Ambient intelligence,

persoonsgegevens en consumentenbescherming

ECP NL
Platform voor eNederland

Binnenzijde
blanco

Ambient intelligence, persoonsgegevens en consumentenbescherming

Een productie van:

ECP NL
Platform voor eNederland

Colofon

Dit is een uitgave van ECP.NL, Platform voor eNederland.

Teksten
mr. dr. Bart W. Schermer

Ontwerp omslag en binnenwerk:
ECP.NL

Druk
Efficiënta Offsetdrukkerij bv

ISBN
978-90-76957-22-7

Management samenvatting

De ontwikkeling en toepassing van nieuwe technologieën verloopt in een razendsnel tempo. Met name op het gebied van informatie- en communicatietechnologieën volgen de ontwikkelingen elkaar in sneltreinvaart op. Onze samenleving is in zo'n twintig tot dertig jaar verworden van een industriële samenleving tot een 'informatiemaatschappij' waarin technologieën zoals het internet en de personal computer centraal staan. Echter, hier stoppen de technologische ontwikkelingen niet. Wij begeven ons inmiddels richting de volgende stap in de evolutie van onze informatiemaatschappij: ambient intelligence. In de ambient intelligence visie wordt de mens omringd door een onzichtbaar netwerk van intelligente computers, sensoren en andere ICT-middelen. In deze visie staat de gebruiker centraal: de intelligente, onzichtbare ICT-infrastructuur is zich 'bewust' van de personen in de omgeving en kan anticiperen en reageren al naar gelang de wensen en de behoeften van deze personen. De eerste voorboden van deze ontwikkeling tekenen zich inmiddels af in de vorm van RFID-toepassingen, intelligente camera's en sensornetwerken (zie hoofdstuk 2).

De komst van ambient intelligence zal veel voordelen hebben voor de consument, met name op het gebied van gemak, snelheid, efficiëntie en veiligheid. Maar, net als met elke andere technologie, zal de toepassing van ambient intelligence technologie ook gepaard gaan met onzekerheden, vragen en risico's. De risico's van ambient intelligence liggen primair in de verkeerde omgang met gegevens over personen.

Omdat in de ambient intelligence visie de gebruiker centraal staat, zal over deze gebruiker allerlei informatie verzameld moeten worden door de ambient intelligente omgeving. Hoewel dit over het algemeen geen probleem zal opleveren, kunnen bij verkeerd gebruik van gegevens of misbruik daarvan, risico's ontstaan voor de privacy van personen. Deze risico's liggen met name in de schaalvergroting bij de verwerking van persoonsgegevens, negatieve sociale en economische effecten die geassocieerd kunnen worden met profilering en personalisatie, risico's voor de privacy die ontstaan door het overvloeien van gegevens van de ene context naar de andere (sfeeroverгangen), risico op systeemdwang, en mogelijk crimineel misbruik van de ambient intelligence infrastructuur (zie hoofdstuk 6).

Doel van deze rapportage is het bijdragen aan de discussie omtrent de bescherming van gegevens over burgers/consumenten in een toekomst waarin steeds meer gegevens worden verwerkt. Wil de consument de toepassing van ambient intelligence accepteren, dan moet hij een gerechtvaardigd vertrouwen hebben in de technologie en de partijen die van deze technologische infrastructuur gebruik maken (zie hoofdstuk 3). Hierbij speelt met name de bescherming van (persoons)gegevens een grote rol, als onderdeel van de bredere noodzaak tot consumentenbescherming (zie hoofdstukken 4 en 5). De hoofdvraag van dit rapport luidt:

Hoe kan de bescherming van gegevens over burgers/consumenten in een ambient intelligente wereld adequaat worden gewaarborgd terwijl tegelijkertijd de economische en maatschappelijke kansen van ambient intelligence worden benut?

Wanneer wij kijken naar de bescherming van persoonsgegevens dan zien wij dat het juridische kader (het recht op privacy) de boventoon voert in de discussies rondom ambient intelligence en consumentenvertrouwen (zie hoofdstuk 5). Gezien het feit dat de geconstateerde risico's primair raken aan de bescherming van (persoons)gegevens wordt over het algemeen het recht op (informationele) privacy gezien als het instrument bij uitstek om deze risico's te beperken. Immers, hoe minder gegevens over een persoon bekend zijn, hoe minder risico's er kunnen ontstaan.

Het huidige juridische kader dat de informationele privacy in Nederland waarborgt, bestaat primair uit de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet (Tw). Hierbij worden de volgende uitgangspunten gehanteerd: 1) limitering van het verzamelen van gegevens, 2) doelbinding en de daarbij behorende beperkingen van gebruik, 3) eisen omtrent de kwaliteit van gegevens, 4) eisen omtrent de beveiliging van gegevens en 5) openheid omtrent het verwerken van gegevens. Deze algemene uitgangspunten van het gegevensbeschermingsrecht doorstaan goed de toets der tijd en blijven ook in de toekomst relevant.

Om nadere invulling te geven aan deze abstracte uitgangspunten worden in de Wet bescherming persoonsgegevens en de Telecommunicatiewet concrete(re) regels gesteld en handhavingsmechanismen geïntroduceerd. Echter, door de (onbewuste) techniekafhankelijkheid van een aantal van deze regels en mechanismen kan het zijn dat zij in de toekomst niet langer optimaal functioneren. Mogelijke knelpunten in de toekomst zijn 1) het huidige begrippenkader (met name de definitie van de term persoonsgegeven), 2) vragen omtrent de verantwoordelijke voor de verwerking van gegevens, 3) het moeilijk tegen kunnen gaan van systeemdwang en vrije keuze, 4) verminderde effectiviteit van de methoden om transparantie en openheid te garanderen, 5) onvoldoende aandacht voor de globalisering van de wereldhandel, 6) veranderende verhoudingen tussen bij gegevensverwerking betrokken partijen en 7) moeilijkheden met de handhaving van de wet (zie hoofdstuk 7).

Tot op heden ligt bij de bescherming van de privacy sterk de nadruk op het juridisch kader voor de bescherming van persoonsgegevens (Wbp en TW). Hoewel dit ook in de toekomst een onmisbaar instrument blijft voor het waarborgen van de privacy en het vertrouwen van de consument, zal gezien de technologische, organisatorische en institutionele veranderingen die het ambient intelligence tijdperk teweeg brengt, het gegevensbeschermingsrecht niet zelfstandig in staat blijken om de privacy en het vertrouwen van de consument te garanderen. Daarom moet gezocht worden naar alternatieve mechanismen die aanvullende bescherming kunnen bieden als aanvulling op het gegevensbeschermingsrecht.

Deze mechanismen hebben een technisch, organisatorisch en juridisch karakter. In de techniek kunnen veel privacybeschermende maatregelen worden ingebouwd (privacy by design). Reeds bij het ontwikkelen van ambient intelligence technologieën en toepassingen moeten daarom de uitgangspunten van het gegevensbeschermingsrecht in ogenschouw worden genomen. Ook moet de consument de technische middelen krijgen om invulling te geven aan zijn rechten. Op organisatorisch niveau kan (sectorale) (zelf)regulering een waardevolle verduidelijking bieden voor de algemene bepalingen uit het gegevensbeschermingsrecht. Ook dienen op organisatorisch niveau maatregelen te worden genomen om de consument te informeren over gegevensverwerkingen. Daarnaast dient de keuzevrijheid van de consument gewaarborgd te worden. Op het juridisch niveau dient met name de handhaving versterkt te worden. Een gedifferentieerd systeem van handhaving via het gegevensbeschermingsrecht, burgerlijk recht en strafrecht verdient daarom nader onderzoek. Ook lijkt het zinvol om naast de bescherming van de bouwstenen van iemands identiteit (de persoonsgegevens), aandacht te besteden aan het reguleren van gegevens binnen een bepaalde context (hoe worden gegevens en identiteiten gebruikt en beoordeeld en welke gevolgen heeft dit?).

Hoewel de uitgangspunten van het juridisch kader dus ook richting de toekomst relevant en adequaat zijn, kan voorzichtig geconcludeerd worden dat de juridische structuur van het gegevensbeschermingsrecht en de daarbinnen gekozen handhavingsmechanismen in de toekomst bepaalde aanpassingen behoeven. Hoewel het op dit moment nog te vroeg is om het juridisch kader aan te passen, strekt het tot aanbeveling om een brede, maatschappelijk gedragen discussie te voeren over de mogelijkheden om het gegevensbeschermingsrecht met het oog op de ontwikkeling van ambient intelligence te versterken. Hierbij moeten ook alternatieve technologische, organisatorische en juridische mechanismen, die flankerend aan het gegevensbeschermingsrecht aanvullende bescherming kunnen bieden, in ogenschouw worden genomen.

Klankbordgroep

Deze publicatie is tot stand gekomen met de hulp van een klankbordgroep van experts en belanghebbenden. De conclusies en standpunten uit deze rapportage vertegenwoordigen niet noodzakelijkerwijs de mening van de individuele deelnemers, noch het standpunt van hun respectievelijke organisaties. ECP.NL dankt de deelnemers voor hun constructieve bijdragen.

