Waarschijnlijk niet	Ja, indien publiek	Ja	Waarschijnlijk niet

Bron: Presentatie C.M.K.C. Cuijpers, EMJD 2014, Eprivacy: fragmentation and law versus practice

39 Cuijpers, C.M.K.C. & Koops, E.J. (2008). *How fragmentation in European law undermines consumer protection: The case of Location Based Services*. European Law Review, 33(6), 880-897.

Techniekafhankelijke keuzes die destijds zijn gemaakt, zijn ingehaald door de technologische ontwikkelingen: de gebruikte technologie bepaalt of het beschermingsregime ingeroepen kan worden. Dat klemt te meer nu het mensen niet zal uitmaken hoe dat gebeurt, maar wel dát het gebeurt.[40]

Locatie-informatie niet vallend onder ePrivacy Richtlijn

Ook als we er zeker van zijn dat de locatie-informatie geen locatiegegeven is in de zin van de ePrivacy Richtlijn, zijn we er nog niet. Immers, dan moet nagegaan worden of de locatie-informatie een persoonsgegeven is in de zin van de Privacy Richtlijn. Ook dat is geen eenvoudige opgave zoals we hieronder zullen zien.

De Wbp

Persoonsgegevens zijn gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Goed beschouwd is locatie-informatie in zijn meeste pure vorm – een x,y coördinaat op een kaart – geen persoonsgegeven: een x,y coördinaat verwijst immers enkel naar een plek op aarde en kan zonder nadere gegevens onmogelijk worden gekoppeld aan een persoon. Echter, zodra locatie-informatie (bijvoorbeeld in een GIS) koppelbaar is aan andere gegevens, is het mogelijk dat er *identificeerbaarheid* van personen ontstaat.

Daarbij speelt allereerst een rol of de locatie-informatie mede bepalend is voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld. Is dat geval, dan is er sprake van een persoonsgegeven.[41] Het is daarbij niet noodzakelijk dat het bij het potentiële resultaat om grote gevolgen gaat. Het is voldoende als de persoon als gevolg van de verwerking van de betrokken gegevens anders wordt behandeld dan anderen.[42]

Van belang is verder of de identiteit van een persoon met de informatie redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld. Hierbij moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren.[43, 44] Het is niet doorslaggevend of de persoon daadwerkelijk door de gegevens is geïdentificeerd.[45] Het is dus van belang of de locatie-informatie met beschikbare middelen op relatief eenvoudige wijze met andere gegevens gecombineerd kan worden. Is dat het geval, dan ontstaat door deze combinatie de identificeerbaarheid. Dat wordt steeds makkelijker zoals uit box 8 blijkt.[46]

Ook de opmerkingen van de wetgever bij de invoering van de Basisregistraties Adressen en Gebouwen (BAG) zijn daarvan een illustratie.[47] In de memorie van toelichting bij de Wet BAG valt te lezen dat de gegevens in

Box 7: De praktijk van Geo-informatie en privacy

Waar de privacywaakhonden geoinformatie als persoonsgegevens beschouwen, zien de bronhouders dit vaak anders. In Engeland verkoopt de Land Registry het Price Paid Data product (PPI), dat gegevens bundelt over het adres van het vastgoed, de verkoopprijs, de datum van de eigendomsoverdracht, het type, de status van het vastgoed (nieuwbouw of niet) en of het eigendom of erfpacht betreft. Ook na overleg met de Information Commission Officer concludeerde de Land Registry dat het PPI geen persoonsgegevens bevat (Land Registry 2012 & 2013).

Hetzelfde verschil tussen de theorie van de privacywaakhonden en de praktijk geldt voor de Basisregistratie adressen en gebouwen en veel andere geo-informatie die als open data beschikbaar wordt gesteld. De vele miljoenen keren dat de geogegevens in PDOK (Publieke dienstverlening op de kaart www.pdok.nl) worden geraadpleegd zijn daar een sprekend voorbeeld van.

Box 8 – indirecte identificatie *a piece of cake*?

Informatie op 6 positie postcode niveau (gemiddeld ongeveer 20 woningen) is gemakkelijk te herleiden tot individuen door deze informatie te combineren met informatie over het geslacht en de geboortedatum. Dit blijkt uit het promotie-onderzoek van Matthijs Koot (2012). Het lukte hem 99% van de 2,8 miljoen van de mensen in de database die hij tot zijn beschikking had uniek te identificeren. Op 4 positie postcode niveau (een heel dorp of wijk) lukte het hem om 67% van de mensen in de database te identificeren door deze informatie te combineren met alleen hun geboortedatum.

40 Artikel 15 van de ePrivacy Richtlijn draagt verder bij aan de verwarring. Dat artikel bepaalt dat Lidstaten op een aantal punten – waaronder artikel 9 waarin de omgang met locatiegegevens is geregeld – eigen afwijkende regels mogen maken indien dat 'in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische-communicatiesysteem'. Dit zet uiteraard de deur open naar divergerende regels op nationaal niveau.

41 De memorie van Toelichting bij de Wbp noemt hier als voorbeeld de eigendom- en waardegegevens over onroerend goed, zoals geregistreerd in het Kadaster (TK 25892 MvT, nr. 9, p. 1).

42 Artikel 29 Werkgroep, 2007.

43 Overweging 26, Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Zie ook art 4. van 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)'

44 Overweging 26, Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

45 College Bescherming Persoonsgegevens 2007, p. 10.

46 In een ver verleden (1996) heeft de Registratiekamer (de rechtsvoorganger van het CBP) in een advies verklaard dat geaggregeerde gegevens op het niveau van de 6-positiepostcode (dus letter, letter, letter, letter, zonder huisnummer) geen persoonsgegevens bevatten. (Loenen, B. van, Jong, J. de, e.a., *Recht en Locatie. Geo-informatie, wat is het en wat is de juridische context?*, Reeds Business, Den Haag, 2008, p. 29. Zie ook Kamerstuk 25892, nummer 3.

47 H.D. Ploeger, B. van Loenen, 2013, De mogelijkheid van een open data beleid voor het Actueel Hoogtebestand Nederland nader onderzocht.

de basisregistraties adressen en gebouwen in beginsel geen persoonsgegevens zijn in de zin van de Wbp omdat ze niet zijn te herleiden tot identificeerbare personen. Wel kan de identiteit van een persoon te herleiden zijn door koppeling met andere gegevens en daarmee moet de verstrekker van BAG-gegevens rekening houden. Als de verstrekker van BAG-gegevens ervan uit mag gaan dat de afnemer de gegevens in combinatie met andere gegevens kan herleiden tot een natuurlijke persoon, dan moeten de gegevens als persoonsgegevens worden aangemerkt.[48] Voor aanbieders van (geografische) gegevens betekent dit dat niet alleen de aangeboden data betrokken moet worden in de vraag of de gegevens identificerend zijn, maar ook andere beschikbare gegevens.[49]

Standpunt Artikel 29 Werkgroep en het CBP

Of een locatie-gegeven een persoonsgegeven is, blijft lastig te duiden door de abstracte normen die de Wbp hanteert. Wel heeft de Artikel 29 Werkgroep in 2007 in een opinie uitgelegd dat volgens haar locatie-informatie – in dit geval het monitoren van de locaties van taxi's – als persoonsgegevens moeten worden aangemerkt, omdat deze gegevens herleidbaar zijn tot een geïdentificeerd of identificeerbaar natuurlijk persoon.[50]

In 2011 kwam het CBP tot de dezelfde conclusies ter zake van door Google verzamelde MAC-adressen van wifi-routers in combinatie met de daarvan berekende locaties. Dit zijn volgens het CBP persoonsgegevens, omdat de unieke aan de hardware gekoppelde nummers in combinatie met de locatiegegevens van die hardware, tot een individuele persoon te herleiden gegevens zijn.[51]

Box 9: Privacywaakhond: Geo-gegevens zijn persoonsgegevens

Volgens de Belgische privacywaakhond zijn op internet gepubliceerde luchtfoto's van percelen van natuurlijke personen op een schaal 1:50.000 (en gedetailleerder) persoonsgegevens omdat de perceeleigenaars kunnen worden geïdentificeerd via het kadaster. (Bron: De Commissie voor de bescherming van de persoonlijke levenssfeer (2006a&b))

De Artikel 29 Werkgroep kwam tot een zelfde conclusie waar het de waarde van een woning aangaat: ' (...) in bepaalde omstandigheden kan deze informatie als persoonsgegeven worden beschouwd. Het huis behoort tot het vermogen van de eigenaar, en dit gegeven wordt dan ook gebruikt om bijvoorbeeld de omvang van de belastingverplichtingen van de eigenaar te bepalen. In een dergelijke context moet deze informatie ongetwijfeld als persoonsgegeven worden beschouwd.'

Bron: Artikel 29 Werkgroep, 2007 opinie 2007/4

48 Kamerstukken II 2006/07, 30 968, nr. 3, p. 17.

49 H.D. Ploeger, B. van Loenen, 2013, De mogelijkheid van een open data beleid voor het Actueel Hoogtebestand Nederland nader onderzocht.

50 Art.29 Working Party, Advies 4/2007 over het begrip persoonsgegevenWP 136, Juni 2007. Zie in dit kader ook Cuijpers C., Koops B.J., *How fragmentation in European Law undermines consumer protection: the case of Location Based Services,* European Law Review, 2008.

51 Onderzoek CBP naar de verzameling van Wifi-gegevens met Street View auto's door Google z2010-00582, 7 december 2010.

De concept Privacy Verordening

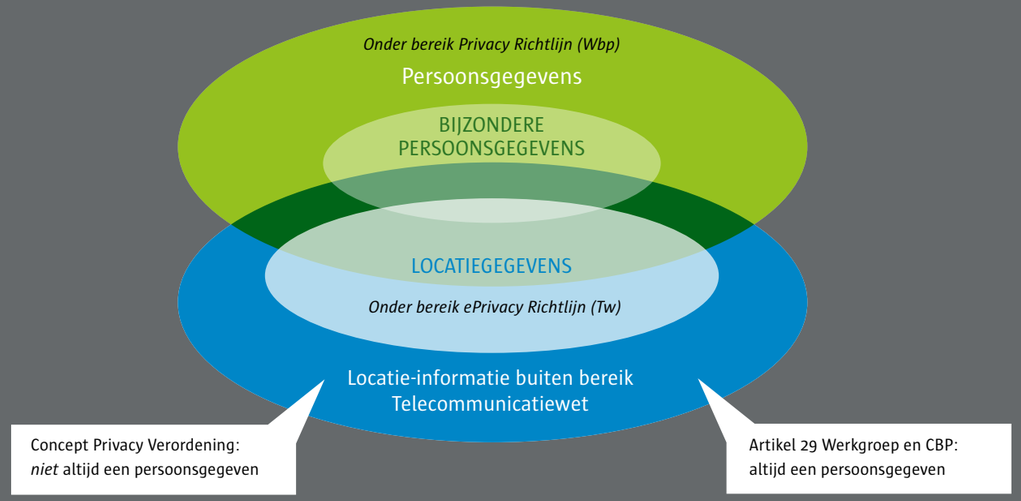
Wie denkt dat de concept Privacy Verordening de mogelijkheid te baat neemt om aan alle twijfels een einde te maken, komt bedrogen uit. De definitie van persoonsgegevens is grotendeels overgenomen uit de gegevensbeschermingsrichtlijn en luidt: 'iedere informatie betreffende een geïdentificeerde natuurlijke persoon of een natuurlijke persoon die direct of indirect, met behulp van middelen waarvan mag worden aangenomen dat zij redelijkerwijs door de voor de verwerking verantwoordelijke dan wel door een andere natuurlijke of rechtspersoon in te zetten zijn, kan worden geïdentificeerd, met name aan de hand van een identificatienummer, gegevens over de verblijfplaats, een online-identificatiemiddel of een of meer specifieke elementen die kenmerkend zijn voor zijn fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit'.

Overweging 24 van de concept Privacy Verordening maakt het allemaal nog ingewikkelder: *'Bij het gebruik van online-diensten kunnen natuurlijke personen worden gekoppeld aan online-identificatiemiddelen via hun apparatuur, applicaties, instrumenten en protocollen, zoals internetprotocol (IP)-adressen en identificatiecookies. Dit kan sporen achterlaten die, in combinatie met unieke identificatoren en andere door de servers ontvangen informatie, kunnen worden gebruikt om profielen op te stellen van personen en personen te herkennen. Identificatienummers, locatiegegevens, online-identificatiemiddelen en andere specifieke factoren hoeven dus niet onder alle omstandigheden als persoonsgegevens te worden beschouwd'.*[52]

Samengevat levert dit een beeld op dat verre van duidelijk is, zoals box 10 duidelijk maakt. Het wettelijk regime is niet alleen gefragmenteerd, maar vooral ook abstract. De toezichthouders hebben niettemin een breed net uitgeworpen: alle locatiegegevens zijn persoonsgegevens.

52 Brussel, 25.1.2012 COM(2012) 11 final 2012/0011 (COD) Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming).

Box 10: semantische problematiek



OM MEE TE NEMEN NAAR HET VOLGENDE HOOFDSTUK

De wereld van de bescherming van de persoonsgegevens is een andere dan die van de dataficatie. Die wereld wordt vooral bewoond door juristen en is gericht op het onder strikte voorwaarden delen van locatie-informatie zodra deze onder het bereik van een van de wettelijke regelingen valt. Deze wettelijke regimes zijn evenwel niet gemakkelijk toe te passen, onder meer doordat sommige gemaakte keuzes ingehaald lijken te zijn door de technologie, doordat de normen nogal abstract zijn en doordat de semantiek, die bepalend is voor de toepasselijkheid van de regels, verwarrend lijkt.