Naam	**Organisatie**
Fred Eisner	ABM Advies
Gerrit-Jan Zwenne	Bird & Bird Advocaten / Universiteit Leiden
Koen Dupon	Consumentenbond
Hielke Hijmans	European Data Protection Supervisor
Matthieu Andriessen	Ministerie van Economische Zaken
Roman Volf	Ministerie van Economische Zaken
Jan Wester	Ministerie van Economische Zaken
Jim Bruinsma	Ministerie van Justitie
Jeroen Terstegge	Philips International BV
Jan Berkvens	Rabobank / Radboud Universiteit Nijmegen
Christian van 't Hof	Rathenau Instituut
Eefje Van den Heuvel	Rathenau Instituut
Peter Blok	Rechtbank 's-Gravenhage
Jeroen	van den Hoven Technische Universiteit Delft
Ronald Leenes	Universiteit van Tilburg
Hubert van Breemen	Vereniging VNO-NCW
Rachel Marbus	ECP.NL, Platform voor eNederland
Bart Schermer	ECP.NL, Platform voor eNederland

Inhoudsopgave

1 INLEIDING 9
1.1 PROBLEEMSTELLING 9
1.2 DOELSTELLING 10
1.3 VRAAGSTELLING 10
1.4 AFBAKENING 10
1.5 PLAN VAN AANPAK 11
1.6 OPBOUW 11

2 TECHNISCH KADER 13
2.1 DE ONTWIKKELING VAN INFORMATIE EN COMMUNICATIE TECHNOLOGIE. 13
2.2 AMBIENT INTELLIGENCE 13
2.3 RELEVANTE TECHNOLOGISCHE ONTWIKKELINGEN 14
2.3.1 Internet 15
2.3.2 Identificatie- en sensortechnologie 15
2.3.3 Kunstmatige intelligentie 16
2.4 SCENARIO'S AMBIENT INTELLIGENCE 17
2.4.1 Huiselijke sfeer 17
2.4.2 Openbare sfeer 17
2.4.3 Werksfeer 18
2.4.4 Winkelsfeer 18
2.4.5 Zorg sfeer 18

3 AMBIENT INTELLIGENCE EN VERTROUWEN 19

4 CONSUMENTENBESCHERMING 20
4.1 DOELSTELLINGEN CONSUMENTENBESCHERMING 20
4.2 JURIDISCH KADER CONSUMENTENBESCHERMING 20
4.2.1 Algemeen BW 20
4.2.2 Handel op afstand 21
4.2.3 Privacy en bescherming van persoonsgegevens 21
4.3 TUSSENCONCLUSIE 22

5 PRIVACY EN DE BESCHERMING VAN PERSOONSGEGEVENS 23
5.1 BEGRIPSBEPALING 23
5.2 VERANDERENDE OPVATTINGEN 23
5.3 BESCHERMDE BELANGEN 23
5.3.1 Beschermen van de persoonlijke levenssfeer 24
5.3.2 Veiligheid 24
5.3.3 (Economische) gelijkheid 24
5.3.4 Het voorkomen van hinder 25
5.3.5 Waarborgen van vrijheid en autonomie 25
5.4 GEGEVENSBESCHERMING IN CONSUMENTENPERSPECTIEF 26
5.5 JURIDISCH KADER NADER BEKEKEN 26
5.5.1 De Wet bescherming persoonsgegevens 26
5.5.2 De telecommunicatiewet (hoofdstuk 11) 27
5.6 TUSSENCONCLUSIE 27

6 PERSOONSGEGEVENS EN CONSUMENTENBESCHERMING IN AMBIENT INTELLIGENCE 28
6.1 ALGEMEEN 28
6.2 AMBIENT INTELLIGENCE EN DE BESCHERMING VAN PERSOONSGEGEVENS 28
6.2.1 Schaalvergroting 28
6.2.2 Profiling en personalisatie 28
6.2.3 Gebrek aan transparantie 29
6.2.4 Systeemdwang en keuzevrijheid 29
6.2.5 Sfeerovergang 30
6.2.6 Misbruik van ambient intelligence 30
6.3 TUSSENCONCLUSIE 30

7 JURIDISCH KADER IN HET LICHT VAN AMBIENT INTELLIGENCE 31
7.1 UITGANGSPUNTEN: EEN ADEQUATE BASIS 31
7.2 MOGELIJKE KNELPUNTEN RICHTING DE TOEKOMST 31
7.2.1 Begrippenkader 31
7.2.2 Verantwoordelijkheid voor de verwerking van gegevens 33
7.2.3 Systeemdwang en vrije keuze 33
7.2.4 Transparantie 34
7.2.5 Globalisering 35
7.2.6 Veranderende verhoudingen 35
7.2.7 Handhaving 35
7.3 TUSSENCONCLUSIE 36

8 OPLOSSINGSRICHTINGEN 37
8.1 GEBRUIKER IN CONTROLE 37
8.1.1 Vergroten bewustzijn 37
8.1.2 Informeren gebruiker 37
8.1.3 Voorkomen systeemdwang 37
8.1.4 Voorkomen vervreemding 37
8.1.5 Versterken recht op inzage 38
8.1.6 Vergemakkelijken mogelijkheden tot verhaal 38
8.2 TECHNOLOGISCHE REGULERING 38
8.2.1 Privacy by design 38
8.2.2 'Privacy Aware Technologies' 39
8.3 JURIDISCHE REGULERING 40
8.3.1 Technologie onafhankelijkheid en rechtszekerheid 40
8.3.2 Internationale focus 41
8.3.3 Gedifferentieerd systeem van toezicht en handhaving 41
8.3.4 Zelfregulering 42
8.3.5 Van bescherming persoonsgegevens naar identity management *42*
8.4 OPMAAT VOOR DISCUSSIE 43

9 CONCLUSIES 44
9.1 DE BESCHERMING VAN PERSOONSGEGEVENS 44
9.2 GEGEVENSBESCHERMING IN HET LICHT VAN AMBIENT INTELLIGENCE 45
9.3 AANVULLENDE MECHANISMEN 45

10 LITERATUURLIJST 47

1 Inleiding

De snelheid waarmee technologische ontwikkelingen zich voltrekken neemt steeds verder toe. Veel technologieën hebben op zichzelf of in samenhang met andere (technologische) ontwikkelingen een belangrijke invloed op de maatschappij. Over het algemeen is de invloed van deze nieuwe technologieën positief: ze dragen bij aan onze welvaart, kwaliteit van leven en de veiligheid van onze samenleving. Echter, de 'technologische turbulentie' die ontstaat door de snelle introductie van nieuwe technologieën kan ook tot onzekerheid bij de burger en het bedrijfsleven leiden (Franken *et al.* 2000, p. 28). De gevolgen van technologische turbulentie komen met name sterk tot uiting in de informatiemaatschappij, waar informatie- en communicatietechnologieën een steeds grotere invloed hebben op ons leven.

1.1 Probleemstelling

Een belangrijk kenmerk van de informatiemaatschappij is dat onze leefomgeving steeds verder 'digitaliseert' en informatie daardoor makkelijker stroomt tussen diverse fysieke en sociale netwerken. Binnen de informatiemaatschappij laten wij namelijk steeds makkelijker bewust en onbewust informatiesporen achter. Deze ontwikkeling wordt in de hand gewerkt door diverse nieuwe technologieën die het verzamelen, verwerken en verrijken van informatie over onze persoon vergemakkelijken. Het gaat dan met name om tweede generatie internettechnologieën, identificatie- en sensortechnologieën en kunstmatige intelligentie. Gezamenlijk zullen deze technologieën vorm gaan geven aan de zogenaamde 'ambient intelligente wereld', een wereld waar wij omringd zullen zijn door intelligente systemen (Aarts en Marzano 2003).

De vergaande digitalisering van onze maatschappij heeft tot gevolg dat de grenzen tussen de publieke en private sfeer steeds verder vervagen en onze maatschappij steeds transparanter wordt.[1] Gegevens die betrekking hebben op personen (de zogenaamde persoonsgegevens) zijn in toenemende mate vast te leggen en te koppelen aan andere informatie uit diverse bronnen. Op deze manier wordt het steeds beter mogelijk om aan de hand van allerhande gegevens een (accuraat) profiel van een persoon samen te stellen. Partijen die in het bezit zijn van veel gegevens over een persoon kunnen hieraan een bepaalde 'informatiemacht' ontlenen.

Naast de hoeveelheid persoonsgegevens die verwerkt worden, neemt ook het belang van persoonsgegevens steeds verder toe in onze maatschappij. Zo worden persoonsgegevens steeds vaker gebruikt voor de identificatie, authenticatie en autorisatie van personen. Hoewel dit de snelheid en het gemak van veel processen vergroot, heeft het helaas ook tot gevolg dat de mogelijkheden tot verkeerd gebruik en misbruik toenemen.

Door de toename in de verwerking van persoonsgegevens en het belang van deze verwerkingen, is het zaak dat er zorgvuldig omgegaan wordt met persoonsgegevens. In zijn algemeenheid kan gesteld worden dat een technologie enkel gebruikt wordt wanneer gebruikers een voldoende mate van zekerheid hebben omtrent de betrouwbaarheid ervan. ECP.NL hanteert de volgende definitie van het begrip vertrouwen:

Het geloof van partijen binnen economische en sociale relaties dat de wederpartij de beste bedoelingen jegens hen heeft, eerlijk is, en in voldoende mate competent is om invulling te geven aan de relatie en de doelen die daarbinnen worden nagestreefd.

Vertrouwen in technologie is uiteraard niet alleen afhankelijk van de manier waarop persoonsgegevens verwerkt en beveiligd worden. Andere aspecten die een rol kunnen spelen zijn bijvoorbeeld de integrale veiligheid van een technologie (met andere woorden: niet noodzakelijk beperkt tot de veiligheid van gegevens) en de mogelijke effecten op het milieu en de volksgezondheid. Echter, deze aspecten zullen met het oog op het doel en de omvang van deze rapportage grotendeels worden uitgesloten van discussie.

In de ambient intelligence visie wordt de mens omringd door een onzichtbaar netwerk van intelligente computers, sensoren en andere ICT-middelen. Deze intelligente, onzichtbare ICT-infrastructuur is zich

1 Er wordt hier gedoeld op een onderscheid tussen de publieke ruimte en de persoonlijke levenssfeer, niet op een onderscheid tussen publieke partijen en private partijen.

'bewust' van de personen in de omgeving en kan anticiperen en reageren al naar gelang de wensen en de behoeften van de personen. Een uitgebreidere beschrijving van de ambient intelligence visie en de relevante technologieën vindt u in hoofdstuk 2.

Regulering van nieuwe technologieën en het gebruik van persoonsgegevens kan een belangrijke rol spelen bij het stimuleren van vertrouwen in ambient intelligence. Echter, overmatige of ineffectieve regulering kan de ontwikkeling van ambient intelligence en de economische en maatschappelijke kansen die zij bieden onnodig verstoren of vertragen.

De probleemstelling van deze rapportage is daarom als volgt geformuleerd:

Hoe kan de bescherming van gegevens over burgers/consumenten in een ambient intelligente wereld adequaat worden gewaarborgd terwijl tegelijkertijd de economische en maatschappelijke kansen van ambient intelligence worden benut?

1.2 Doelstelling

Het doel van deze rapportage is bij te dragen aan de discussie omtrent de bescherming van gegevens over burgers/consumenten in een toekomst waarin steeds meer van dergelijke gegevens worden verwerkt. In deze rapportage zal een aanzet worden gedaan voor de beoordeling van de vraag in hoeverre het huidige instrumentarium voor de bescherming van (persoons)gegevens in de toekomst adequaat blijkt in het licht van nieuwe technologieën die het verzamelen en verwerken van persoonsgegevens nog verder vergemakkelijken.

Diverse organisatorische, technische en juridische instrumenten worden aangewend om persoonsgegevens te beschermen in onze huidige maatschappij. Doelstelling van onderhavige rapportage is het verkrijgen van een beter inzicht in de werking, toepasbaarheid en houdbaarheid van deze instrumenten in de ambient intelligente wereld.

Bij deze verkenning zal de nadruk liggen op een analyse van het juridisch instrumentarium omdat dit momenteel het primaire middel is om de bescherming van persoonsgegevens gestalte te geven. Daarom zullen wij het juridisch kader voor de bescherming van persoonsgegevens analyseren en beoordelen in hoeverre dit juridisch kader toegesneden is op de introductie van nieuwe technologieën.

Met de inzichten uit deze rapportage kan een betere inschatting worden gemaakt hoe nieuwe technologieën de verzameling en verwerking van persoonsgegevens in de toekomst zullen beïnvloeden en hoe de bescherming van persoonsgegevens in de toekomst moet worden vormgegeven. Op basis van de verworven inzichten kan aldus een beter antwoord worden geformuleerd op de vraag of het instrumentarium voor de bescherming van persoonsgegevens ook in de toekomst genoeg bescherming kan bieden aan de burger en genoeg houvast biedt voor het versneld en gecoördineerd invoeren van nieuwe technologieën.

1.3 Vraagstelling

De vraagstelling die bij de bovenstaande probleemstelling hoort is de volgende:

1 Biedt het huidige instrumentarium voor de bescherming van persoonsgegevens genoeg handvatten voor een gerechtvaardigd vertrouwen in ambient intelligence?

2 Is het huidige juridische kader voor de bescherming van persoonsgegevens afdoende toegerust om om te gaan met de gevolgen van ambient intelligence?

3 Welke instrumenten kunnen in de toekomst bijdragen aan het vergroten van het vertrouwen in ambient intelligence?

1.4 Afbakening

Een onderzoek naar de gevolgen van ambient intelligence voor de bescherming van persoonsgegevens loopt al snel het risico om te abstract of te breed te worden om bruikbaar te zijn. Om deze reden is ervoor gekozen om de reikwijdte van het onderzoek duidelijk af te bakenen, zowel qua onderzochte technologieën als qua juridisch kader.

Met betrekking tot de onderzochte technologieën zal de reikwijdte hoofdzakelijk beperkt worden tot informatie- en communicatie technologieën. Te weten: de tweede generatie internet, identificatie- en sensortechnologieën en kunstmatige intelligentie. De invloed die deze technologieën kunnen hebben op het recht op privacy zullen niet zozeer afzonderlijk worden behandeld, maar veeleer

in hun samenhang worden besproken. Het uitgangspunt dat hierbij genomen zal worden is de zogenaamde 'ambient intelligence' visie. Momenteel zijn de eerste tekenen van deze visie al zichtbaar en zijn de eerste applicaties operationeel. De volledige ambient intelligence visie moet in de komende twee decennia tot wasdom komen.

Met betrekking tot het juridisch kader zal de reikwijdte worden beperkt tot de verwerking van persoonsgegevens. De Wet bescherming persoonsgegevens zal het voornaamste uitgangspunt vormen voor een bespreking van het huidige juridische kader. Bij een bespreking van het juridisch kader zullen diverse relaties worden meegenomen zoals consument-bedrijfsleven, burger-overheid, patiënt-zorginstelling, werknemer-werkgever, en burger-burger. Door de complexiteit en dynamiek van deze verschillende relaties is een uitputtende beschrijving van het juridisch kader in al deze verhoudingen echter niet realistisch. In deze rapportage zal daarom de nadruk worden gelegd op de relatie consument-bedrijfsleven.

Een belangrijke beperking op de reikwijdte wordt gevormd door de uitsluiting van een bespreking van het gebruik van persoonsgegevens binnen de opsporing. Het verwerken van informatie in zijn algemeenheid en persoonsgegevens in het bijzonder is van groot belang voor de opsporing in Nederland. Artikel 2 van de Wet bescherming persoonsgegevens geeft aan dat de bepalingen uit de wet niet van toepassing zijn op het werk van opsporingsinstanties en de veiligheidsdiensten. Gezien de specifieke vragen rondom privacy en opsporing wordt deze problematiek uitgesloten van verdere bespreking in deze rapportage.

1.5 Plan van aanpak

Met het oog op de doelstelling van deze rapportage wordt de volgende aanpak gehanteerd:

Allereerst wordt een beschrijving gegeven van de technische ontwikkelingen die zullen leiden tot de ‘ambient intelligente wereld’. Vervolgens wordt een analyse gemaakt van de voornaamste doelstellingen van de huidige wetgeving aangaande consumentenbescherming in het algemeen en de bescherming van privacy en persoonsgegevens in het bijzonder. Daarna wordt gekeken hoe de opkomst van ambient intelligence de verwerking van persoonsgegevens zal beïnvloeden en wat de weerslag hiervan is op de met de wet- en regelgeving nagestreefde belangen.

Gegeven het feit dat de technologie en de wet elkaar wederzijds beïnvloeden, zal bekeken worden of het huidige juridisch kader en het bijbehorende instrumentarium het hoofd kan bieden aan toekomstige technologische ontwikkelingen. Op deze manier kan bepaald worden in hoeverre aanpassingen aan het juridisch kader noodzakelijk zijn, en in hoeverre de techniek zich moet aanpassen aan het juridisch kader. Ook worden alternatieve instrumenten bekeken die de consument in de toekomst bescherming kunnen bieden.

1.6 Opbouw

Om een gedegen evaluatie te maken van de bescherming van persoonsgegevens en het vertrouwen in de ambient intelligente wereld, moeten wij ons allereerst een goed beeld vormen van de veranderingen die de toekomst zal brengen. Daarom wordt begonnen met het schetsen van de technologische ontwikkelingen die zullen uitmonden in de ambient intelligente wereld en het in kaart brengen van de hiervoor relevante technologieën in hoofdstuk 2. In hoofdstuk 2 wordt ook een ambient intelligence scenario geschetst om de materie tastbaarder te maken.

In hoofdstuk 3 wordt een beschouwing gegeven op de verhouding tussen technologie en vertrouwen. In hoofdstuk 4 wordt dit algemene beeld toegespitst op de bescherming van de consument en wordt gekeken welke middelen momenteel gebruikt worden voor de bescherming van de consument.

Vervolgens wordt in hoofdstuk 5 ingezoomd op de bescherming van persoonsgegevens en de daarmee nagestreefde belangen. Hierbij staat de rol die de gegevensbescherming speelt bij het beschermen van de consument en het stimuleren van vertrouwen centraal.

In hoofdstuk 6 wordt gekeken hoe ambient intelligence de bescherming van persoonsgegevens kan beïnvloeden. Op basis van deze conclusies wordt in hoofdstuk 7 geanalyseerd in hoeverre het huidige juridische kader hieraan het hoofd kan bieden.

Op basis van de conclusie uit hoofdstuk 7

wordt in hoofdstuk 8 gekeken of aanpassingen noodzakelijk zijn en hoe andere instrumenten complementair aan het juridisch kader moeten functioneren om het vertrouwen in de ambient intelligente wereld te vergroten.

In hoofdstuk 9 volgen de conclusies.

Een aantal hoofdstukken wordt afgesloten met een korte samenvatting welke een opmaat moet vormen voor verdere discussie.

2 Technisch kader

De evolutie van mens en maatschappij hangt nauw samen met de ontwikkeling van technologie. Bijna zo lang als de mens bestaat, maakt hij gebruik van zijn kennis om werktuigen te ontwikkelen en te gebruiken. Technologie kan worden omschreven als het toepassen van in de wetenschap verworven inzichten ten behoeve van praktische doeleinden.