Dit zullen we ook zien in het volgende hoofdstuk waarin we kennismaken met de mensen die graag het potentieel van de dataficatie willen benutten, daarvoor locatie-informatie willen inzetten, en daarbij tegen het een en ander aanlopen!

Gebruik van locatie-informatie en toepassing van de regels in de praktijk

Hiervoor hebben we gezien wat het potentieel en de impact van dataficatie is en welke rol locatie-informatie daarbinnen kan spelen. Tevens hebben we gezien dat er een stelsel aan regels is die de bescherming van de privacy beoogt en daartoe de verwerking aan strikte criteria bindt. Die regels zijn uiterst relevant omdat locatiegegevens hetzij zelf hetzij door hun koppelmogelijkheden al snel onder het bereik van de regimes zullen vallen.
Aan de ene kant hebben we dus het potentieel en aan de andere kant de regels. In dit hoofdstuk kijken we daarom hoe de praktijk hiermee omgaat. Wat de perceptie over de regels is en hoe men deze (al dan niet) toepast, wat de overwegingen daarbij zijn en welke effecten optreden.

ZEVEN CASES

Keuze van de cases en breedte van de interviews
Om voeling te krijgen met die praktijk is een serie interviews gehouden met organisaties die innovatief gebruik maken van locatie-informatie. Binnen de overheid is gesproken met het Centraal Bureau voor de Statistiek en de gemeentes Almere, Amsterdam, Eindhoven en Zwolle en daarbuiten met enkele private gebruikers van locatie-informatie, te weten TomTom en Vodafone. Dit is neergeslagen in zeven 'case beschrijvingen'. Ook is gesproken met de hoeders van de privacybelangen: het CBP en de *civil society* organisatie *Bits of Freedom*.[53]

Gemeente Almere
De gemeente Almere heeft de zogenaamde 'Straatkubus' ontwikkeld, een hulpmiddel om de integrale wijkaanpak te verbeteren en zo de leefbaarheid van Almere te vergroten. De Straatkubus is een *'early-warning'* systeem waarin gegevens uit het fysieke, sociale en veiligheidsdomein op 6-positiepostcodeniveau op de kaart van Almere worden gepresenteerd. Het gaat bijvoorbeeld om gegevens als: cijfers over schuldhulp-

53 Omdat dit geen cases zijn – gebruik van locatie-informatie in de praktijk – zijn deze niet opgenomen in de beschrijvingen. Uiteraard zijn de bevindingen van de interviews wel meegenomen in de analyse.

verlening, huurachterstanden, overlast in openbare ruimten, vroegtijdig schoolverlaten. De Straatkubus koppelt daarbij 'koude' statistieken aan 'warme' waarnemingen (bijvoorbeeld de verhalen van mensen die werken in de wijk, zoals gebiedscoördinatoren).

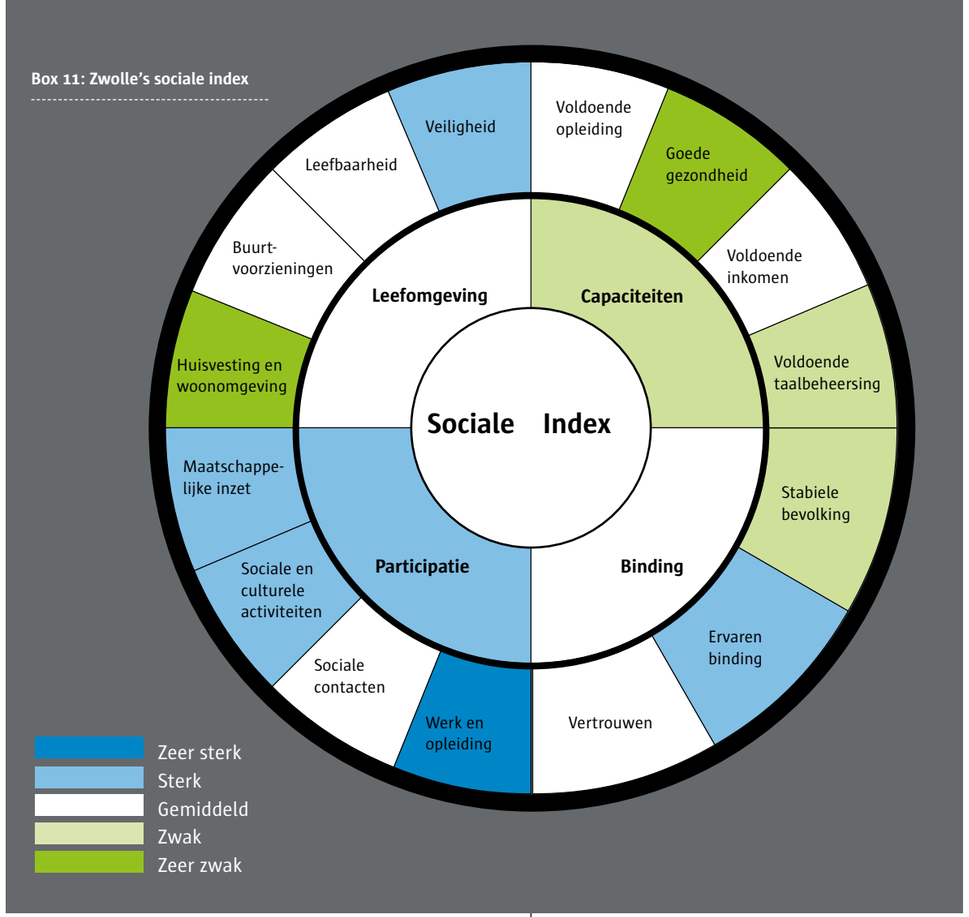
Gemeente Zwolle

De gemeente Zwolle is al een aantal jaren bezig met het systematische en in onderling verband monitoren van tal van data om de leefbaarheid en veiligheid van de verschillende wijken te verbeteren. Zwolle maakt hierbij gebruik van sociale-, fysieke-, economische- en veiligheidsindices die gevoed worden door objectieve gegevens, zoals cijfers over bevolkingssamenstelling, criminaliteit, opleiding, werk, inkomen, stedelijkheidsgraad, hoeveelheid voorzieningen – als ook subjectieve gegevens, zoals woonbeleving, beleving van overlast (bijv. lawaai en stank), gevoel van onveiligheid (zie box 11 ter illustratie, deze is niet gebaseerd op daadwerkelijke cijfers). Al deze gegevens 'stapelt' Zwolle op straatniveau op de kaart zodat er niet alleen een breed en gedetailleerd beeld van de verschillende wijken ontstaat, maar ook verbanden – eveneens door de tijd heen – gezien worden die anders onzichtbaar zouden blijven.

Gemeente Amsterdam

De gemeente Amsterdam is gestart met Gebiedsgericht Werken (kortweg GGW). Het doel van GGW is, aldus Amsterdam, 'van buiten naar binnen werken in vertrouwen samen bouwen aan de stad, met Amsterdammers, ondernemers en andere partners analyseren en ontwikkelen wat nodig is, loslaten wat anderen doen, onvoorziene kansen snel verzilveren en uitvoering geven aan beleid dat aansluit bij de maatschappelijke opgaven, de energie en de doelgroepen van een gebied.' Dit houdt in de praktijk in dat gegevens uit verschillende bronnen (uit de eigen organisatie maar ook daarbuiten) op de kaart van Amsterdam worden geplaatst, waardoor er een gedetailleerd beeld ontstaat van de verschillende wijken. Voorbeelden van die gegevens zijn: cijfers over schuldhulpverlening, schoolverlaters, het woonbestand en meldingen van overlast. Daarbij is een relatief hoog detailniveau van gegevens gewenst, omdat anders de echt belangrijke cijfers weer verdwijnen in de aggregatie.

Box 11: Zwolle's sociale index



Box 12: Stratumseind Living Lab

Gemeente Eindhoven

Het Stratumseind is dé uitgaansstraat van Eindhoven. Om de leefbaarheid, veiligheid en aantrekkelijkheid van het Stratumseind te verbeteren, is de gemeente Eindhoven recent het project 'Stratumseind 2.0' gestart, waarbij het Stratumseind een 'Living Lab' wordt. Kern is dat de locatie het Stratumseind – circa 400 meter lang – een culminatiepunt wordt van tal van metingen waarbij omgevingsfactoren (licht, omgeving, geluid) worden gekruist met big data uit maar liefst 20 verschillende (publieke en private) bronnen, zoals:

- Opgehangen 3D-microfoons meten het geluid van de mensenmassa en of hier stress-signalen te herkennen zijn (geen spraakherkenning);
- Camera's taggen personen als 'objecten' (dus geen gezichtsherkenning of spraakherkenning). Met deze camera's wordt het aantal bezoekers geteld en de dichtheid van de mensenmassa gemeten;
- Geanonimiseerde politiecijfers over incidenten;
- Procentuele verdeling van herkomst (gemeente) van aanwezige en ingeschakelde mobiele telefoons met Vodafone abonnement;
- Aantallen geparkeerde auto's in de rond Stratumseind gevestigde parkeergarages;
- Hoeveelheden opgehaald afval;
- Berichtgeving over Stratumseind in sociale media;
- Het aantal gebruikers van bluetooth en WiFi en hun locaties;
- Informatie van (bier)brouwerijen, waaronder ingekochte hoeveelheden bier;
- Door het samenbrengen en koppelen van al deze verschillende data ontstaat een breed en gedetailleerd beeld van menselijke activiteiten op het Stratumseind en de omstandigheden waaronder dit gebeurt. Aldus hoopt Eindhoven relaties te kunnen leggen tussen deze data en op basis daarvan interventies te doen die leefbaarheid, veiligheid en aantrekkelijkheid van het Stratumseind te verbeteren.

Centraal bureau voor de Statistiek

De taak van het Centraal bureau voor de Statistiek (CBS) is het publiceren van betrouwbare en samenhangende statistische informatie, die inspeelt op de behoeftes van de samenleving. Om deze statistieken te maken en statistisch onderzoek te plegen, verzamelt het CBS diverse gegevens van burgers, bedrijven als de overheid. Praktisch al deze gegevens bevatten een locatiecomponent:

veel onderzoek kent een regionale of ruimtelijk invalshoek. Door het plaatsen van onderzoeksgegevens op de kaart van Nederland, ontstaat er een breed en gedetailleerd beeld van ons land. Ook kunnen kaartjes over elkaar heen worden gelegd, waardoor er een goed beeld ontstaat van de ontwikkelingen door de tijd heen.

Sinds kort experimenteert het CBS ook met externe bronnen, waaronder locatiegegevens van mobiele telefoonklanten van Vodafone. Vodafone anonimiseert en aggregeert deze gegevens zelf voordat deze door Mezuro BV (een van Vodafoneonafhankelijk partij) aan afnemers, zoals het CBS, geleverd worden. Het verschil met de traditionele werkwijze van het CBS is uiteraard enorm: het gaat, in vergelijking met 'oude statistieken', om massale hoeveelheden, extern gegenereerde, dynamische, bijna real time data.[54] Daarbij is de verandering van de betekenis van het begrip 'locatie' cruciaal. De verzameleenheid is niet langer een provincie of een gemeente: het kan een bijna willekeurige lijn of vlak zijn, zolang er maar dekking is. Daarnaast worden locaties koppelbaar in de tijd, doordat gegevens over bewegingen van individualiseerbare randapparatuur deze aan elkaar linken. De koppeling tussen de nieuwe en oude manier van werken, levert geheel nieuwe cijfers en inzichten op en zal naar verwachting van het CBS de manier van statistiek bedrijven fundamenteel veranderen.

Vodafone
Vodafone is internationale marktleider op het gebied van mobiele telefonie. Naast haar kernactiviteiten is Vodafone enkele pilots gestart met big data op het gebied van mobiliteit. Een aantal daarvan voert Vodafone uit in samenwerking met externe partijen. Het gaat daarbij om de overheids- en aan de overheid gelieerde partijen]. Bij deze (pilot) projecten blijven alle bron data binnen het Vodafone domein. Deze data worden volledig geanonimiseerd en geaggregeerd.

54 Bij Vodafone worden er maandelijks circa 4,5 miljard records van 6 miljoen aansluitingen opgeslagen en verwerkt.

Box 13: CBS en Big Data

Voor het maken van mobiliteitsanalyses heeft Vodafone een samenwerkingsverband gesloten met marktpartij Mezuro. Mezuro voert 'blind' bepaalde mobiliteitsanalyses uit op de desbetreffende data en krijgt dus niet zelf de beschikking over de Vodafone data. Het proces is met waarborgen omkleed en wordt periodiek door een gerenommeerd onderzoeksinstituut getoetst. Mezuro verkoopt en verstrekt de resultaten van haar mobiliteitsanalyses aan externe partijen (vanwege bijdrage aan onderzoeken en mogelijke baten voor de maatschappij worden daarvoor soms geen kosten in rekening gebracht). Aanvankelijk was een contractvoorwaarde dat Mezuro alleen zaken mocht doen met de overheid en aan de overheid gelieerde partijen, voor doeleinden die het maatschappelijk nut dienden. Inmiddels werkt Mezuro ook samen met private partijen. Er bestaat in de praktijk zeer veel interesse in deze data.

TomTom
TomTom is leverancier van locatie- en navigatieproducten en -services (zoals filemeldingen, weerberichten, locaties van flitspalen). Om haar dienstverlening te verbeteren, verzamelt Tom Tom, slechts na expliciete toestemming, (locatie)gegevens van haar gebruikers. Het gaat hierbij om enorme hoeveelheden data: zo ontvangt TomTom dagelijks wel 1 miljard snelheidsmetingen en 5 miljard verkeersmetingen van meer dan 65 miljoen klanten wereldwijd.