In dit hoofdstuk zal een kort overzicht worden gegeven van de technologische ontwikkelingen en hun maatschappelijke consequenties. Met het oog op de reikwijdte van deze rapportage beperken wij ons hoofdzakelijk tot ontwikkelingen op het gebied van informatie- en communicatietechnologie (ICT). Op basis van de in dit hoofdstuk verkregen inzichten kan een beter beeld worden gevormd van de invloed die de technologie op het recht op privacy heeft.

2.1 De ontwikkeling van informatie en communicatie technologie.

De digitale revolutie kenmerkt zich door de overgang van analoge informatieverwerking naar binaire informatieverwerking. Binaire informatieverwerking stelt ons in staat om informatie eindeloos te verveelvoudigen zonder verlies van kwaliteit en tegen minimale kosten. Hierdoor werd het mogelijk om snel, eenvoudig, en efficiënt informatie te verspreiden en te verwerken. De voornaamste katalysatoren van de digitale revolutie waren de computer en het internet. De ontwikkeling van de computer en het internet zijn bijzonder relevant voor het onderwerp van deze rapportage omdat zij de grootschalige verwerking van persoonsgegevens mogelijk maakten.

Als gevolg van de digitale revolutie kan onze maatschappij inmiddels het beste gekarakteriseerd worden als een 'informatiemaatschappij' waarin het creëren, distribueren en het verwerken van informatie een substantiële economische en culturele activiteit is geworden.

Diverse demografische, economische en sociaal-politieke factoren dragen bij aan de verdere ontwikkeling van ICT. Belangrijke demografische factoren die bijdragen aan de ontwikkeling van ICT zijn de vergrijzing van de (Westerse) maatschappijen en teruglopende bevolkingsaantallen in de toekomst. De vergrijzing heeft tot gevolg dat er een grotere vraag ontstaat naar zorg en comfort, die deels met behulp van ICT vervuld kan worden. Door de teruglopende bevolkingsaantallen neemt de arbeidsbevolking af, maar door slim gebruik van ICT kan de arbeidsproductiviteit op peil gehouden worden. Belangrijke economische drijfveren voor de verdere ontwikkeling van ICT zijn met name de hogere (arbeids)productiviteit en efficiëntie die met behulp van ICT behaald kunnen worden. Daarnaast spelen risicomanagement en beter inzicht in bedrijfsprocessen ook een belangrijke rol. Tot slot zijn er tal van sociaal-politieke factoren die het gebruik van ICT binnen onze maatschappij stimuleren. In zijn algemeenheid kan ICT de kwaliteit van leven vergroten (gemak, zorg, plezier, *et cetera*) en kan het bijdragen aan onze veiligheid. Met name het belang van deze laatste factor is de laatste jaren sterk toegenomen.

Het gebruik van ICT in onze maatschappij concentreerde zich tot voorkort voornamelijk rondom de personal computer. Door een samenspel van technologische ontwikkelingen en de hierboven genoemde maatschappelijke factoren valt echter een verschuiving te constateren richting mobiele toepassingen, convergentie van infrastructuren (mobiel, vast, WIFI) en diensten (telefoon, televisie, internet) en het verwerken van computerkracht in objecten in onze omgeving. Deze ontwikkeling wordt aangeduid met de term 'ambient intelligence'.

2.2 Ambient intelligence

In zijn algemeenheid kunnen we stellen dat in de ontwikkeling van ICT vijf belangrijke trends een rol spelen: 1) alomtegenwoordigheid, 2) intelligentie, 3) delegatie, 4) interconnectiviteit, en 5) een focus op de gebruiker.[2]

Door het steeds kleiner en krachtiger worden van microprocessoren kunnen steeds meer objecten worden uitgerust met computerkracht, waardoor computerkracht steeds meer een *alomtegenwoordig* fenomeen wordt (ook wel 'ubiquitous computing' of 'pervasive computing' genoemd). Als wij kijken naar

2 Wooldridge 2002

onze huidige omgeving kunnen wij deze trend al duidelijk waarnemen: de mobiele telefoon, de auto, de videorecorder en de televisie zijn allemaal voorbeelden van voorwerpen die microprocessoren bevatten. Hierbij wordt ook het klassieke onderscheid tussen publiek en privaat steeds vager. Een goed voorbeeld zijn onze woningen: deze zullen in de toekomst steeds meer in direct contact met de buitenwereld staan door middel van allerlei vaste en draadloze (internet)verbindingen.

Door de alomtegenwoordigheid van computerkracht en de ontwikkelingen op het vlak van de kunstmatige intelligentie wordt het ook in toenemende mate mogelijk om objecten in onze fysieke leefwereld te voorzien van een bepaalde mate van *intelligentie*. Hierdoor wordt het mogelijk voor onze omgeving om op ons te reageren en zelfs tot op zekere hoogte te anticiperen op onze wensen en behoeften. Een voorbeeld hiervan is een intelligente woonkamer die bij binnenkomst van de bewoner diens favoriete muziekvoorkeur laat spelen en de kamertemperatuur of het licht aan zijn of haar wensen aanpast.

Door de toenemende intelligentie van ICT-systemen kunnen steeds meer taken aan deze systemen worden *gedelegeerd*. Taken die bijvoorbeeld te eentonig of te ingewikkeld zijn kunnen uitbesteed worden aan het systeem, waardoor de gebruiker tijd bespaart.

Door de vooruitgang in (draadloze) netwerktechnologie wordt het steeds beter mogelijk om systemen met elkaar te verbinden. Door deze toename in *interconnectiviteit* staan gebruikers en systemen in de toekomst steeds meer in permanente verbinding met elkaar.

Een laatste trend is de *focus op de gebruiker* van ICT-systemen. In toenemende mate wordt de mens in plaats van de technologie als uitgangspunt genomen bij de bouw van ICT-systemen. Een goed voorbeeld hiervan is de ontwikkeling van de grafische interface (GUI). Tot de komst van de eerste grafische interface, die als uitgangspunt voor de bediening de metafoor van een bureaublad nam, moesten alle commando's voor het bedienen van een computer worden ingevoerd in een voor de computer begrijpelijke taal. Een dergelijke aanpak was veel minder gebruiksvriendelijk dan het manipuleren van voorwerpen op een bureaublad.

In hun samenhang zullen deze trends in de toekomst samenkomen in de zogenaamde 'Ambient Intelligence' visie (Aarts en Marzano 2003). Ambient Intelligence is een visie op de toekomst van de informatiemaatschappij waarin technologie naar de achtergrond van ons leven verdwijnt en opgaat in onze (fysieke) omgeving. Hiermee kan onze leefomgeving intelligent reageren en anticiperen op onze wensen en behoeften. Gebruiksvriendelijkheid, menselijke communicatie en efficiëntie staan in deze toekomstvisie centraal.[3]

2.3 Relevante technologische ontwikkelingen

De verwachte technologische ontwikkelingen, zoals hierboven beschreven, en hun mogelijke effecten worden ingegeven door de min of meer gelijktijdige opkomst van een aantal relevante technologieën. Hieronder zullen de voor dit rapport meest relevante technologische ontwikkelingen kort afzonderlijk worden besproken. Het is uitdrukkelijk niet de bedoeling om een volledig overzicht te geven van alle technologieën die een rol spelen bij de ontwikkeling van de ambient intelligence visie, veeleer is het doel om een idee te krijgen van hoe diverse technologieën interacteren met elkaar en hun omgeving.

Het gaat dan met name om technologieën die het verzamelen en verwerken van (persoons)gegevens vergemakkelijken. Hierbij zijn, zeker voor de middellange termijn, met name de ontwikkeling van de nieuwe generatie internet, identificatie- en sensortechnologieën, evenals kunstmatige intelligentie van belang.

In een later stadium zullen ook biotechnologie en nano-technologie de nodige vragen opwerpen. Deze laatste twee technologische ontwikkelingen zullen echter grotendeels worden uitgesloten van bespreking in deze rapportage, omdat zij op de korte tot middellange termijn nog geen bijzonder grote rol van betekenis gaan spelen.

3 Bron: Rathenau Instituut

2.3.1 Internet

Met het oog op het verzamelen, verspreiden en verder verwerken van (persoons)gegevens is het internet uiteraard een belangrijke ontwikkeling. Met het oog op de privacy van de consument en de bescherming van zijn persoonsgegevens is de verdere evolutie van het internet relevant. Op dit gebied zijn er een aantal in het oog springende ontwikkelingen.

Web 2.0

Web 2.0 is een populaire benaming voor de volgende generatie internet. Er is geen duidelijke definitie van het Web 2.0 en door velen wordt het slechts gezien als een marketing buzzword. In zijn algemeenheid wordt met het Web 2.0 de ontwikkeling bedoeld naar een world wide web met een veel hogere participatie door de gebruiker. Het klassieke world wide web (het Web 1.0) is opgebouwd uit statische HTML-pagina's. Binnen deze structuur is er weinig ruimte voor gebruikers om zelf content te creëren, te delen, of om via internet gebruik te maken van applicaties. Door een combinatie van technologieën (waaronder AJAX, RSS en XHTML mark-up) wordt het steeds beter mogelijk voor gebruikers om op het internet zelf gecreëerde content (webblogs, podcasts, wiki's) te delen en via het internet gebruik te maken van programma's (online spreadsheets, wordprocessoren enzovoorts). Binnen het Web 2.0 ligt dan ook meer de nadruk op door de consument zelf gecreëerde content, social-networking elementen (Wikipedia, Hyves, LinkedIn) en interactie. Ook de komst van virtuele werelden zoals *World of Warcraft* en *Second Life* past binnen deze ontwikkeling.

Web 3.0

De volgende stap in de ontwikkeling van het internet wordt wel aangeduid met de term Web 3.0 (Spivack 2006). Web 3.0 is de populaire benaming voor de derde generatie internet. Deze ontwikkeling, die nu langzaam op gang komt, moet het internet opener, robuuster, maar bovenal 'intelligenter' maken door middel van kunstmatige intelligentie technologieën zoals het Semantic Web, datamining, natural language processing en software agents.

Een belangrijke tekortkoming van het huidige internet is dat machines (computers) de tekst op het internet niet kunnen begrijpen omdat het in natuurlijke taal (mensentaal) is geschreven. Omdat natuurlijke taal niet door computers begrepen wordt, is het voor computers bijzonder moeilijk om zelfstandig taken uit te voeren. Wanneer de informatie op het internet leesbaar wordt gemaakt voor machines, is het voor deze machines veel eenvoudiger om zelfstandig taken uit te voeren. Het Semantic Web structureert de op het internet aanwezige data op zo'n manier dat deze voor computers begrijpelijk wordt. Op die plaatsen waar natuurlijke taal wordt gebruikt kan met behulp van natural language processing door computers alsnog inzicht worden gekregen in wat de mens bedoelt.

Door deze ontwikkelingen kunnen computers uiteindelijk zelfstandig communiceren met mensen en zelfs met andere computers, omdat ze uitgaan van een gemeenschappelijk referentiekader. Daarnaast zullen computers dankzij software agents en data mining steeds beter in staat zijn om wijs te worden uit de enorme hoeveelheden data die worden gegenereerd in de informatiemaatschappij.

IPv6

Om gebruik te kunnen maken van netwerkdiensten moeten computers en andere randapparatuur een internet protocol adres hebben (IP-adres). De huidige standaard die voor het toewijzen van IP-adressen wordt gebruikt is IP versie 4 (IPv4). Deze versie heeft echter beperkte beveiligingsmogelijkheden en kent daarnaast een beperkte hoeveelheid adresruimte. Om deze reden wordt langzaam maar zeker een nieuwe versie van het Internet Protocol geïntroduceerd: IP versie 6. Met IPv6 wordt het mogelijk om elk individueel object op aarde een uniek netwerkadres te geven, waardoor objecten als lichtknoppen, koffiezetapparaten en zelfs vloertegels allemaal een eigen IP-adres kunnen krijgen.

2.3.2 Identificatie- en sensortechnologie

Zoals eerder aangegeven is er een duidelijke trend waarneembaar richting de alomtegenwoordigheid van computerkracht en een focus op de gebruiker. Dit betekent dat in toenemende mate computers hun weg vinden naar de fysieke wereld en in contact staan met gebruikers. Om dit contact te faciliteren wordt gebruik gemaakt van identificatie- en sensortechnologie.

Om de ambient intelligence visie te realiseren is het allereerst noodzakelijk dat zowel personen als objecten op eenvoudige wijze

automatisch zichzelf kunnen identificeren. De reden hiervoor is dat steeds meer communicatie over afstand en/of zonder menselijke tussenkomst plaatsvindt. Daarnaast moeten ICT-systemen uitgerust worden met sensoren om de wereld te kunnen waarnemen, hetgeen ze in staat stelt om intelligent en effectief te reageren op hun omgeving en de gebruiker.

Camera's
Videocamera's zijn zo langzamerhand een onderdeel van het straatbeeld geworden. Zij worden hoofdzakelijk gebruikt om de veiligheid van processen te vergroten of om toezicht te houden op de publieke ruimte en de daarin aanwezige personen of goederen. Technologische ontwikkelingen op het gebied van kunstmatige perceptie zorgen ervoor dat videocamera's steeds beter in staat zijn om patronen zoals nummerborden, gezichten en gedrag te herkennen. Hierdoor neemt de effectiviteit van videocamera's toe en is het niet langer noodzakelijk om altijd een menselijke operator aanwezig te hebben die de videobeelden interpreteert.

RFID
RFID is een methode om automatisch objecten, mensen of dieren te identificeren en informatie te verzamelen met behulp van radiofrequentie (RF) technologie. RFID is hiermee een verschijningsvorm van automatische identificatie en data capture (AIDC) technologie. AIDC is een verzamelnaam voor apparatuur en programmatuur die het mogelijk maakt om snel en accuraat informatie over objecten, mensen of dieren te verzamelen, op te slaan en te raadplegen. Wanneer gebruik wordt gemaakt van AIDC-technologie is het niet langer noodzakelijk om handmatig informatie in te voeren in een computersysteem. Veruit de bekendste vorm van AIDC is de streepjescode (barcode). De magneetstrip is een ander bekend voorbeeld.

Biometrie
Biometrische gegevens zijn gegevens die een persoon kunnen identificeren aan de hand van lichamelijke kenmerken. Bekende biometrische kenmerken zijn de vingerafdruk, het DNA en de stem. Minder bekende biometrische kenmerken zijn gezichtstemperatuur, oorafdruk en de wijze waarop iemand loopt. Biometrie wordt vaak in combinatie met andere technologieën (bijvoorbeeld RFID) gebruikt om de identificatie van personen te bewerkstelligen.

2.3.3 Kunstmatige intelligentie

Kunstmatige intelligentie is de tak van wetenschap die zich bezighoudt met het maken van machines die taken kunnen uitvoeren die normaal gesproken voor hun uitvoering menselijke intelligentie zouden vergen.[4] Bij kunstmatige intelligentie denkt men al snel aan robots en computers met intellectuele capaciteiten die vergelijkbaar zijn met die van mensen. Dergelijke 'sterke' kunstmatige intelligentie ligt echter nog ver in de toekomst. Kunstmatige intelligentie is echter nu al in staat om veel taken uit te voeren die voor mensen te eentonig of te ingewikkeld zijn. Met het oog op de verwerking van (persoons)gegevens is met name de ontwikkeling van data mining en autonome systemen van belang.

Data mining
Data mining is een methode om nuttige informatie uit grote hoeveelheden ruwe data te destilleren. Met behulp van data mining technologie is het mogelijk om automatisch databanken te analyseren en daarin belangrijke trends of patronen te herkennen.[5] Op basis van gesignaleerde trends kan onder andere een beter inzicht in de werking van processen worden verkregen en kunnen voorspellingen voor de toekomst worden gedaan. Data mining technologie wordt steeds belangrijker in onze informatiemaatschappij omdat de hoeveelheid data die op dagelijkse basis wordt gegenereerd exponentieel toeneemt en het steeds moeilijker wordt om wijs te worden uit deze data. Dit probleem staat bekend als 'information overload'. Als gevolg van ambient intelligence zal de hoeveelheid data alleen nog maar verder toenemen en zal het probleem van information overload groter worden. Data mining is dus een nuttige technologie om effectief met grote hoeveelheden data om te gaan.

Text mining
Text mining is het zoeken naar relevante informatie in teksten. Het overgrote deel van de informatie op het internet is geschreven in

4 Kurzweil 1990
5 Mena 2004, p. 29

'natuurlijke taal'. Hiermee worden normale, voor mensen begrijpelijke, teksten bedoeld. Echter, computers begrijpen deze teksten niet. Door gebruik te maken van kunstmatige intelligentie kunnen computers beter inzicht krijgen in natuurlijke taal en kunnen zij relevante informatie uit teksten destilleren. Dit proces wordt aangeduid met de term text mining.

Autonome systemen
Een autonoom systeem is een systeem dat zonder directe tussenkomst van een mens een bepaalde taak zelfstandig kan uitvoeren. Autonome systemen kunnen fysieke machines zijn of slimme softwareprogramma's. In het eerste geval spreken we van robots, in het tweede geval van software agenten. Met name deze tweede categorie is van belang in het kader van deze rapportage.

We spreken van software agenten als we het hebben over relatief zelfstandig handelende computerprogramma's. Het voornaamste onderscheid tussen een normaal computerprogramma en een software agent is dat - in tegenstelling tot een normaal computerprogramma - een software agent voor een gebruiker onafgebroken en zelfstandig taken uitvoert. Software agenten worden vaak gezien als 'digitale assistenten'. Zo kunnen ze automatisch het internet doorzoeken op voor de gebruiker relevante informatie, efficiënt de agenda van een gebruiker plannen, helpen bij het nemen van beslissingen, en ondersteuning bieden bij kritieke taken zoals luchtverkeersleiding en crisismanagement.

Software agenten zullen naar alle waarschijnlijkheid een belangrijke plaats in gaan nemen binnen de ambient intelligence visie omdat zij zelfstandig wijs kunnen worden uit de enorme hoeveelheid beschikbare informatie en de gebruiker kunnen helpen bij het uitvoeren van allerlei taken.

2.4 Scenario's ambient intelligence

De hierboven beschreven technologieën zullen gezamenlijk de ambient intelligente wereld gaan vormgeven. Om de notie van ambient intelligence wat tastbaarder te maken, zal in deze paragraaf een ambient intelligence scenario worden geschetst waarin een persoon (Mark) zich gedurende de dag door verschillende ambient intelligente sferen/contexten beweegt. Het is van belang te vermelden dat getracht is dit scenario te beschrijven vanuit een consument-centrieke manier: welke diensten zouden de consument/patiënt/reiziger aangeboden kunnen worden met behulp van ambient intelligence? Voorts is geprobeerd om de scenario's, voor zover mogelijk, vrij te houden van waardeoordelen omtrent de wenselijkheid of noodzakelijkheid van de geschetste ontwikkelingen.