Eind april 2011 kwamen er berichten in de media dat TomTom locatiegegevens van gebruikers van TomTom apparaten via een verkeersadviesbureau zou verstrekken aan overheden, politie en enkele commerciële partijen. TomTom heeft hierover op eigen initiatief contact opgenomen met het CBP, waarna een ambtshalve onderzoek volgde.

Uitkomst was dat het CBP van mening was dat voor de zogenaamde historische locatiegegevens de toestemmingsaanvraag aan klanten onvoldoende specifiek was en dat die voor de realtime locatiegegevens niet aan de wettelijke vereisten voldeed (de enkele verwijzing naar de on-line privacyverklaring van TomTom volstond niet). TomTom heeft deze vervolgens netjes aangepast (hier was het al mee bezig).

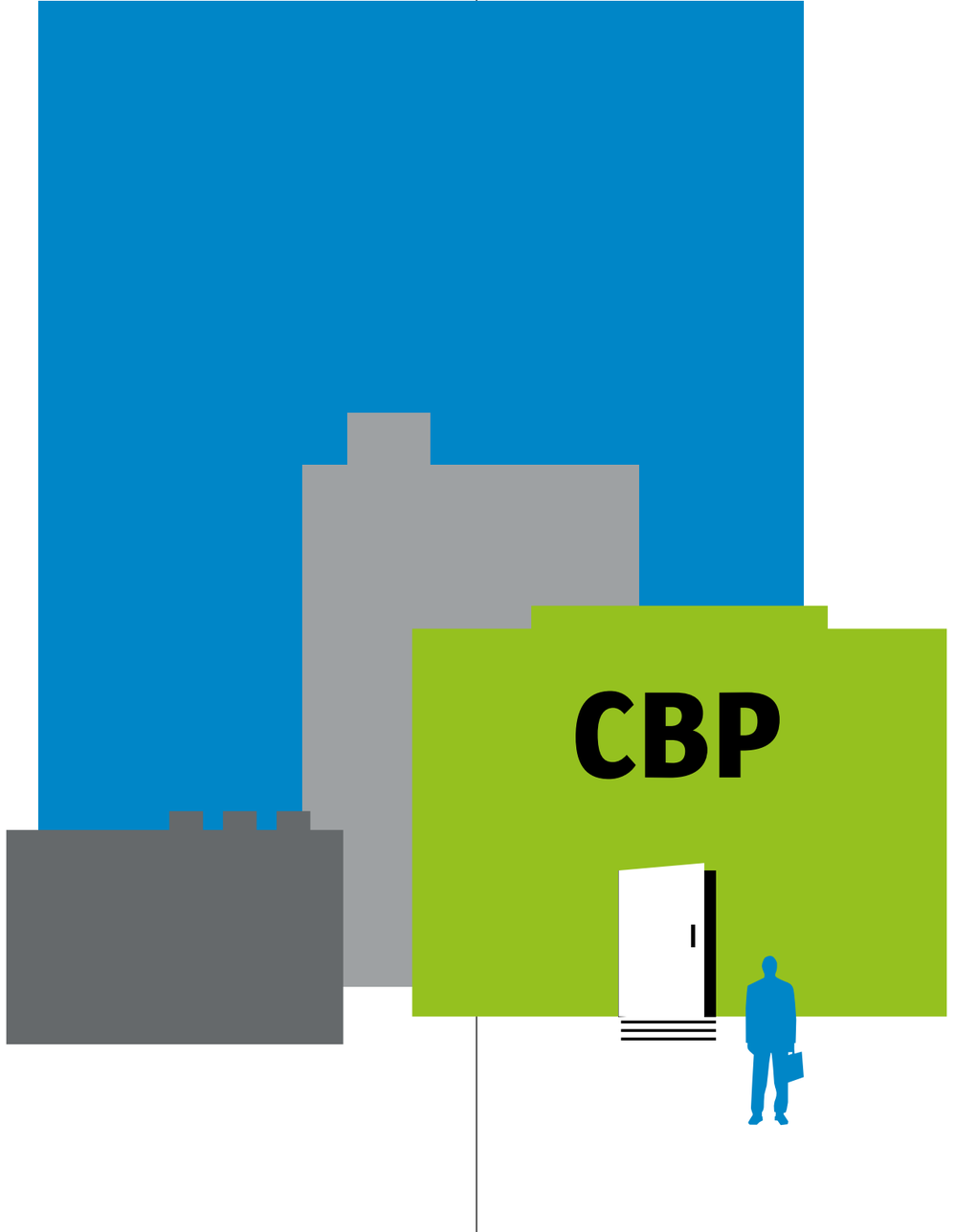
Kortom
Samengevat moge het duidelijk zijn dat er in Nederland, ook in de publieke sector, op dit moment volop gekeken wordt naar en geëxperimenteerd wordt met onconventioneel gebruik van locatie-informatie. Het in acht nemen van de privacyregels levert een hoop kopzorgen op en de omgang met de regels en de daarmee samenhangende onzekerheden vormt een bonte verzameling, zoals we hierna zullen zien.

DE VRAGEN EN ONZEKERHEDEN EN DE OMGANG DAARMEE

Wat zijn de vragen en onzekerheden waarmee de pioniers kampen en hebben gekampt en hoe is men hiermee omgegaan. Om 'de privacy' van de cases te beschermen en om hun experimenten niet te verstoren, is er hier en daar voor gekozen de bevindingen geaggregeerd dan wel anoniem weer te geven.

Bewustheid privacy gerelateerde vragen
Alle cases zijn ontstaan vanuit een concrete behoefte en het gevoel dat met data wellicht aan die behoefte voldaan zou kunnen worden en dus typisch op de plekken waar de interactie met de buitenwereld plaatsvindt (de uitvoering). Daarbij realiseert men zich terdege dat de activiteiten mogelijk onder het bereik van privacybeschermingsregels kunnen vallen, maar of dat het geval is en, zo ja, wat hiervan de implicaties zijn, is onbekend (bij de personen die het initiatief starten). Over het algemeen parkeert men deze zorgen een tijdje – men vreest dat als de juristen binnen komen het gedaan is met de activiteiten – maar op enig moment wint men toch advies in. Bij de 'ervaringsdeskundigen', zoals het CBS, waarbij het omgaan met (persoonsgerelateerde) data *daily business* is, ligt dit anders: daar zijn de routines en protocollen zo dat de juristen van meet af aan betrokken zijn.

Onduidelijkheid van regelgeving
Uit alle gesprekken kwam naar voren dat privacyregels als zeer complex worden ervaren (we zagen al in het vorige hoofdstuk dat dit niet uit de lucht gegrepen is). Men vindt de normen zeer abstract en open: bij



termen als 'behoorlijk', 'zorgvuldig', 'onevenredig', 'gerechtvaardigd', 'toereikend', 'relevant', 'nauwkeurig', 'niet langer dan noodzakelijk' kan men zich vaak geen voorstelling maken. Bovendien bestaat het beeld dat toepassing steeds zeer casuïstisch is en de uitkomsten daarvan onderhevig zijn aan veranderingen in de tijd.

Op zoek naar zekerheid
In alle cases is de juridische afdeling binnen de organisatie het eerste aanspreekpunt geweest. Evenwel wordt dikwijls (vervolgens) ook extern advies ingewonnen. Boeiend genoeg levert deze consultatie (intern en/of extern) meestal geen definitieve antwoorden op over wat mag en niet mag. Uiteraard op grote lijnen wel, maar de cases zijn zeer concreet en uitsluitsel of de verwerking van de gegevens in dat concrete geval mag, kan lang niet altijd verkregen worden.

Adviesfunctie wordt gemist
Bijna alle geïnterviewde organisaties hebben pogingen gedaan zekerheid te zoeken bij overheidsorganisaties ter zake van hun experimenten. Soms betrof het contacten met ministeries (Binnenlandse Zaken en Veiligheid en Justitie) maar veelal (ook) met het CBP. Opmerkelijk is dat slechts één erin geslaagd ook werkelijk advies van het CBP te krijgen. Effect van dit advies was overigens dat deze partij in zijn geheel aan de veilige kant is gaan zitten: ook die gegevens waar het CBP geen privacyrisico zag zijn geaggregeerd (tot het niveau ver boven dat van herleidbaarheid).

Relatie met CBP wordt gedomineerd door angst
In een groot aantal gesprekken is aangegeven dat men het CBP vreest. Deze vrees zit in de (vermeend) onvoorspelbare uitkomst en het gegeven dat 'als je eenmaal gemeld hebt wat je wil gaan doen, ze het wel weten'. In een enkel geval is er daarom bewust voor gekozen (nog) te wachten het CBP te benaderen: men vreesde dat het initiatief, bij betrokkenheid van het CBP, gevaar zou kunnen lopen.

CBP vertrouwt niet op eigen verantwoordelijkheid verwerkers
Een veel gehoorde klacht, vooral ook van de geïnterviewde markt-

partijen, is dat het CBP voorbij zou gaan aan het feit dat het ook in het belang is van organisaties om zorgvuldig met de privacy van hun burgers en klanten om te gaan en dat er dus een gemeenschappelijk belang is om samen te werken om tot een goede privacybescherming te komen, wat uiteindelijk het doel is van de privacywetgeving. Het wordt daarom unaniem als wenselijk ervaren dat het CBP zijn benadering in dit opzicht verandert en de deur (weer) op een kier zou zetten.

Wie controleert de controleur?

Voorts is opgemerkt dat het CBP de adviezen van de Artikel 29 Werkgroep standaard overneemt, alsof deze juridisch bindend zijn. De adviezen bevatten soms vergaande interpretaties van bestaande wetgeving waardoor het toepassingsbereik van de privacywetgeving almaar groter wordt. Ook nationale rechters zijn geneigd deze te volgen. Deze krijgen als het ware kracht van wet, terwijl er geen enkele volksvertegenwoordiger naar gekeken heeft en er geen enkele belangenafweging heeft plaatsgevonden. Anders gezegd, men meent dat er noodzakelijke *checks and balances* ontbreken.

Interne vertaling van de onzekerheden

Bij afwezigheid van eenduidige antwoorden zien we dat de organisaties vervolgens processen en structuren inrichten waarin *checks and balances* zitten en waarin gepoogd wordt de privacyregels zo goed mogelijk na te leven. Zo zien we in een aantal cases dat het privacybelang steeds opnieuw wordt afgezet tegen het belang van het oplossen van het concrete probleem. Langs die lijn heeft men regels en processen geschapen waarin transparantie, eerlijkheid, onafhankelijk toezicht en de toetsbaarheid van beslissingen geborgd worden.

Bonte verzameling oplossingen

Bestuurlijk-organisatorisch zien we overigens een veelheid aan oplossingen. Dikwijls is de verantwoordelijkheid voor de naleving van de Wbp-regels neergelegd bij de ‘data-inwinners’. Dit wordt echter wel als klemmend ervaren omdat zij in toenemende mate, naast hun traditionele werkzaamheden, moeten beoordelen of het voorziene gebruik van hun data – door andere afdelingen! – nog wel past binnen het doel en de grondslag van de verzameling. Ze moeten dan dus beslissen over gebruik in domeinen die hun relatief vreemd zijn. Uiteraard helpt het als ter zake een functionaris gegevensbescherming (FG) geconsulteerd kan worden. Maar in de praktijk gebeurt dit niet altijd – data-inwinners hebben dus een keuze – onder meer omdat men soms meent dat de FG te ver van de beleidspraktijk af staat.

Op en over het randje

Dat neemt niet weg dat men soms, ondanks de organisatorische en procedurele waarborgen, het gevoel heeft ‘op het randje te zitten’ en het gebruik van de gegevens in de praktijk tot herleidbaarheid leidt. Bijvoorbeeld in gebieden waar de bevolkingsdichtheid laag is. Met andere woorden: hoewel men de uiterste best doet om herleidbaarheid te voorkomen, kan dit van te voren soms niet waterdicht worden geregeld.

Impact van de onzekerheden

De onzekerheden, de gepercipieerde onmogelijkheid om die onzekerheden weg te nemen en de bestuurlijke realiteit leiden ertoe dat het risico ontstaat dat men ‘dingen in een hoekje gaat doen’ en men bestuurders ‘zekerheidshalve ongeïnformeerd’ laat. Datzelfde geldt voor de betrokkenheid van interne privacy-deskundigen (zoals een FG). Een meer open dialoog, meer hulp en een helderder kader, gericht op de (geo-)praktijk, zou dit kunnen voorkomen, zo is de mening.

De gevoelde rechtsonzekerheid – ingewikkelde regels en geen instantie die definitieve zekerheid kan geven – heeft voorts een negatieve impact op het innoverend vermogen en bemoeilijkt de interne besluitvorming rondom nieuwe toepassingen. Zo heeft een van de cases aangegeven dat circa 50% van de tijdsbesteding gemoeid met de innovatie op ging aan het vormgeven van de ‘juridische *compliance*’. Eindresultaat is dat men erg voorzichtig is: men probeert, zo goed en kwaad als dat gaat, vast te stellen wat mag en bouwt vervolgens bij de uitvoering (behoorlijk) wat veiligheidsmarges in.

OM MEE TE NEMEN NAAR HET VOLGENDE HOOFDSTUK

We hebben gezien dat op diverse plaatsen binnen de overheid – en ook daarbuiten uiteraard – druk geëxperimenteerd wordt met locatie-informatie. De geocomponent in die data vormt daarbij steevast het koppelpunt. De doelen zijn steeds nobel en staan in het teken van het verhogen van de effectiviteit en efficiency bij het uitvoeren van de publieke taken en bedrijfsprocessen. Dat men daarbij de regels rond bescherming van persoonsgegevens in acht moet nemen is goed bekend. Evenwel is de concrete toepassing van de regels op het voorgenomen gebruik van de locatie-informatie voor velen een black box: men snapt de regels niet en vindt ze veel te abstract. Alhoewel men in eerste instantie de juristen liever buiten de deur houdt, gaat men op zeker moment toch op zoek naar de antwoorden.