2.4.1 Huiselijke sfeer

Om 6:30 uur wordt Mark gewekt door zijn persoonlijke wekker. De wekker is ingesteld op het specifieke bioritme van Mark en kiest de beste methode om Mark te wekken: een combinatie van licht dat de opgaande zon simuleert en zachte audio impulsen die in intensiteit toenemen naarmate de uiterste wektijd dichterbij komt. Mark staat op en loopt naar de badkamer, zijn vrouw Helena kan nog een half uurtje blijven liggen. De badkamerspiegel heeft inmiddels de sensorinformatie van Mark's bed verwerkt en geeft aan dat Mark zijn bloeddruk iets te hoog is. Waarschijnlijke oorzaak: te hoge werkdruk. Verder is Mark in goede conditie. De spiegel vertelt Mark verder dat hij vandaag beter de trein naar zijn werk kan nemen omdat de file- en GPS data gecombineerd met de beschikbare historische data aangeven dat de kans op een file langer dan 10 kilometer vandaag groter is dan de grenswaarde van 67 procent die Mark heeft aangegeven.

Na zich gewassen te hebben gaat Mark ontbijten. Het koffiezetapparaat heeft van Mark's bed reeds doorgekregen dat hij opgestaan is en de koffie staat al klaar. Een glas melk zit er helaas niet in: de rode gloed die van de in het pak verwerkte OLED-folie afkomt is een waarschuwing dat de melk over de datum is. Mark vraagt zich af waarom de koelkast nog geen nieuwe melk heeft besteld. Wanneer hij het de koelkast vraagt blijkt het antwoord simpel: Helena heeft het de koelkast verboden omdat Mark toch altijd de melk laat bederven.

2.4.2 Openbare sfeer

Mark verlaat zijn huis en ziet dat de grasmaairobot zijn gazon vannacht weer keurig heeft getrimd. Mark is net verhuisd en weet de weg naar het station nog niet zo goed te vinden, daarom vraagt hij zijn persoonlijke digitale assistent om de routebeschrijving te activeren. De route wordt getoond via een

schermpje in zijn bril. Mark zijn persoonlijke digitale assistent bevindt zich op zijn Ambient Communicator (een apparaat dat de functie van mobieltje, agenda, computer, GPS, RFID en NFC leesapparaat in één apparaat verenigt).[6]

Aangekomen op het station houdt Mark zijn Ambient Communicator (AC) tegen het poortje om toegang te krijgen tot het station. Mark heeft een hekel aan losse pasjes en heeft daarom al zijn pasjes op de AC gezet. Hij koopt bij de frisdrankautomaat met zijn AC nog een pakje melk en stapt vervolgens op de trein. In de trein leest hij de Volkskrant die automatisch gedownload is naar zijn AC. Aangekomen op de plaats van bestemming houdt hij zijn AC wederom tegen het poortje: de ritprijs wordt automatisch in rekening gebracht. Onderweg naar kantoor ziet Mark een reclame voor een nieuw type AC: eentje die volledig verwerkt is in je kleding. Dit lijkt Mark wel wat. Hij haalt zijn AC langs de poster en de informatie van de poster wordt automatisch doorgestuurd naar zijn emailadres.

2.4.3 Werksfeer

Aangekomen op het werk klokt Mark in met zijn AC. De kantoorsoftware registreert wie er binnen is gekomen en activeert Mark zijn werkstation. Aan de hand van de tijdsregistratie is te zien wanneer Mark binnenkomt, wanneer hij vertrekt en of hij al dan niet in het pand aanwezig is. Ook de lunch kan Mark betalen via zijn AC, de kosten voor de lunch worden direct van zijn loon afgetrokken. Mark kiest hoofdzakelijk gezonde producten voor zijn lunch: de baas geeft hem een bonus als hij gezond eet.

2.4.4 Winkelsfeer

Voordat hij naar huis gaat, wandelt Mark nog even langs het winkelcentrum. Hij heeft nog geen voet binnen het winkelcentrum gezet of het billboard links van hem verandert van een reclame voor babyvoeding in een reclame voor digitale camera's. Het billboard vraagt of hij interesse heeft in een interessante korting en biedt hem aan de route-informatie van de elektronicazaak up te loaden naar zijn AC. Stom, vergeten mijn privacyprofiel in te stellen op 'streng', denkt Mark bij zichzelf. Mark schakelt zijn privacyprofiel om naar 'streng' en vervolgt zijn weg. Alleen de door Mark zelf geautoriseerde winkeliers kunnen hem nu nog bereiken. Wanneer Mark in de buurt van zijn favoriete juwelier komt krijgt hij een seintje van de juwelier: de verjaardag van Helena is morgen: of hij geïnteresseerd is in een toepasselijk cadeau. Mark legt via zijn AC contact met de kledingkast van Helena, deze laat de kledingcollectie van Helena zien. De computer van de juwelier en Helena's kledingkast matchen beide collecties en kiezen op basis hiervan de best passende juwelen: een elegante halsketting en een paar oorbellen. Mark verlaat de juwelier met zijn cadeaus en loopt nog even langs de slijter voor een mooi flesje wijn. Door zijn AC bij de RFID-tag in de fles wijn te houden kan hij allerlei achtergrondinformatie over de wijn en het Chateau opvragen. Zijn persoonlijke wijndatabase geeft aan dat de Bordeaux die de slijter in de aanbieding heeft een 87% match is met zijn favoriete smaak en goed past bij de Franse kaas die nog in de koelkast ligt. Na nog wat kleine aankopen te hebben gedaan vertrekt Mark richting huis.

2.4.5 Zorg sfeer[7]

Thuis aangekomen belt Mark zijn ouders. De aanleunwoning van zijn ouders beantwoord de telefoon en geeft aan dat zijn ouders slapen. Mark besluit om zijn ouders niet te wekken. Omdat zijn moeder wat kwakkelt met haar gezondheid vraagt hij voor de zekerheid wel nog even de medische gegevens van zijn moeder op via de woning. Nadat hij zich met behulp van zijn wachtwoord en biometrische gegevens heeft geauthenticeerd, krijgt hij de gegevens. Het ziet er gelukkig allemaal geruststellend uit.

6 Het concept van de ambient communicator is ontleend aan de Ubiquitous Communicator van prof. Sakamura.

7 Voor een uitgebreide bespreking van ambient intelligence in het kader van de zorg zie het rapport *Ambient Intelligence: toekomst van de zorg of zorg van de toekomst?* van het Rathenau Instituut.

3 Ambient intelligence en vertrouwen

In hoofdstuk 2 is de ontwikkeling van ICT richting het concept van ambient intelligence omschreven. Wat duidelijk naar voren komt in dit hoofdstuk is dat de consument in de nabije toekomst steeds meer door slimme technologie omringd wordt. Naarmate steeds meer alledaagse processen worden ondersteund of zelfs worden overgenomen door intelligente technologie, neemt de 'technologische afhankelijkheid' van de consument toe. Dit vergt van de consument een hoge mate van vertrouwen in zijn slimme omgeving.

Vertrouwen is het mechanisme dat mensen in staat stelt om te gaan met situaties die gekenmerkt worden door onzekerheid en de aanwezigheid van risico's (De Vries 2004, p. 153). Wil een consument bereid zijn onzekerheid en risico's, die voortvloeien uit het gebruik van een bepaalde technologie, te aanvaarden, dan moet deze allereerst het gevoel krijgen dat een technologie toegevoegde waarde biedt. Met andere woorden: de situatie waarin de consument een nieuwe technologie gebruikt, moet bepaalde voordelen bieden boven de situatie waarin de consument de technologie niet zou gebruiken.

Bij deze beslissing speelt de mate van risico en onzekerheid natuurlijk een belangrijke rol. Door het nemen van bepaalde maatregelen kan de mate van risico en onzekerheid worden teruggebracht en kan het vertrouwen in de technologie worden vergroot. Hierbij is het belangrijk om een onderscheid te maken tussen 1) het vertrouwen in de technologie zelf (het systeem) en 2) het vertrouwen in de achterliggende actoren die de technologie aanbieden of gebruiken.

Vertrouwen in de technologie zelf omvat verschillende elementen. Een technologie moet veilig zijn, de uitkomsten van het systeem moeten voorspelbaar en consistent zijn en de technologie moet voldoende robuust zijn.

Vertrouwen in de achterliggende actoren die de technologie aanbieden of gebruiken heeft met name betrekking op de wetenschap dat de achterliggende partij zorgvuldig omgaat met hetgeen hen wordt toevertrouwd (geld, goederen, informatie enzovoorts). In het kader van dit rapport betreft het voornamelijk de zorgvuldige omgang met gegevens. Voorts is van belang om te weten of de wederpartij eerlijk en competent is en dat deze de beste bedoelingen heeft.