Deze zoektocht naar meer zekerheid gaat niet over rozen: intern schiet de inhoudelijke kennis vaak tekort en bovendien is men dikwijls huiverig er (van meet af aan) een jurist bij te betrekken. Enkele cases doen pogingen om de te maken afwegingen (tussen doel van de verwerking en de mogelijke privacyimpact) onderdeel te maken van beslisroutines. Dit wordt evenwel als moeilijk ervaren.

Ook extern advies levert lang niet altijd de antwoorden op waar men naar op zoek is. Pogingen ‘bij de officiële instanties’ uitsluitsel te krijgen – zoals het CBP en het ministerie van BZK – bleken in de meeste gevallen tevergeefs. Daarbij komt nog dat er weinig vertrouwen is in een open dialoog. Veel meer wordt de relatie beheerst door angst en wantrouwen. De onzekerheid en wantrouwen dragen niet bij aan het realiseren van de beoogde doelen. Integendeel, veelal leidt dit tot suboptimalisatie en vertraging.

Veel gepercipieerde obstakels dus, en weinig oplossingen. Niettemin, er zijn voldoende aanknopingspunten voor het ontwarren van kluwen. Daar gaat het laatste hoofdstuk over.

De spanningen en de mogelijke richting van oplossingen

We hebben het potentieel gezien, de regels en de worsteling in de praktijk. Waar zitten nu spanningen en waar zitten de aanknopingspunten voor oplossingen? Gezien het feit dat we ervoor gekozen hebben een Witboek te schrijven – en dus vooral observeren in plaats van te opiniëren – zit er een grens aan de concreetheid van de adviezen.

ANALYSE VAN DE SPANNINGEN

Zoals we in het vorige hoofdstuk hebben gezien ervaren gebruikers van locatie-informatie spanningen tussen enerzijds de beleidsambities die ze hebben en anderzijds de regels die ze daarbij in acht moeten nemen. Hieronder fileren we deze spanningen, waarmee aanknopingspunten ontstaan deze te reduceren.

Spanning op het niveau van regels
Een eerste spanningsveld is gelegen in de regels zelve. Hoe men het ook wendt of keert: het regelgevingskader is gericht op het tegengaan van ongebreidelde verwerking van persoonsgegevens waaronder (de meeste) locatie-informatie. Dit botst dus met de belangen van de gebruikers van die informatie, die juist lekker zorgeloos willen verwerken om hun ambities te realiseren.

Het binaire karakter van de persoonsgegevenbeschermingsregels speelt hierbij een rol: er zitten geen grijstinten in. Als een gegeven een persoonsgegeven is, moet verwerking conform alle Wbp-regels plaatsvinden. Daarmee komen verwerkingen die een geheel onschuldig karakter hebben en die goed beschouwd het ‘goede’ beogen – betere en efficiëntere diensterlening – op dezelfde stapel te liggen als verwerkingen met een minder nobel doel. Daar komt nog bij dat het bereik van het begrip ‘persoonsgegeven’ door de jaren heen steeds groter is geworden, onder meer onder invloed van de Artikel 29 Werkgroep.

Daarbij komt dat het regelgevingsmandaat in Brussel ligt. Over het algemeen zullen hier compromissen uitkomen. Dit impliceert ook dat

de ruimte om het nationaal anders te doen zeer beperkt is, zeker als dit onderwerp per Verordening geregeld gaat worden. Voor velen is ook het huidig functioneren van de Artikel 29 Werkgroep een doorn in het oog. Via haar opinies en adviezen heeft zij (beweerdelijk) veel invloed op de toepassing en het bereik van de regels, terwijl daar geen enkele democratische controle op zit.

Spanning op het niveau van referentiekaders en perspectieven
Omdat de attributen van locatie-informatie in toenemende mate verbonden zijn dan wel herleidbaar zijn tot natuurlijke personen, worden zij die deze informatie gebruiken onvermijdelijk het domein van de privacybescherming ingetrokken. Hierdoor komen twee werelden samen die voorheen gescheiden waren. Ook dit levert spanning op.

De wereld van de privacybescherming wordt bevolkt door juristen (advocaten, regelgevers en toezichthouders) en verschilt fundamenteel van, wat we maar noemen, de locatie-informatie-gebruikers-wereld. De eerste groep denkt vanuit de potentiële risico's en de *worst case scenario's,* en veel minder vanuit het concrete gebruik. De *potentie* van een inbreuk op de persoonlijke levenssfeer is leidend.

De gebruikers van (en dienstenaanbieders rond) locatie-informatie denken anders: hun perspectief is het oplossen van een concreet probleem of het benutten van een kans die zich aandient. Hun context is concreet en relatief te overzien en hun *mindset* is niet gedreven door wat mogelijk mis kan gaan. Dat wil niet zeggen dat hetgeen ze doen verboden is, maar het referentiekader verschilt: het is een afweging tussen de kans en het risico van het benutten van die kans (zoals mogelijk negatieve publiciteit en het verlies van klanten). Aldus normeren ze privacy veel meer vanuit een sociaal-economisch-maatschappelijk perspectief en hun missie daarbinnen. Kortom, het handelingsperspectief alsmede de *drivers* van de gebruikers en zij die de regels maken, interpreteren en bewaken zijn fundamenteel anders, net als de eenheden waarin ze rekenen.

Spanning op het niveau van de communicatie
Privacyregels worden als onduidelijk en abstract ervaren, waardoor er onzekerheid heerst over de juiste toepassing. Daarbij is behoefte aan een dialoog met de toezichthouder, met name het CBP. Deze heeft echter in de loop der tijd, mede tegen de achtergrond van de almaar stijgende werkdruk en de budgettaire beperkingen, deze adviesrol teruggesnoeid en in de praktijk is het voor partijen zeer lastig gebleken (inhoudelijk) in gesprek te komen met het CBP. De verwerkers lopen het risico achteraf te horen te krijgen dat ze het verkeerd hebben gedaan, terwijl zij juist op voorhand graag hadden willen weten wat de juiste toepassing geweest zou zijn. Dit wekt wrevel. Een kleine nuancering hierop is dat het CBP haar beleid recentelijk heeft bijgesteld en weer vaker in gesprek wil gaan met belangen- en koepelorganisaties.

Spanning op het niveau van de zeggenschap en regie
Op een hoger abstractieniveau speelt een discussie over de rechtvaardiging (in deze tijd) van de in 1995 – het jaar dat de Privacy Richtlijn werd aangenomen – gemaakte keuzes. Sommigen menen dat deze niet meer van deze tijd zijn en dat een nieuwe weging van belangen gemaakt zou moeten worden die zou moeten leiden tot een herallocatie van rechten, plichten en bevoegdheden. Daarbij wordt dikwijls gesteld dat het huidig model te paternalistisch is en dat een deel van de zwaardmacht, die thans bij de toezichthouders ligt, niet terug zou moeten naar de burgers, meer recht doende aan *the power of the crowd.*

MOGELIJKE OPLOSSINGSRICHTINGEN

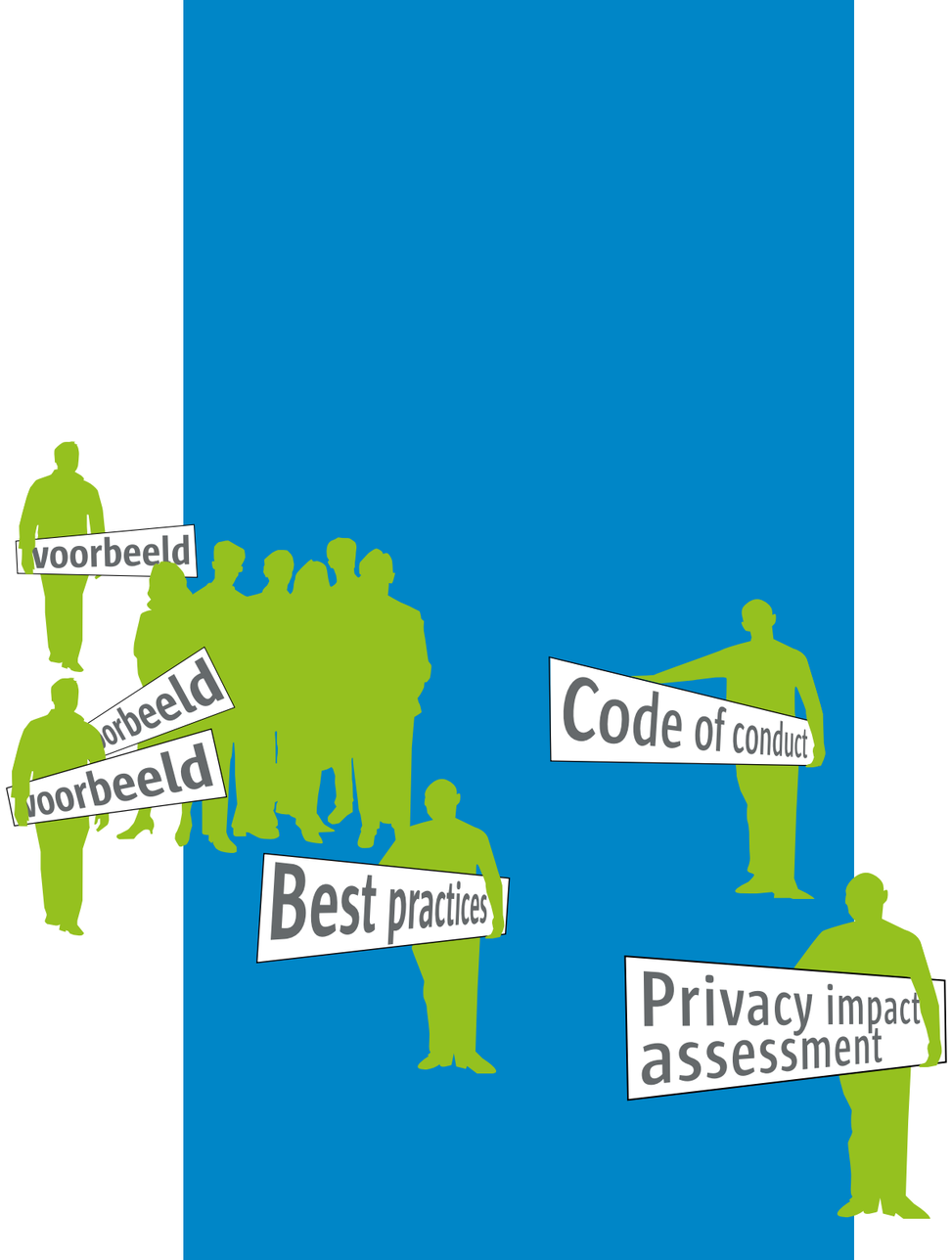
De aanwezigheid van de spanningen leidt tot suboptimalisatie: mogelijkheden blijven on- of onderbenut, kosten worden gemaakt die niet gemaakt zouden hoeven worden en energie stroomt weg naar de verkeerde activiteiten. Anders gezegd: het is zinvol om waar mogelijk deze spanningen te reduceren. Wij denken dat hiervoor drie pistes zijn, met ieder een eigen horizon en ambitieniveau.

Piste 1: proberen en doen in het hier en het nu
De eerste piste wordt gevormd door de directe belanghebbenden bij het juiste gebruik van locatiegegevens. Zij hebben een acuut belang bij

het wegnemen van de bestaande spanningen en de concrete barrières die thans het innovatieve gebruik van locatiegegevens obstrueren. Dit zijn typisch de partijen die in de uitvoering tegen vragen aanlopen die onbeantwoord blijven, zoals bijvoorbeeld de gemeentes beschreven in hoofdstuk 3 van dit Witboek, en uiteraard ook, in enige hoedanigheid, de toezichthouder.

Binnen deze setting moet ook plaats zijn voor andere belanghebbenden. Daarbij valt allereerst te denken aan geo-informatie gerelateerde bedrijven die toegevoegde waarde diensten bouwen op de locatie-gegevens. De aanwezigheid van een goed functionerend koepel, zoals Geobusiness Nederland – die heeft aangegeven graag in deze beweging mee te gaan – is een mooi bijkomend voordeel. Daarnaast zou ook de positie van de burger *rechtstreeks* verwoord kunnen worden, bijvoorbeeld door een *civil society* organisatie *als Bits of Freedom*. Ook van deze kant is met enthousiasme op deze suggestie gereageerd. Ook zou het denkbaar zijn dat een solide volledig te vertrouwen partij aansluit, bijvoorbeeld het CBS.

Het interessante van het aangaan van de dialoog op dit niveau, is dat dit informeel in projectmatige vorm kan plaatsvinden en de vraagstukken en dilemma's zich materialiseren in een concrete context, met concrete belangen, concrete potentiële baten en concrete risico's. Door deze te expliciteren ontstaan er afwegingen die echt zijn waarmee de discussie uit de principiële en abstracte hoek wordt gehaald (die discussies moeten ook niet op deze piste gevoerd worden). Anders gezegd: de potentiële baten (mogelijk gemaakt door de verwerking) kunnen dan afgewogen worden tegen potentiële kosten (de werkelijke risico's van schending van privacybelangen en de schade die daaruit voort zou komen). Langs die lijn wordt ook het treffen van maatregelen ter beperking en mitigatie van de risico's inzichtelijk, te begroten en te financieren. De cases liggen hierbij voor het oprapen, met name in het kader van de decentralisatie van taken en de processen die hierbij georganiseerd moeten worden. Ook het werk dat op dit moment gedaan wordt in het kader van het Doorbraakproject Open Geodata zou hier naadloos op aansluiten.



Het aangaan van deze samenwerking en dialoog in deze zeer informele context beantwoordt aan de behoefte aan scharrelruimte en een sparringpartner die vanuit de praktijk zeer gevoeld wordt. Dit vereist uiteraard wel dat de toezichthouder niet alleen de ruimte laat om te scharrelen, maar ook de bereidheid heeft om, informeel, aan de dialoog deel te nemen en daarop in te zetten. Zulks natuurlijk met de afspraak dat het hier om een scharrelpartijtje gaat zonder precedentwerking. Typische uitkomsten van dit proces zouden kunnen zijn – naast meer kennis, meer begrip en verbeterde verstandhoudingen – het opstellen van zeer praktische hulpmiddelen waarmee verwerkers uit de voeten kunnen, zoals gebruiksvriendelijk Privacy Impact Assessments, *codes of conduct, best practices* en dergelijke.

De opbrengsten van een dergelijk initiatief zijn evident: de dialoog ontstaat, het wederzijds vertrouwen wordt verder opgebouwd en er wordt gezamenlijk gewerkt aan concrete oplossingen voor echte problemen: *two worlds merge!* Bij gebleken succes is dit initiatief uiteraard opschaalbaar.

Piste 2: praten en denken over het waarom en straks

De tweede piste ligt op nationaal niveau en is gericht op de middellange termijn. Doelstelling van deze piste is het aangaan van het gesprek over de strategische beleidsmatige vragen die spelen rond het goed gebruik van geo-informatie en het in acht nemen van privacybelangen. Ook daar is de kern van de truc het aangaan van het gesprek, maar dit keer op een beleidsmatig niveau, dus niet op het niveau van de concrete uitvoering die op piste 1 ligt. Aan tafel moeten plaatsnemen zij die het beleid maken, waarbij te denken valt aan: het Ministerie van Infrastructuur en Milieu (verantwoordelijk voor het goed gebruik van geo-informatie), het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (vanuit burgerperspectief en het Open Data dossier), het Kadaster (als houder van een aantal grote geo-basisregistraties), Geonovum (als coördinerende instantie) het Ministerie van Veiligheid en Justitie (als eigenaar van het privacydossier en als initiatiefnemer van de verkenning naar een Kaderwet Gegevensuitwisseling), het Ministerie van Economische Zaken (de bedrijvenkant), de Vereniging Nederlandse Gemeenten, het

Interprovinciaal Overleg, GeoBusiness, GeoSamen, en uiteraard het CBP en *civil society* organisaties zoals *Bits of Freedom*.

Als gezegd gaat het hier om de grotere strategische en ethische vraagstukken. Typische onderwerpen zouden kunnen zijn:

- Welke balans is nodig tussen de behoefte aan innovatie en bescherming van persoonsgegevens;
- Wat zijn de grondslagen voor en draaipunten van het functioneren van bescherming van persoonsgegevens;
- Wat is de slijtvastheid van de gehanteerde axioma's;
- Wat zou de allocatie moeten zijn van rechten en plichten, het toezicht en de rechtsbescherming;
- Welke vrijheid moet gelden voor de burger vrijelijk te beschikken over zijn persoonsgegevens richting bedrijven;
- Wat zijn de ordeningsmechanismen - de krachten van de markt, toezicht door de overheid, of de macht van de 'crowd'- en hoe interacteren ze;
- Wie heeft de regie over het proces van verandering? Kan dit overgelaten worden aan de markt? Zijn er sectorale oplossingen denkbaar, of is dit achterhaald?
- Hoe gaan we om met territorialiteit van regelgeving en de wereldwijde bewegingsmogelijkheden van data? Welke eisen stelt dit aan internationale afstemming en welke eenheden zijn daarbij het aangrijpingspunt? Bedrijven, staten, gebruik, natuurrechten van burgers, contracten? Etc.

Gezien de bezetting ligt het voor de hand dat dit vanuit het GI-Beraad geïnitieerd zou worden. Om het te verrichten denkwerk handjes te geven, lijkt het raadzaam hier ook wat onderzoekscapaciteit aan te verbinden waarin een breed spectrum van relevante kennis vertegenwoordigd is (techniek, recht, bestuurskunde, ethiek en dergelijke). Uiteraard vergt dit ook enige uithoudingsvermogen en zal het zaak zijn concrete doelstellingen te formuleren, wellicht ook in een meer programmatische aanpak. Natuurlijk is het raadzaam hierbij de internationale verbindingen te zoeken, dit kan sectoraal zijn, maar ook horizontaal, bijvoorbeeld langs de lijnen van het INSPIRE netwerk.

Piste 3: concrete dialoog over de concept Privacy Verordening
Een derde piste is die in Brussel. Het is namelijk niet ondenkbaar dat de discussies over de concept Privacy Verordening wederom ten principale gevoerd gaat worden, nu er een nieuwe Europese Commissie en een nieuw parlement gekozen is. Op vele plaatsen in Europa wordt namelijk inmiddels hardop de vraag gesteld of de keuzes die de concept Verordening maakt – op veel punten borduurt deze voort op de axioma's van de Privacy Richtlijn – wel echt de juiste zijn.

Bij deze tweede ronde zal het zaak zijn op tijd aan tafel te zitten. Waar dit dossier bij het ministerie van Veiligheid en Justitie ligt, zou het raadzaam zijn dat het ministerie van Infrastructuur en Milieu voortvarend zou schakelen op het juiste ambtelijke niveau. Dit mede gezien de vaart die de Europese Commissie heeft aangekondigd te willen maken.

TOT SLOT

De mogelijkheden die de alom aanwezigheid en bruikbaarheid van locatie-informatie biedt, schept in toenemende mate een spanningsveld met de regels ter bescherming van de verwerking van persoonsgegevens en de hoeders daarvan. Deze spanning manifesteert zich op tal van niveaus en leidt tot een suboptimale benutting van het potentieel, verlies van energie en onnodige kosten.

De oplossingen zijn gelegen in het bijeenbrengen van de twee werelden door het scheppen van een dialoog, die leidt tot erkenning van wederzijdse belangen met het besef dat de voortzetting van de huidige praktijk op termijn geen (te verkiezen) optie is. Om de dialoog te laten werken moet een onderscheid gemaakt worden tussen de uitvoering – die dringend verlegen zit om concrete oplossingen – en het meer principiële, strategische, ja bijna ethische niveau, die op nationaal niveau en in Brussel gevoerd moet worden.

Overzicht bijlagen

Bijlage I
Onderzoeksverantwoording

Wie?
Dit Witboek is geschreven door Angélique van Oortmarssen, Marc de Vries en Bastiaan van Loenen (korte resumés van de auteurs zijn opgenomen in bijlage VI) in opdracht van de Programmaraad van Geonovum. De begeleidingsgroep bestond uit Rob van de Velde (Geonovum), Bastiaan van Loenen (Geonovum | TU Delft) en Dirk van Barneveld (Ministerie van Infrastructuur en Milieu).

Daarnaast hebben circa 50 andere personen bijgedragen aan de totstandkoming in de vorm van gesprekspartner dan wel deelnemer aan de Bubbelbijeenkomst gehouden op 8 juli 2014. Hun – persoons! – gegevens zijn opgenomen in de Bijlage II.

Waarom?
Met het massaal vrijkomen van data (binnen en buiten de overheid), krijg geo-informatie – meer in het bijzonder specifieke informatie over iemands locatie –een steeds belangrijker rol bij de invulling van het begrip ‘persoonsgegeven’ dat het thans draaipunt vormt van de bescherming van persoonsgegevens. Goed beschouwd is een locatie het koppel- en culminatiepunt van persoonsgegevens aan het worden.

De kennis over deze rol van geo-informatie en het grootschalig inwinnen daarvan, lijkt evenwel, zeker buiten het geo-domein, beperkt. Dit klemt te meer omdat op dit moment tal van belangrijke beslissingen op de rol staan waarin het geo-perspectief vertegenwoordigd zou moeten zijn. Het niet betrekken van dit perspectief zou tot gevolg kunnen hebben dat het de daarmee samenhangende belangen onvoldoende voor het voetlicht zouden komen hetgeen een negatieve invloed zou kunnen hebben niet alleen op het geo-domein zelve, maar ook op de ‘export van de baten’ daarbuiten.

Reden waarom de Programmaraad van Geonovum verzocht heeft dit onderwerp in de vorm van een project op te pakken en, bij gebleken noodzakelijkheid, de discussies daarover te beleggen en nader te borgen.

Wat?
Met deze context in gedachten beoogt dit onderzoek de kennis over en het bewustzijn van de relatie tussen locatie-informatie en dataprotectie te vergroten in die gremia wiens besluiten een impact zullen hebben het goed functioneren van (afspraken over) locatie-informatie en, daar waar nodig, duurzaam te agenderen en beleggen.

Uiteraard heeft Geonovum dit gedaan vanuit haar kerntaak: het bijdragen aan de samenwerking en afstemming tussen overheden op het gebeid van geo-informatie en het goed gebruik van geo-informatie ten algemene nutte. Voorts spreekt het voor zich dat bij de uitvoering zo veel mogelijk aansluiting is gezocht bij reeds bestaande relevante initiatieven, zoals bijvoorbeeld het privacy-spoor binnen het Doorbraakproject Open (geo) Data en het Programma Beter benutten.

Hoe?
De uitvoering van het onderzoek heeft plaatsgevonden langs vier actielijnen:
- Het inventariseren en samenvatten van bestaand onderzoek;
- De in de praktijk gevoelde knelpunten beschrijven aan de hand van interviews met praktijkmensen (overheid, bedrijfsleven, toezichthouders etc.);
- Het initiëren van de discussies in diverse gremia (binnen en buiten de geo-wereld);
- Het opstellen van een Witboek waarin de bevindingen worden samengevat in een voor onze doelgroepen goed verteerbaar stuk.

In dit kader hebben interviews met 14 organisaties plaatsgevonden, te weten: Centraal Bureau voor de Statistiek, de Universiteit van Tilburg, Net2Legal Consultants, TomTom N.V., ESRI BV, gemeente Zwolle, Vodafone Group Trading Limited, de Technische Universiteit Delft, de gemeente Eindhoven, het College Bescherming Persoonsgegevens, de gemeente Almere, de gemeente Amsterdam, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Bits Of Freedom.

Daarnaast is op 8 juli 2014 in Amersfoort een Bubbelbijeenkomst gehouden waarbij deelnemers met de benen op tafel hebben meegedacht over het onderwerp en hun visie op de toekomst hebben gegeven. Voorts is op 9 september 2014 een gehele ‘Geonovum Programmaraad@’ aan dit onderwerp gewijd, inclusief presentaties van externen (waaronder de KLPD) en een paneldiscussie. Tenslotte is het concept van het Witboek en de oplegnotitie voorgelegd aan de Programmaraad van Geonovum en wel op 6 november 2014 en zijn deze gepresenteerd aan het GI-beraad op 20 november 2014.

De tekst van het Witboek is afgesloten op 13 november 2014.

Bijlage II
Lijst van personen die hebben bijgedragen aan totstandkoming Witboek

Lijst van namen geïnterviewde personen
In het kader van dit onderzoek hebben we gesprekken gehad met de navolgende personen:

Naam	Organisatie
Barendswaard, P.	Centraal Bureau voor de Statistiek
Cuijpers, C.	Tilburg University
Fokke, E.	Centraal Bureau voor de Statistiek
Gardeniers, H.	Net2Legal Consultants
Hania, S.	TomTom N.V.
Herbold, M.	Environmental Systems Research Institute Nederland
Jager, E.	Gemeente Amsterdam
Kuiper, N.	Gemeente Zwolle
Lichtenberg, J.	Vodafone Group Trading Limited
Loenen, B. van	Technische Universiteit Delft
Kanters, T.	Gemeente Eindhoven
Nas, S.	College Bescherming Persoonsgegevens
Offermans, M.	Centraal Bureau voor de Statistiek
Raab, R.	Vodafone Group Trading Limited
Oelens, U.	College Bescherming Persoonsgegevens
Pleeging, J.	Gemeente Zwolle
Steeg, T. van der	Gemeente Almere
Sonnenschein, L.	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Zenger, R.	Bits Of Freedom

Lijst van namen van deelnemers aan de Bubbelbijeenkomst
Op 8 juli 2014 is een Bubbelbijeenkomst gehouden. Doel daarvan was partijen die met dit onderwerp te maken hebben samen te brengen, niet alleen om (kort) te vertellen wat de bevindingen tot dan toe waren, maar vooral ook om deze mensen met elkaar in gesprek te brengen. In totaal hebben 21 genodigden meegepraat en meegedacht, te weten:

Naam	Organisatie
Barneveld, D. van	Ministerie van Infrastructuur en Milieu
Bergmeijer-Weerman, E.	Kadaster
Broekhaar, M.	Gemeente Zwolle
Eck, J. van	Environmental Systems Research Institute Nederland
Gardeniers, H.	Net2Legal Consultants B.V.
Grothe, M.	Stichting Geonovum
Harten, C. van der	GeoBusiness Nederland
Jager, E.	Gemeente Amsterdam
Kanters, T.	Gemeente Eindhoven
Kloet, K.	Ministerie van Economische zaken
Oortmarssen, A. van	Stichting Geonovum
Schilderman, S.	The Green Land B.V.
Rooy, K. de	Provincie Noord-Holland
Steeg, T. van der	Gemeente Almere
Steenbruggen, J.	Rijkswaterstaat
Stor, R.	Stichting Geonovum
Verdonk, Y.	Stichting Geonovum
Velde, R. van de	Stichting Geonovum
Vetjens, B.	Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek
Vries, M. de	Stichting Geonovum
Vosselman, W.	Centraal Bureau voor de Statistiek
Zijlstra, T.	The Green Land B.V.
Zoest, V. van	Stichting Geonovum

Bijlage III
Semantiek

Nota bene: er wordt een scherp onderscheid gemaakt tussen enerzijds het begrip ‘locatiegegevens’ en anderzijds het begrip ‘locatie-informatie’ dan wel ‘locatie-data’. ‘Locatiegegeven’ wordt *alleen dan* gebruikt als daarmee gedoeld wordt op de term zoals gedefinieerd in de ePrivacy Richtlijn.