Gegeven het voorgaande kan vertrouwen in ambient intelligence problematisch zijn omdat de technologie in veel gevallen 'onzichtbaar' is en vaak niet in een één oogopslag duidelijk is hoe de technologie nou precies werkt achter de schermen. De consument heeft dus geen directe 'controle' over zijn slimme omgeving (en over de achterliggende partijen die de technologie en de daarop draaiende diensten aanbieden). Dit gegeven wordt versterkt door het feit dat de gebruikte technologieën in veel gevallen adaptief en zelflerend zullen zijn waardoor de uitkomsten over tijd kunnen verschillen (en dus niet noodzakelijkerwijs consistent zijn). Ook moet de consument rekening houden met mogelijk misbruik van de ambient intelligence omgeving door kwaadwillende derden. Een ambient intelligence omgeving kan dus als nuttig en handig worden ervaren, maar bij een gebrek aan maatregelen die risico's en onzekerheden inperken, in het ergste geval ook als onveilig, vervreemdend of zelfs beangstigend beschouwd worden.[8]

Om het vertrouwen van de consument in ambient intelligence (en de partijen die de achterliggende technologieën en diensten aanbieden) te stimuleren zijn tal van maatregelen noodzakelijk. Met het oog op het onderwerp van deze rapportage richten wij ons niet zozeer op het vertrouwen in de technologie zelf, maar meer op het stimuleren van het vertrouwen in de achterliggende actoren. Het juridisch kader voor consumentenbescherming vormt hierin het primaire mechanisme.

8 Zie voor een uitgebreide bespreking van deze problematiek: Wright *et al.* 2008

4 Consumentenbescherming

Naarmate de (informatie)maatschappij complexer wordt, neemt het belang van effectieve consumentenbescherming toe. Consumentenbescherming is niet alleen wenselijk om de positie van de consument als mogelijk kwetsbare partij te versterken ten opzichte van het bedrijfsleven (en de overheid), maar ook om het vertrouwen van de consument in het gebruik van nieuwe technologieën en innovatieve diensten te stimuleren. Om de juiste randvoorwaarden voor de consument te creëren kunnen diverse instrumenten worden gebruikt, zoals voorlichting, technische beschermingsmaatregelen en wet- en regelgeving. Met name deze laatste categorie is relevant met het oog op het doel van deze rapportage. Daarom wordt in dit hoofdstuk met name aandacht besteed aan het juridische instrumentarium voor consumentenbescherming.

4.1 Doelstellingen consumentenbescherming

Consumentenbescherming is een ruim begrip waar verschillende doelstellingen onder kunnen vallen. Aspecten waaraan men kan denken in het kader van consumentenbescherming zijn onder andere: 1) bescherming tegen oneerlijke handelspraktijken en misbruik, 2) het verhogen van de rechtszekerheid van de consument, 3) zorgen voor 'economische equality of arms' tussen bedrijven en consumenten, 4) het beschermen van de consument tegen overlast of hinder, 5) het beschermen van de consument tegen criminele gedragingen, 6) het wegnemen van procedurele struikelblokken of hindernissen en 7) het de consument verschaffen van toegankelijke, efficiënte en goedkope manieren van geschillenbeslechting.

De bescherming van consumenten wordt via het wettelijk kader op verschillende manieren gerealiseerd. Zo zijn er bepalingen die 1) de informatiepositie van de consument verbeteren, 2) de consument beschermen tegen oneerlijke handelspraktijken, 3) de consument een herroepingsrecht geven, en 4) het de consument mogelijk maken zichzelf of zijn gegevens af te schermen voor derden of het gebruik ervan te beperken. Deze laatste categorie is voor het onderwerp van deze rapportage met name van belang omdat hier privacy en de bescherming van persoonsgegevens als middel worden ingezet.

4.2 Juridisch kader consumentenbescherming

In Nederland zijn diverse wetten en zelfregulerende initiatieven die de consument beschermen en daarmee ook bijdragen aan het vertrouwen in het gebruik van nieuwe technologieën. Bij de bespreking van de juridische bescherming van consumenten in Nederland wordt de nadruk gelegd op de bepalingen uit het consumentenrecht die specifiek in het leven zijn geroepen als gevolg van het ontstaan van de informatiemaatschappij.

4.2.1 Algemeen BW

Bij een overeenkomst tussen bedrijven (b2b) gelden veelal andere regels dan bij een overeenkomst tussen bedrijven en consumenten (b2c). In het Burgerlijk Wetboek (BW) zijn daarvoor verschillende bepalingen opgenomen. De meest relevante bepalingen zijn die van boek 7 (consumentenkoop) en de bepalingen over de algemene voorwaarden uit Boek 6 van het Burgerlijk Wetboek.

In Boek 7 BW is een aparte afdeling opgenomen dat de zogenaamde consumentenkoop regelt. Het betreft hier de koopovereenkomst tussen een bedrijf en een particulier. De consument wordt aanvullende rechtsbescherming geboden bij het kopen van zaken (met andere woorden producten).[9]

Verder is in de verhouding tussen bedrijven en consumenten met name artikel 6:233 BW (over de onredelijk bezwarende bedingen in algemene voorwaarden) van belang. Omdat algemene voorwaarden over het algemeen integraal en eenzijdig door de consument geaccepteerd moeten worden, is artikel 6:233 in het BW opgenomen dat stelt dat bedingen uit algemene voorwaarden niet onredelijk de positie van de consument in nadelige zin mogen beïnvloeden. Dit is een open norm die nader wordt ingevuld door de grijze en zwarte lijsten uit de artikelen 6:236 en 6:237 BW. In deze lijsten staan bedingen waarvan vermoedt wordt dat zij onredelijk bezwarend zijn (grijze bedingen, zie artikel

9 Het betreft hier met name bepalingen over nakoming en garanties op producten.

6:236 BW) en bedingen die per definitie onredelijk bezwarend zijn (zwarte bedingen, zie artikel 6:237 BW).

Naast deze algemene bepalingen zijn er voor specifieke overeenkomsten en diensten, zoals betalingsverkeer, aparte aanvullende regelingen. Het voert echter te ver om deze afzonderlijk in deze rapportage te bespreken.

De algemene bepalingen hebben voornamelijk tot doel de rechtspositie van de consument in het handelsverkeer te versterken en het economisch verkeer in goede banen te leiden. De achterliggende gedachte is dat de machtsverhoudingen tussen bedrijven en consumenten anders nadelig uit zou pakken voor de consument.

4.2.2 Handel op afstand

In de informatiemaatschappij vinden steeds meer transacties over afstand plaats. Het gaat hierbij met name om overeenkomsten die via elektronische weg (bijvoorbeeld via het internet) zijn gesloten. Door de komst van de 'elektronische handel' ontstonden nieuwe vragen over de bescherming van consumenten en hun verhouding tot nieuwe spelers in de markt zoals Internet Service Providers. Om deze reden is op Europees niveau de Richtlijn elektronische handel aangenomen (ook wel de e-commercerichtlijn genoemd). In Nederland is deze richtlijn als de Wet Elektronische Handel geïmplementeerd.

De Wet Elektronische handel stelt, met het oog op consumentenbescherming, 1) eisen aan de informatie die bedrijven op hun website moeten plaatsen, 2) geeft aan dat bedrijven de manier waarop een overeenkomst online tot stand komt duidelijk moeten zijn voor de consument, 3) dat de algemene voorwaarden toegankelijk moeten zijn ten tijde van het sluiten van de overeenkomst en dat deze opgeslagen moet kunnen worden door de consument.

Naast de Wet Elektronische Handel is met de opkomst van het e-commerce tijdperk ook de Richtlijn Koop op Afstand door de EU vastgesteld, in Nederland geïmplementeerd als de Wet Koop op afstand (Boek 7a titel 1, afdeling 9a BW). De Wet Koop op afstand ziet alleen op de overeenkomsten tussen bedrijven en consumenten die op afstand (via elektronische weg) worden gesloten.

De Wet Koop op afstand is niet van toepassing op overeenkomsten die de verkoop van financiële diensten als onderwerp hebben. Hiervoor is Richtlijn 2002/65/EG betreffende de verkoop van financiële diensten op afstand (en de implementatie daarvan in de diverse Nederlandse wetten) in het leven geroepen.

Tot slot zijn er in het kader van de elektronische handel nog een aantal wetten die de rechtszekerheid voor consumenten kunnen helpen vergroten, zoals de Wet op de Elektronische Handtekening en de regelingen inzake elektronisch factureren.

In zijn algemeenheid kunnen we stellen dat de wettelijke bepalingen tot doel hebben om de consument 'online' eenzelfde niveau van rechtsbescherming te bieden als 'offline'. De verschillen tussen online en offline transacties die negatief kunnen uitpakken voor de consument (zoals het ontbreken van een fysieke locatie, het niet kunnen zien van een product, of het met één druk op een knop accepteren van algemene voorwaarden) worden aldus via de wet geadresseerd.

4.2.3 Privacy en bescherming van persoonsgegevens

Privacy en de bescherming van persoonsgegevens spelen in het kader van consumentenbescherming een belangrijke rol en dienen verschillende belangen die in paragraaf 5.3 nader uiteen gezet worden. Het recht op privacy kent vele verschillende verschijningsvormen en dient verschillende doeleinden (zie verder paragraaf 5.3). Het recht op bescherming van de persoonlijke levenssfeer (de privacy) is in Nederland grondwettelijk vastgelegd. Aan deze grondwettelijke bescherming wordt door middel van diverse (formele) wetten en zelfregulerende initiatieven nadere invulling gegeven. In het kader van deze rapportage zijn met name de Wet bescherming persoonsgegevens en de Telecommunicatiewet van belang. Deze zullen in hoofdstuk 5 nader besproken worden.