In dit Witboek komt een aantal termen veelvuldig voor. Tenzij in de tekst anders aangegeven, hebben zij de hieronder weergegeven betekenis.

- **Geo-informatie** - informatie over objecten of fenomenen die direct of indirect geassocieerd zijn met een locatie gerelateerd aan de aarde, op basis van een x- en y-coördinaat.
- **Locatie-informatie** – een met x- en y-coördinaten geduide plek op aarde van een tastbaar (persoon of object) of virtueel (grens, bestemmingsplan) attribuut.
- **Persoonsgegeven** – elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 1a Wbp)
- **Verwerking van persoonsgegevens** – *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 (artikel 1b Wbp)*
- **Locatiegegevens** – gegevens die worden verwerkt in een elektronische-communicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker van een algemeen beschikbaar elektronische-communicatiedienst wordt aangegeven (artikel 2c van de ePrivacy Richtlijn)

Bijlage IV
Beschrijving van juridische kader bescherming van persoonsgegevens

CONTOUREN VAN PRIVACYBESCHERMING

Voor privacy bestaat geen algemeen aanvaarde definitie. Eerder is het een 'elastisch concept', dat afhankelijk is van eigen percepties en varieert in de tijd, mede onder invloed van technologische en sociaal maatschappelijke ontwikkelingen.[55] Niettemin zitten in de vele definities die in de loop der jaren bedacht zijn wel een aantal gemeenschappelijke elementen, namelijk (1) iemands beheersmacht over zijn interacties en communicatie met anderen en (2) iemands beheersmacht over gebruik van zijn gegevens door anderen, waardoor iemands kwetsbaarheid wordt beschermd en zijn beslis- en gedragskeuzes toenemen.[56]

Privacy is geen doel op zich, het is een middel om andere doelen te bereiken, zoals individualiteit, waardigheid, integriteit en creativiteit.[57] Privacy stelt in staat eigen keuzes te maken en diepste gevoelens te tonen. Afwezigheid van privacy zal een *'chilling effect'* hebben op de bereidheid af te wijken van de norm en bereidheid kritische te zijn ten opzichte van autoriteiten.[58] En zonder privacy besluiten anderen welke keuzes iemand heeft in het leven.[59]

Privacybehoefte is vaak sferisch: je wil niet dat je huisarts informatie deelt met je werkgever, maar diezelfde huisarts mag die informatie wel delen met het ziekenhuis waar je behandeld wordt. Deze behoefte is ook cultureel bepaald: zo kijken Amerikanen fundamenteel anders aan tegen bescherming van privacy dan Europeanen.[60] Tegelijkertijd is de privacyverwachting 'een levend ding', continu onderhevig aan sociaal-maatschappelijke veranderingen en ontwikkelingen in de technologie.[61]

Het recht op privacy wordt vaak ingedeeld op basis van de mate waarin men beheersmacht heeft over de toegang die anderen kunnen hebben: lichamelijke privacy, geestelijke privacy, territoriale privacy en gedragsprivacy. Deze laatste kan weer opgedeeld worden in fysieke privacy (het recht om zich te kunnen afsluiten, zonder benaderd te worden), informationele privacy (het recht te bepalen welke informatie over iemand aan anderen bekend is, ook wel 'gegevensbescherming' genoemd) en communicatieprivacy (het recht dat anderen geen toegang hebben tot de inhoud van communicatie).[62]

WETTELIJK KADER BESCHERMING VAN PERSOONSGEGEVENS EN LOCATIEGEGEVENS

Inleiding

De wereld van de bescherming van persoonsgegevens wordt met name bewoond door juristen en dan ook nog eens 'privacyrecht' juristen. Privacyrecht kenmerkt zich door een hoog abstract karakter en is bovendien niet echt in één van de klassieke rechtsgebieden te plaatsen (privaatrecht, publiekrecht, strafrecht, internationaal recht). In feite, zoals wel meer 'ICT-onderwerpen', stoort privacyrecht zich niet aan deze grenzen en heeft het een beetje van alles. Logischerwijs is privacyrecht dan ook een echt specialisme geworden, dat voor de buitenstaander – zelfs het juridische soort daarvan – soms moeilijk te doorgronden en toe te passen is. Dit gezegd zijnde, doen we hieronder niettemin een poging het recht rond bescherming van persoons- en locatiegegevens inzichtelijk te maken.

55 Loenen, B. van, Jong J. de, Zevenbergen J., *'Locating mobile devices; balancing privacy and national security,* NWO Research Report, 2008, p. 17.

56 Margulis, S.T., *On the Status and Contributions of Westin's and Altman's Theories of Privacy,* Journal of Social Issues, 50, no. 2, 2003, p. 415.

57 Westin, A.F., Privacy and Freedom, Atheneum, New York, 1967, p. 13, Pederson, D.M. *Model for Types of Privacy by Privacy Functions,* Journal of Environmental Psychology 19, no. 4

58 Onsrud, H.J, Johson, J. Lopez, X., *Protection Personal Privacy in Using Geograpic Information Systems.* Photogrammetric Engineering and Reomte Sensing LX, no. 9: 1083-95.

59 Koops, B.J., Tendensen in *Opsoring en Technologie; over Twee Honden En Een Kalf, Nijmegen:* Wolf Legal Publishers, 2006, p. 32.

60 Whitman 2004.Whitman, J.Q, *The Two Western Cultures of Privacy: Dignity Versus Liberty,* The Yale Law Journal 113, 2004, p. 1161.

61 Koops, B.J., Leenes, R., 'Code' and the Slow Eriosion of Privacy, *Michigan Telecommuncations and Technology Law Review 12,* no. 1: 115-88, pp. 132 en 149.

62 Nouwt S., Privacyrecht voor doe-het-zelvers. *Over zelfregulering en het verwerken van persoonsgegevens via internet,* SDU Uitgevers, Den Haag, 2005, p. 19.

Verankering bescherming persoonsgegevens
Het recht op bescherming van persoonsgegevens ligt vast in de Grondwet[63], het Handvest van de Grondrechten van de Europese Unie[64] en het Verdrag betreffende de werking van de Europese Unie[65].

De Europese wetgever heeft voorts nadere regels gemaakt met betrekking tot de bescherming van locatie- en persoonsgegevens en wel in de ePrivacy Richtlijn (uit 2002[66], aangepast in 2009)[67] en de algemene Privacy Richtlijn[68]. Deze regels zijn grotendeels geïmplementeerd in de Telecommunicatiewet[69], respectievelijk de Wet Bescherming Persoonsgegevens[70]. De ePrivacy Richtlijn is een sectorspecifieke richtlijn die voorgaat op de algemene regels van de Privacyrichtlijn. Waar de ePrivacyrichtlijn niet voorziet, is de Privacyrichtlijn van toepassing. De algemene regels van de Privacyrichtlijn vormen dus een belangrijk vangnet.

63 Artikel 10 lid 2 en 3 Grondwet, Hierin is verankerd dat nadere wetgeving regels stelt *'ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens en inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens'.*
64 Artikel 7 van dit Handvest bepaalt dat eenieder recht heeft op bescherming van de hem betreffende persoonsgegevens en geeft hiervoor ook een aantal spelregels, namelijk: (a) eerlijke verwerking, (b) voor bepaalde doeleinden, (c) met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet, (d) met een recht van inzage en rectificatie (e) allemaal onder toezicht van een onafhankelijke autoriteit.
65 Artikel 16 van dit verdrag bepaalt dat eenieder recht heeft op bescherming van de hem betreffende persoonsgegevens en bepaalt voorts dat het stellen van regels over de verwerking van persoonsgegevens en het vrij verkeer daarvan een Brusselse competentie is.
66 Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie).
67 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming.
68 Richtlijn 1995/46/EG van het Europese Parlement en de Raad van betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
69 Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie.
70 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens.

ePrivacy Richtlijn (Telecommunicatiewet)
De ePrivacy Richtlijn richt zich specifiek op gegevensverwerking in de telecommunicatiesector, waaronder de verwerking van verkeers- en locatiegegevens. Deze Richtlijn is daarmee slechts van toepassing op aanbieders van elektronische-communicatiediensten die communiceren via openbare netwerken en legt hen specifieke verantwoordelijkheden en verplichtingen op (onder meer ter zake van opslag, beveiliging, vertrouwelijkheidsgaranties, spamming en het gebruik van cookies).

Definitie verkeers- en locatiegegevens
Art. 2 sub b van de ePrivacy Richtlijn definieert verkeersgegevens als *'gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische communicatienetwerk of voor de facturering ervan'.* Art. 2 sub c van de ePrivacy Richtlijn definieert locatiegegevens als gegevens *'die worden verwerkt in een elektronische-communicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker van een algemeen beschikbaar elektronische-communicatiedienst wordt aangegeven'.*[71] Als locatiegegevens worden verwerkt voor het overbrengen van de communicatie, vallen zij onder verkeersgegevens: als locatiegegevens worden verwerkt ten behoeve van diensten met toegevoegde waarde, vallen zij niet onder verkeersgegevens.[72]

Verwerking verkeers- en locatiegegevens
Verkeersgegevens, die in sommige gevallen dus tevens locatiegegevens zijn, mogen volgens art. 6 van de ePrivacy Richtlijn slechts worden verwerkt 1) voor de transmissie van de communicatie, 2) indien noodzakelijk voor de facturering[73] en 3) ten behoeve van marketingdoeleinden of voor de levering van diensten met toegevoegde waarde (dit slechts na expliciete toestemming van de abonnee, welke toestemming op elk moment weer kan worden ingetrokken). Als gegevens niet meer nodig zijn voor de transmissie van de communicatie moeten deze worden geanonimiseerd of verwijderd, tenzij de gegevens nog noodzakelijk zijn voor de verwerkingen als genoemd onder 2 en 3. De gegevensverwerking moet beperkt

71 Artikel 2 sub c ePrivacy Richtlijn.
72 Knol, P.C. en Zwenne, G.J. Telecommunicatiewet: tekst en commentaar, Kluwer, Deventer, 2009, p. 319.
73 Deze verwerking is slechts toegestaan tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen.

blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen bereiken en moet onder bevoegd gezag worden uitgevoerd.[74]

Locatiegegevens, anders dan verkeersgegevens, mogen volgens art. 9 van de ePrivacy Richtlijn slechts worden verwerkt als 1) deze anoniem zijn gemaakt of 2) als deze verwerking nodig is voor de levering van een dienst met toegevoegde waarde[75] en gebruikers hiervoor ook hun expliciete toestemming hebben gegeven. Voorts moet de verwerking noodzakelijk zijn voor het te bereiken doel en dient de verwerking onder bevoegd gezag plaats te vinden.[76] Voor het verkrijgen van de toestemming moet de dienstaanbieder de gebruiker of abonnee in kennis stellen van de soort locatiegegevens die zullen worden verwerkt, de doeleinden waarvoor de locatiegegevens zullen worden verwerkt en de duur van de verwerking. Ook moet de dienstaanbieder aangeven of de gegevens aan een derde zullen worden doorgegeven ten behoeve van de levering van de dienst met toegevoegde waarde. Gebruikers of abonnees kunnen hun toestemming voor de verwerking locatiegegevens te allen tijde intrekken.

Privacy Richtlijn (Wbp)

De Privacy Richtlijn beoogt dataprotectieregels in de Lidstaten te harmoniseren. Dit enerzijds met het doel het fundamentele recht op privacy (bij het verwerken van persoonsgegevens) te beschermen en anderzijds om een vrij verkeer van data tussen Lidstaten te scheppen. Daarmee bevat de Richtlijn in zichzelf al een behoorlijk spanningsveld.

De Richtlijn heeft een horizontaal karakter: het maakt geen onderscheid tussen verwerking door overheden en bedrijven. Het bevat een aantal kernbegrippen die vrij abstract van karakter zijn, zoals de begrippen ‘persoonsgegevens’ en ‘verwerking’. Dit geldt ook voor de personae dramatis waarop de Richtlijn ziet –

74 Artikel 6 lid 5 ePrivacy Richtijn: onder het gezag van de aanbieders van de openbare communicatienetwerken of – diensten voor facturering of verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude en marketing van elektronische-communicatiediensten van de aanbieder of de levering van diensten met toegevoegde waarde.

75 Zoals adviezen over de voordeligste tariefpakketen, routegeleiding, verkeersinformatie, weerberichten en toeristische informatie. Zie overweging 18 bij Richtlijn 2002/58/EU.

76 Onder het gezag de aanbieder van het openbare elektronische-communicatienetwerk of de openbare elektronische-communicatiedienst, of de derde die de dienst met de toegevoegde waarde levert.

de verantwoordelijke, de bewaarder, de betrokkene – waaraan dan weer specifieke verantwoordelijkheden en plichten respectievelijk rechten verbonden zijn. De inhoud van de Richtlijn is grotendeels één op één in de Nederlandse regelgeving geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp).

De Wbp is van toepassing op verwerking van persoonsgegevens door een (vestiging van een) verantwoordelijke in Nederland. Daarmee hebben we direct de kernbegrippen te pakken:

- **persoonsgegevens:** gegevens die direct of indirect herleidbaar zijn tot een natuurlijk persoon.[77] Ook gegevens ‘die mede bepalend zijn voor de wijze waarop de betrokken persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld’ dienen te worden aangemerkt als persoonsgegevens;[78]
- **betrokkene:** degene op wie persoonsgegevens betrekking hebben[79];
- **verwerken:** goed beschouwd vallen alle handelingen hieronder van creatie tot vernietiging van persoonsgegevens;[80]
- **verantwoordelijke:** degene die het doel van en de middelen voor de verwerking vaststelt.[81]

De Wbp strekt zich uit over verschillende rechtsgebieden. Zo past ‘onrechtmatige karakter van ongeoorloofde verwerking’ binnen het civiele recht (onrechtmatige daad), de grondrechtelijke bescherming van de persoonlijke levenssfeer binnen het klassieke staatsrecht en de regels over de instelling van en de taakuitoefening door het CBP binnen het bestuursrecht.[82] De Wbp kent een gelaagd karakter: (1) de laag van regels die van toepassing is op iedere verwerking (binnen de Wbp), (2) de laag van strengere regels die ziet op verwerking van zogenaamde bijzondere persoonsgegevens (zoals gezondheid, godsdienst, ras etc.) en (3) de laag gericht op doorgifte van persoonsgegevens naar landen buiten de EU.[83]

77 Artikel 1 sub a Wbp.

78 TK 25892, nr. 3 (MvT), blz. 46.

79 Artikel 1 sub f Wbp.

80 Artikel 1 sub b Wbp. Zie in dit kader ook Cuijpers C.,e.a., *Bestuursrecht en ICT.* SDU Uitgevers, Den Haag, 2012, p. 62. en SDU Commentaar, *Wet Bescherming Persoonsgegevens,* SDU Uitgevers, Den Haag, 2013, p. 19.

81 Artikel 1 sub d Wet bescherming persoonsgegevens.

82 Nouwt S., Hooghiemstra T.F.M., *SDU Commentaar Wet Bescherming Persoonsgegevens,* SDU Uitgevers, Den Haag, 2013, p. 7.

83 Cuijpers C.,e.a., *Bestuursrecht en ICT.* SDU Uitgevers, Den Haag, 2012, p. 62 en SDU Commentaar, *Wet Bescherming Persoonsgegevens,* SDU Uitgevers, Den Haag, 2013, p. 22.

De verplichtingen uit deze drie lagen werken cumulatief: bij verstrekking van bijzondere persoonsgegevens aan een land buiten de EU gelden de regels uit alle drie de lagen. Naast deze drie lagen kunnen er ook nog sectorspecifieke regels zijn – bijvoorbeeld regels uit hoofde van de ePrivacy Richtlijn, maar ook nationale regels (bijvoorbeeld in het kader van geneeskundige behandelingen) – waaraan eveneens voldaan moet worden, alsmede contractuele bedingen (bijvoorbeeld geheimhoudingsclausules).[84]

De materiële normen

Artikel 6 van de Wbp bevat de essentie van de hele regeling: als er sprake is van verwerking van persoonsgegevens, moet dit behoorlijk en zorgvuldig gebeuren overeenkomstig de regels van de Wbp.

Een rechtmatige, dat wil zeggen, conform de regels van de Wbp, verwerking moeten de persoonsgegevens eerst en vooral *verzameld* zijn voor een gerechtvaardigd, duidelijk bepaald en goed omschreven doel (artikel 7). Dat doel vormt steeds het toetsingskader, dus ook bij verdere verwerking. Anders gezegd: verdere verwerking mag mits verenigbaar met het oorspronkelijke doel, ongeacht of dit plaatsvindt binnen of buiten de organisatie van de verantwoordelijke. De Wbp concretiseert niet nader wat nog wel en niet meer verenigbaar is met het oorspronkelijke doel, maar geeft in artikel 9 wel een aantal factoren die bij die afweging meegewogen moeten worden (zoals de aard van de gegevens en de ingrijpendheid van de gevolgen (voor de betrokkene) bij dit volgend gebruik).
Daarnaast moet iedere verwerking gebaseerd zijn op tenminste één van de in artikel 8 Wbp limitatief omschreven verwerkingsgronden, waarvan de belangrijkste zijn (geparafraseerd):

- *ondubbelzinnige toestemming van de betrokkene;*
- *de noodzaak daartoe op grond van een (te sluiten) overeenkomst;*
- *een wettelijke verplichting dan wel de uitvoering van een publiekrechtelijke taak die daartoe noopt;*
- *de aanwezigheid van een gerechtvaardigde belang van de verantwoordelijke dat boven het belang van de betrokkene prevaleert.*

Daar komt bij dat de verwerking ook moet voldoen aan de beginselen van proportionaliteit en subsidiariteit: de inbreuk moet in verhouding staan tot het met de verwerking te dienen doel en er moet geen andere, voor de betrokkene minder nadelige weg, bestaan. Daarnaast wordt een aantal eisen aan de gegevens gesteld: toereikend, ter zake dienend, niet bovenmatig en nauwkeurig en ze moeten ook nog eens beveiligd worden[85] en niet langer dan nodig bewaard worden.[86] Voor zogenaamde bijzondere gegevens – ras, afkomst, geloof etc. – geldt een nog stringenter regime, dus bovenop deze algemene verplichtingen van de Wbp. De hoofdregel daarbij is dat verwerking verboden is, tenzij aan zeer specifiek omschreven en zware eisen is voldaan.[87]

Verder heeft de verantwoordelijke tal van informatieplichten[88] en moeten de door hem verwerkte gegevens ook aan bepaalde kwaliteitseisen voldoen, afdoende beveiligd zijn en zorgvuldig bewaard worden.[89] Betrokkenen hebben inzage- en correctierechten90 en rechtsbescherming kan gevonden worden bij zowel de bestuursrechter (als het om een besluit gaat) en de civiele rechter (als er sprake is van een onrechtmatige daad).

Toezichthouders

De toepassing van de Wbp en de Telecommunicatiewet wordt gekenmerkt door de aanwezigheid van een aantal waakhonden met grote en minder grote tanden.

Het College bescherming persoonsgegevens

Het College bescherming persoonsgegevens (CBP) is belast met het toezicht op de naleving van de regels in de Wbp (en nog enkele regelingen).[91] De Privacy Richtlijn, op grond waarvan het CBP is ingesteld, bepaalt dat het zijn taak in onafhankelijkheid moet kunnen vervullen. Niettemin moet het bestuurlijk wel ‘ergens hangen’ en aldus ressorteert het als zelfstandig bestuursorgaan zonder rechtspersoonlijkheid onder het Ministerie van Veiligheid en Justitie. De bevoegdheden van het ministerie tegenover het CBP zijn echter beperkt. Het CBP bestaat uit circa 80 fte’s en had in 2013 een budget van in totaal € 7.586.000,-.[92]

84 Cuijpers C.,e.a., Bestuursrecht en ICT. SDU Uitgevers, Den Haag, 2012, p. 61.

85 Artikelen 11,12,13 en 14 Wbp.
86 Artikel 10 Wbp.
87 Art. 16 Wbp.
88 Zie artikelen 33 en 34 Wbp.
89 Zie o.a. artikelen 13 en 14 Wbp.
90 Zie artikelen 33 tot en met 42 Wbp.
91 Artikelen 51 tot en met 61 Wbp.
92 Jaarverslag CBP 2013, p. 66.

De belangrijkste wettelijke taken van het CBP betreffen het houden van toezicht en het geven van advies en voorlichting. In het kader van de toezichtstaak kan het, ook uit eigen beweging, onderzoek doen naar overtredingen van de wet en sancties (bestuursdwang of bestuurlijke boetes) opleggen (waartegen rechtsbescherming bestaat). Het CBP legt daarbij de nadruk op ernstige overtredingen die structureel van aard zijn en veel mensen raken. Andere toezichtactiviteiten betreffen: het bijhouden van verplichte meldingen, het toetsen van aan haar voorgelegde sectorale gedragscodes, het behandelen van klachten en bemiddelen bij geschillen over de uitoefening van het recht op inzage, correctie of verzet (waarbij het naar eigen zeggen een restrictief beleid voert).

Advisering is specifiek gericht op de regering en/of het parlement (ter zake van relevante voorgenomen wet- en regelgeving) en de Minister van Justitie (ter zake van doorgifte van persoonsgegevens naar landen buiten de Europese Unie (EU)). Volgens de website van het CBP bestaan de voorlichtingsactiviteiten uit: het verschaffen van helderheid over de uitleg van wettelijke normen in de vorm van richtsnoeren of zienswijzen, het verstrekken van informatie via haar websites (www.cbpweb.nl en www.mijnprivacy.nl) en via het telefonisch spreekuur en het publiceren van een jaarverslag.

Autoriteit Consument en Mededinging

Op 1 april 2013 zijn de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), de Mededingingsautoriteit en de Consumentenautoriteit samengevoegd tot één autoriteit: de Autoriteit Commerciële Markt (ACM). De ACM is zelfstandig bestuursorgaan zonder rechtspersoonlijkheid en valt budgettair onder het ministerie van Economische Zaken. De hoofdtaak van de ACM is het houden van toezicht op de mededinging, het consumentenrecht en – voor ons Witboek het belangrijkste – de Telecommunicatieregels. Zo houdt de ACM dus ook toezicht op aanbieders van openbare elektronische communicatiediensten of zij de locatie- en verkeersgegevens van consumenten wel op een juiste manier gebruiken en verwerken en of zij voldoen aan de privacyverplichtingen. Bij overtreding van de regels kan de ACM een dwangsom opleggen. De ACM werkt bij het toezicht op hoofdstuk 11 van de Telecommunicatiewet, waarin regels zijn neergelegd met betrekking tot de bescherming van persoonsgegevens, nauw samen met het CBP. In 2005 heeft de OPTA en het CBP een samenwerkingsprotocol opgesteld waarin afspraken zijn gemaakt over mogelijke samenloop van bevoegdheden. De ACM bestond in 2013 uit ongeveer 500 fte's[93] en het budget voor 2013 was € 771.000.[94]

De functionaris voor de gegevensverwerking

Organisaties kunnen er ook voor kiezen binnen hun eigen muren een toezichthouder in te stellen: de functionaris voor de gegevensbescherming, kortweg 'een FG'.[95] Deze FG heeft op grond van de Wbp een onafhankelijke positie en heeft als taak ervoor zorgen dat deze regeling netjes wordt nageleefd. Voorts is de FG aanspreekpunt voor alle betrokkenen, de natuurlijke personen waarvan de organisatie persoonsgegevens verwerkt. Het Cbp houdt een openbaar register van FGs bij. Daaruit blijkt dat circa 400 organisaties er eentje hebben. De FGs hebben zich ook in een club verenigd: de Nederlandse beroepsvereniging van Functionarissen Gegevensbescherming.[96]

De artikel 29 Werkgroep

Artikel 29 van de Privacy Richtlijn voorziet in de oprichting van een onafhankelijke advies- en overlegorgaan van Europese privacytoezichthouders, die men – heel toepasselijk – , de 'Artikel 29 Werkgroep' heeft genoemd. Hierin zitten alle Lidstaatwaakhonden op het gebied van bescherming van persoonsgegevens betreffende de interne markt – dus niet betreffende politie en justitie. Strevend naar een uniforme toepassing van de principes uit de privacyrichtlijn kan zij, gevraagd en ongevraagd, hierover uitleg geven. Dit doen ze dan ook veelvuldig in de vorm van werkdocumenten en opinies. Daarnaast coördineert de Werkgroep gezamenlijke handhaving van de nationale toezichthouders. De Nederlanders Peter Hustinx en Jacob Kohstamm zijn lid van de Artikel-29 Werkgroep. Peter Hustinx is al sinds 1994 lid en was van 1996 tot 2000 voorzitter van de Werkgroep. In 2004 is Peter Hustinx benoemd als Europees Toezichthouder voor de gegevensbescherming.[97] In 2008 werd Jacob Kohstamm genoemd tot vice-voorzitter van de Artikel 29 Werkgroep, waar hij van 2010 tot dit jaar voorzitter was.[98]

93 Op 1 april 2013 waren het 506 fte's, op 31 december 2013 495.
94 Jaarverslag ACM 2013, p. 21.
95 Artikelen 62 tot en met 64 Wbp.
96 Zie www.ngfg.nl.
97 www.parlement.com/id/vhy1gy6vqem0/p_j_peter_hustinx, laatstelijk geraadpleegd op 23 juli 2014.
98 www.cbpweb.nl/Pages/ind_cbp_college_kohnstamm.aspx, laatstelijk geraadpleegd op 23 juli 2014.

Bijlage V
Bibliografie

Literatuur

- Borking, J., Privacyrecht is code. Over het gebruik van Privacy Enhancing Technologies, Kluwer, Deventer, 2010.
- Cuijpers C., Koops B.J., How fragmentation in European Law undermines consumer protection: the case of Location Based Services, European Law Review, 2008.
- Cuijpers C., Privacy, overheid en digitalisering, in M. M. Groothuis (Ed.), Bestuursrecht en ICT; Monografieën Recht en Informatietechnologie (pp. 59-77). Den Haag: Sdu uitgevers., 2012.
- Cuijpers, C. Pekárek M., The Regulation of Location Based Services: Challenges to the European Union Data, Journal of Location Based Services, 2011.
- Cuijpers, C. Privacyrecht of Privaatrecht? Een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn, Sdu Uitgevers, Den Haag, 2004.
- Cuijpers, C., Berkvens J., Holvast J., e.a. Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2007.
- Cuijpers, C., Marcelis P., Oprekking van het concept persoonsgegevens beperking van privacybescherming?, Tijdschrift voor Computerrecht, Editie 13, 2012.
- Cuijpers, C.M.K.C. & Koops, E.J. (2008). How fragmentation in European law undermines consumer protection: The case of Location Based Services. European Law Review, 33(6), 880-897.
- Cvrcek, D., Marek Kumpost, Vashek Matyas, and George Danezis (2006). A Study on the Value of Location Privacy. a study undertaken in the framework activities around the FIDIS Network of Excellence presented at WPES, 2006.
- Dancet, L. Dammers, W. Kager, P., Privacy, deskundig en praktisch juridisch advies, Ius Mentis, Eindhoven, 2013.
- Dempsey Morais, C., Where is the Phrase “80% of Data is Geographic” From? in GIS Lounge, 2012.
- Dijk, T.E. van, Duthler, A.W. e.a., Uitsprakenbundel Wet bescherming persoonsgegevens, SDU Uitgevers, Den Haag, 2009.
- Doorbraakproject open(geo)data. Routekaart Doorbraakproject ‘Open Geodata als grondstof voor groei en innovatie, Den Haag, 2013.
- European Union Agency for Fundamental Rights, Handbook on European data protection law, Luxembourg: Publications Office of the European Union, 2014.
- Franken, H. e.a. Zeven essays over informatietechnologie en recht, SDU Uitgevers, Den Haag, 2003.
- Geonovum, Kracht van de kaart; de betekenis van locatie voor gemeentelijke dienstverlening.
- Geonovum, Verslag bijeenkomst: INSPIRE en gegevensbescherming (privacy), Amersfoort, 17 maart 2014.
- Geonovum, Verslag bijeenkomst: Privacy en geo-informatie, een onmogelijke combinatie!?, 10 februari 2010.
- Geonovum, Verslag bijeenkomst: Privacy en geo-informatie: een onmogelijke combinatie?!, Amersfoort, 10 februari 2010.
- Groothuis, M. M. (Ed.), Bestuursrecht en ICT; Monografieën Recht en Informatietechnologie. Den Haag: Sdu uitgevers, 2012.
- Hania, S. Locatiegegevens en de zin van exemplarische handhaving, Privacy en Compliance, 2012.
- Hert, P. de en Papakonstantinou, The Amanded EU Law on ePrivacy and Electronic Communications’, The John Marshall Journal of Computer & Information Law, 2011, 29-74.
- Hert, P. de en Papakonstantinou, V., ‘The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, Computer Law & Security Review, 2012, Vol, 28. Iss 2, 13-142.
- Hilty, L., Oertel, B., Wölk, M. Pärli, K., Geographical signposts in cyberspace, Localization technologies as a challenge for an open society, TA-Swiss 2012.
- Hilty, L., Oertel, B., Wölk, M. Pärli, K., Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern, TA-Swiss 2012.
- Hoepman J., Het recht op inzage is een wassen neus. Wat nu?, Tijdschrift voor Informatievoorziening, Editie 6, 2011.
- Jong, J. de, Privacybescherming in de geo-informatiesector, Geodesia, 2001, Jaargang: 43, 1, p. 12-17.
- Koops, B.J., Leenes, R., ‘Code’ and the Slow Erosion of Privacy, Michigan Telecommuncations and Technology Law Review 12, no. 1: 115-88, pp. 132 en 149.
- Koops, B.J., Tendensen in Opsporing en Technologie; over Twee Honden En Een Kalf, Nijmegen: Wolf Legal Publishers, 2006
- Koot, M. R., Measuring and Predicting Anonymity. University of Amsterdam, Amsterdam, (2012).
- Korff, D., EC Study on Implementation of Data Protection Directive Comparative Summary of National Laws, Cambridge (UK), 2002.

- Kranenborg, H. Wet bescherming persoonsgegevens in Europees perspectief, Deventer, Kluwer, 2011.
- Krumm, A Survey of Computational Location Privacy, Personal and Ubiquitous Computing, 2008.
- Land Registry, Privacy Impact Assessment Report; Making price paid data available through publication in a machine readable and reusable format, 2012.
- Land Registry, Privacy Impact Assessment; Review Price Paid Data, Transaction Data and Historical Price Paid Data, 2013.
- Loenen, B. van, & Kulk, S. (2012). De juridische en praktische kaders bij het hergebruiken van digitale publieke geografische informatie. In M. M. Groothuis (Ed.), Bestuursrecht en ICT; Monografieën Recht en Informatietechnologie (pp. 111-131). Den Haag: Sdu uitgevers.
- Loenen, B. van, Jong J. de, Zevenbergen J., 'Locating mobile devices; balancing privacy and national security, NWO Research Report, 2008.
- Loenen, B. van, Jong, J. de, J.A. Zevenbergen, Recht en Locatie. Geo-informatie, wat is het en wat is de juridische context?, Reeds Business, Den Haag, 2008, p. 12.
- Loenen, B. van, Memo: Relatie INSPIRE en de Wet Bescherming persoonsgegevens', 25 april 2013.
- Longley, P., Goodschild M.,, Maguire, D. J., & Rhind, D. W.,. Geographic Information Systems and Science, Chicester, John Wiley and Sons Ltd, 2011.
- Margulis, S.T., On the Status and Contributions of Westin's and Altman's Theories of Privacy, Journal of Social Issues, 50, no. 2, 2003.
- Mark P. Mills, "The Next Great Growth Cycle", The American, augustus 2012
- Mayer-Schonberger Viktor & Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think, Houghton Mifflin Harcourt, 2012
- Ministerie van Justitie, Leidraad Afstemmen Wetgeving op de Wet bescherming persoonsgegevens, bijlage kamerstuk 32761, 2010/2011 (gepubliceerd 31 mei 2011).
- Ministerie van Justitie, Sauerwein L. en Linnemann J., De Wet Bescherming Persoonsgegevens. Handleiding voor verwerkers van persoonsgegevens, Den Haag, 2002.
- Ministerie van Justitie, Winter H. Jong P. e.a., Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk, 2008.
- Ministerie van Justitie, Zwenne, G.J., Duthler, A.W., Groothuis M., e.a., Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek en knelpuntenanalyse, 2012.

- Nouwt S., Hooghiemstra T.F.M., SDU Commentaar Wet Bescherming Persoonsgegevens, SDU Uitgevers, Den Haag, 2013.
- Nouwt S., Privacyrecht voor doe-het-zelvers. Over zelfregulering en het verwerken van persoonsgegevens via internet, SDU Uitgevers, Den Haag, 2005.
- Nouwt, S. en Wees, L. van der, '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', Tilburg Institute for Law, Technology, and Society, Versie 1.0, november 2008.
- Office of Management and Budget, Open Data Policy –Managing Information as an Asset; Memorandum for the heads of executive departments and agencies, 2013.
- Onsrud, H.J, Johson, J. Lopez, X., Protection Personal Privacy in Using Geograpic Information Systems. Photogrammetric Engineering and Remote Sensing LX, no. 9: 1083-95.
- Pederson, D.M. Model for Types of Privacy by Privacy Functions, Journal of Environmental Psychology 19, no. 4.
- Ploeger, H.D., B. van Loenen, 2013, De mogelijkheid van een open data beleid voor het Actueel Hoogtebestand Nederland nader onderzocht.
- Schoenmakers, J. Privacy wordt steeds kostbaarder. EU scherpt eisen aan en geeft hoge boetes, Goed Bestuur, editie 1 2013.
- Smink, G. Privacybeleving van burgers in de informatiemaatschappij, Rathenau Instituut, Den Haag, 1999.
- Steenbruggen J., Beinat, E., Wagtendonk, A. Location Awareness 2020. A fore sight study on location and sensor services, Spinlab, Amsterdam 2007.
- Steenbruggen, J., Smits, J.M., Jong H. de., Juridische implicaties van locatie- en sensordiensten in 2020, Utrecht, 2005.
- Velde, R. te, De impact van ICT op de Nederlandse economie, onderzoek in opdracht van het ministerie van Economische Zaken
- Walle, E. van der, De privacy wordt nauwelijks bewaakt, NRC Handelsblad, De Persgroep Nederland, Amsterdam 15 juli 2011.
- Wees van der, L., Nouwt, S., Croes, R., Loenen van, B., H. de Jong, R. Peters, R. Winkels, T. van Engbers, J. Smits, W. Wefers Bettink, J. Zevenbergen. Recht en Locatie. Geo-informatie in een juridische context, Reed Business, Den Haag, 2008.
- Westin, A.F., Privacy and Freedom, Atheneum, New York, 1967.

Relevante wet- en regelgeving

- Tweede Kamer der Staten-Generaal, Memorie van Toelichting Wet Bescherming Persoonsgegevens, Vergaderjaar 1997-1998, 25 892, nr. 3.
- Tweede Kamer der Staten-Generaal, Wijziging van de Telecommunicatiewet en enkele andere wetten in verband met de implementatie van een nieuw Europees geharmoniseerd regelgevingskader voor elektronische communicatienetwerken en – diensten en de nieuwe dienstenrichtlijn van de Commissie van de Europese Gemeenschappen, Vergaderjaar 2002-2003, Kamerstuk 28 851 nr. 3.
- Tweede Kamer der Staten-Generaal, Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, Vergaderjaar 2010-2011, Kamerstuk 32 549, nr. 9.Vergaderjaar 2010-2011.
- Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).
- Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet).
- Grondwet voor het Koninkrijk der Nederlanden, 24 augustus 1815.
- 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.
- Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie.
- Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (vernietigd door het Europees Hof).
- Europees Parlement, Aangenomen teksten privacyverordening, Brussel, 12 maart 2014.
- Besluit van 7 mei 2001, Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens (Vrijstellingsbesluit Wbp).

Uitspraken/rapporten College Bescherming Persoonsgegevens, Artikel 29 Werkgroep, en Commissie voor de bescherming van de persoonlijke levenssfeer

- Artikel 29 Werkgroep, Opinion 13/2011 on Geolocation on smart mobile devices, 2011.
- Artikel 29 Werkgroep, Opinion 02/2013 on apps on smart devices, 2013.
- Artikel 29 Werkgroep, Opinion 15/2011 on the definition of consent, 2011.
- Artikel 29 Werkgroep, Advies 4/2007 over het begrip persoonsgegeven, 2007.
- College Bescherming Persoonsgegevens, 18 augustus 2005, z2005-00481, Camera's met geluidsdetectie in Groningse pilot toegestaan.
- College Bescherming Persoonsgegevens, Richtsnoeren Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer, 2009.
- College Bescherming Persoonsgegevens, 16 februari 2011, z2000-1172: Geo-informatie in de vorm van digitale 'rondkijkbeelden' van openbare ruimten valt voor een deel onder de Wbp.
- College Bescherming persoonsgegevens, Ambtshalve onderzoek CBP naar de verwerking van geo-locatiegegevens door TomTom N.V., 2011.
- College Bescherming Persoonsgegevens, De wet bescherming persoonsgegevens. Over de bescherming van uw persoonlijke gegevens, SDU Grafische Bedrijven, Den Haag, 2001.
- Commissie voor de bescherming van de persoonlijke levenssfeer, 2006a, ADVIES Nr 26 / 2006 van 12 juli 2006, BETREFT: Adviesaanvraag inzake het gebruik van satellietbeelden bij de opsporing en de vaststelling van bouwovertredingen, O. Ref. : SA2 / A / 2006 / 015, AD 26 / 2006 - 1 / 10
- Commissie voor de bescherming van de persoonlijke levenssfeer, 2006b, ADVIES Nr 40 / 2006 van 27 september 2006, BETREFT: Bijhouden van gemeentelijke registers van onbebouwde percelen waarvan sprake in artikel 62 van het Vlaams Decreet van 18 mei 1999 houdende de organisatie van de ruimtelijke ordening en hun bekendmaking op het Internet via het toekomstige geoloket, O. Ref. : SA2 / A / 2006 / 030.

Bijlage VI
Korte resumés van de auteurs

Angélique van Oortmarssen
Angélique heeft in 2012 de master Staats- en Bestuursrecht afgerond. Binnen deze master heeft zij de richting omgevingsrecht gevolgd. Zij heeft voor haar masterscriptie een juridische analyse gemaakt van een overheidsproject, namelijk de versterking van de Zwakke Schakel Noordwijk aan Zee. Deze masterscriptie was onderdeel van een groot onderzoek wat de Universiteit Utrecht deed naar dergelijke overheidsprojecten. Angélique heeft een brede juridische achtergrond en heeft werkervaring opgedaan bij verschillende advocaten- en notariskantoren.

Marc de Vries
Marc is een van de oprichters van The Green Land (www.thegreenland.eu) en is al meer dan 15 jaar werkzaam op het kruispunt van ICT, recht en bestuurlijke processen. Vanuit een gedegen juridische en economische achtergrond adviseert hij overheden uit alle lagen (EU, nationaal, provincies en gemeenten) bij het openstellen en benutten van overheidsinformatie. Hij doet dit met passie en overtuiging, zonder de bestuurlijke en economische realiteit uit het oog te verliezen. Daarnaast publiceert Marc regelmatig en draagt hij daar graag uit voor in binnen- en buitenland.

Bastiaan van Loenen
Bastiaan is een van de oprichters van het Kenniscentrum open data van de TU Delft (www.otb.tudelft.nl/opendata). Binnen het kenniscentrum wordt onderzoek gedaan naar de bestuurlijk-juridische kaders van open (geo) data vanuit zowel een nationaal als internationaal perspectief. Gegevensbescherming en hergebruik van geo-grafische gegevens behoort tot een van de huidige speerpunten van het onderzoek. Bij Geonovum verbindt Bastiaan zijn wetenschappelijke werk en resultaten met de praktische geo-realiteit. Hij publiceert en presenteert frequent over deze materie in wetenschappelijke journals, internationale congressen en expertbijeenkomsten.

Colofon

Teksten
Angélique van Oortmarssen
Marc de Vries
Bastiaan van Loenen

Vormgeving
Ontwerpstudio Spanjaard

GEONOVUM

Bezoekadres: Barchman Wuytierslaan 10 | 3818 LH Amersfoort
Postadres: Postbus 508 | 3800 AM Amersfoort

T 033 460 41 00
@geonovum
E info@geonovum.nl
I www.geonovum.nl