De bescherming van persoonlijke informatie (persoonsgegevens) heeft door de opkomst van de informatiemaatschappij sterk aan relevantie gewonnen. Deze vorm van privacybescherming wordt ook wel de informationele privacy genoemd (Westin 1967). Omdat in het economisch verkeer het gebruik van persoonsgegevens steeds belangrijker wordt

(voor identificatie, het sluiten van contracten, marketing enzovoorts), is het noodzakelijk een goede balans te vinden tussen het vrije verkeer van deze gegevens en de bescherming van de burger/consument. In Nederland wordt daarom het gebruik van persoonsgegevens gereguleerd door de Wet bescherming persoonsgegevens (Wbp). De Wbp schetst het kader waarbinnen gegevens mogen worden gebruikt en is aldus de belangrijkste wet op het gebied van privacy en consumentenbescherming.

Met de komst van de elektronische communicatiemiddelen zoals de fax en email kwam ook de opmars van de zogenoemde 'automatische oproepssystemen'. Deze systemen maken het mogelijk om volledig geautomatiseerd grote hoeveelheden ongevraagde (commerciële) communicatie ('spam') te versturen naar faxen en/of emailadressen. Deze spam zorgt voor veel ongemak en overlast bij de consument. Om de consument voor overlast van ongevraagde commerciële communicatie te behoeden stelt hoofdstuk 11 van de Telecommunicatiewet alsmede onderdelen uit de Wet Koop op afstand en de Wet elektronische handel regels over het gebruik van automatische oproepsystemen.

4.3 Tussenconclusie

In hoofdstuk 3 is geconstateerd dat de acceptatie van ambient intelligence door de consument alleen plaats zal vinden wanneer zij er voldoende voordeel van genieten en wanneer zij afdoende beschermd zijn tegen mogelijke negatieve gevolgen van het verkeerd gebruik of misbruik van de ambient intelligence omgeving. Om het vertrouwen in ambient intelligence te vergroten (en dan met name het vertrouwen in de achterliggende partijen) wordt onder andere het consumentenrecht ingeroepen.

Consumentenbescherming via het consumentenrecht heeft primair de volgende doelstellingen: 1) bescherming tegen oneerlijke handelspraktijken en misbruik, 2) het verhogen van de rechtszekerheid van de consument, 3) zorgen voor 'economische equality of arms' tussen bedrijven en consumenten, 4) het beschermen van de consument tegen overlast of hinder, 5) het beschermen van de consument tegen criminele gedragingen, 6) het wegnemen van procedurele struikelblokken of hindernissen en 7) het de consument verschaffen van toegankelijke, efficiënte en goedkope manieren van geschillenbeslechting.

Via het Burgerlijk Wetboek, de Wet bescherming persoonsgegevens en de Telecommunicatiewet wordt juridische invulling gegeven aan deze doelstellingen.

5 Privacy en de bescherming van persoonsgegevens

Met het oog op de probleemstelling van deze rapportage gaan wij in dit hoofdstuk nader in op het onderwerp privacy en de bescherming van persoonsgegevens. Zoals op te maken valt uit het geschetste ambient intelligence scenario zal in diverse contexten en sferen informatie over de consument verzameld en verwerkt gaan worden. In sommige gevallen zullen zelfs beslissingen worden genomen voor de consument. Het spreekt dus voor zich dat de bescherming van gegevens van groot belang is in de ambient intelligente wereld.

Alvorens het juridisch kader te bespreken, moeten we ons eerst een beeld vormen van het begrip privacy en kijken welke doelstellingen worden nagestreefd met de wetgeving op het gebied van privacy en persoonsgegevens.

5.1 Begripsbepaling

Een eenduidige definitie van het begrip privacy is moeilijk tot niet te geven. Dit komt hoofdzakelijk door het feit dat het begrip privacy slechts vorm krijgt door verwijzing naar een complex geheel van sociale, culturele, politieke, juridische en filosofische factoren waarvan het afhankelijk is (Gutwirth 1998). Het recht op privacy beschermt een nauwomlijnde, maar relatief onschendbare persoonlijke levenssfeer tegen bemoeienis van buitenstaanders (Blok 2002). In dit kader kan het recht op privacy onderverdeeld worden in een aantal concepties (wat tracht men met het recht op privacy te bewerkstelligen) en een aantal dimensies (waarop is het recht op privacy van toepassing) (Schermer 2007a, p. 71). Tot de concepties van het recht op privacy behoren onder andere: het beschermen van de persoonlijke autonomie, het afsluiten voor invloeden van buitenaf en het mogelijk maken van sociale interactie (zie verder paragraaf 5.3). Tot de dimensies van privacy behoren onder andere: het lichaam, het huis, de communicatie en het familieleven (Nieuwenhuis 2001, p. 31).

5.2 Veranderende opvattingen

Het privacybegrip is bij uitstek een begrip dat onderhevig is aan technologische en maatschappelijke ontwikkelingen. De ideeën over privacy (en de bescherming die het geniet via het recht) worden met name sterk beïnvloed door de stand van de techniek.

De eerste keer dat het recht op privacy expliciet genoemd werd, was in een artikel van de Amerikaanse rechters Warren en Brandeis (1890). In dit artikel pleitten de rechters voor een “recht om alleen gelaten te worden”. Een dergelijke conceptie van privacy was volgens hen noodzakelijk om ervoor te zorgen dat met name de roddelpers niet verder door zou dringen in de persoonlijke levenssfeer van de burger. Eén van de factoren die een rol speelden bij de totstandkoming van het artikel was de sterke opmars van de fotografie.

De opkomst van de computer in de jaren zestig en zeventig van de vorige eeuw heeft tot een revolutie in het privacydenken geleid. De vastlegging van informatie over personen in talloze databases (persoonsgegevens) werd vanaf de jaren zestig steeds meer gemeengoed. Deze ontwikkeling had een dusdanige invloed op de persoonlijke levenssfeer dat het uiteindelijk heeft geleid tot een nieuwe vorm van privacybescherming: de informationele privacy (Westin 1967). De informationele privacy is vastgelegd in de Wet bescherming persoonsgegevens, Richtlijn 95/46/EG, Conventie 108 van de Raad van Europa, en OESO-richtlijnen voor grensoverschrijdend verkeer van gegevens.

Het lijkt erop dat door de komst van het ambient intelligence tijdperk het privacybegrip een verdere transformatie zal (moeten) doormaken.

5.3 Beschermde belangen

Om een antwoord te kunnen geven op de vraag of het huidige juridische kader voor de bescherming van persoonsgegevens volstaat in de toekomst, moet allereerst worden vastgesteld wat de belangen van de burger zijn die het juridisch kader tracht te beschermen.

Voorop gesteld dient te worden dat de verwerking van persoonsgegevens onlosmakelijk verbonden is met de ontwikkeling van de informatiemaatschappij. De efficiëntie, veiligheid en het gemak van veel processen in onze moderne, consumentgerichte maatschappij is afhankelijk van de verwerking van persoonsgegevens. De consument heeft dus een direct belang bij de verwerking van (zijn) gegevens. Alleen wanneer persoonsgegevens

op een oneigenlijke manier gebruikt worden, kunnen de beschermde belangen in het gedrang komen. De beschermde belangen zijn dus niet in het geding bij het *gebruik* van gegevens, enkel bij het *verkeerd gebruik* of bij het *misbruiken* van gegevens.

In zijn algemeenheid worden met het gegevensbeschermingsrecht de volgende belangen nagestreefd: (1) bescherming van de persoonlijke levenssfeer, (2) veiligheid, (3) (economische) gelijkheid, (4) het voorkomen van hinder en (5) waarborgen van vrijheid/autonomie.[10] Je zou dus kunnen stellen dat het recht op (informationele) privacy vaak niet zozeer een doel op zichzelf is, maar eerder een middel om (onder andere) de hierboven genoemde achterliggende belangen te beschermen.

5.3.1 Beschermen van de persoonlijke levenssfeer

De klassieke functie van het recht op privacy (en nog steeds één van de meest belangrijke functies) is het afschermen van de persoonlijke levenssfeer. Dit is het beeld dat de meeste mensen hebben bij het recht op privacy: het afschermen van privé-aangelegenheden zoals het lichaam, familieleven en seksuele relaties. Het recht op privacy is in deze context dus een doel op zichzelf en niet een middel om andere doelen te realiseren zoals veiligheid, vrijheid of gelijkheid.

Wat precies de 'persoonlijke levenssfeer' omvat, is moeilijk vast te stellen. Zoals hierboven aangegeven omvat de persoonlijke levenssfeer in ieder geval dimensies als het lichaam, het huis en het familieleven, maar beperkt het zich niet noodzakelijk hiertoe. Met name door de komst van informatie- en communicatietechnologieën (en de daarbij behorende proliferatie van persoonsgegevens) is het begrip persoonlijke levenssfeer steeds minder duidelijk geworden en daarmee ook minder goed hanteerbaar. Vroeger waren er duidelijke fysieke barrières (kleding, muren) die bepaalden wat privé was en wat openbaar. Echter, deze barrières zijn de laatste jaren steeds minder scherp geworden. Hoe het ook zij, de bescherming van persoonsgegevens vervult een duidelijke rol bij het afschermen van privé-aangelegenheden.

Het valt te verwachten dat met de komst van het ambient intelligence tijdperk, waar de publieke en de private sfeer volledig via ICT-netwerken met elkaar verweven zullen zijn, de vraag wat de persoonlijke levenssfeer behelst nog moeilijker te beantwoorden zijn.

5.3.2 Veiligheid

In onze informatiemaatschappij wordt het belang van persoonsgegevens steeds groter. Omdat steeds meer van onze economische en sociale activiteiten op afstand plaatsvinden en de consument sterk hecht aan snelle en efficiënte dienstverlening, wordt het proces van identificatie, authenticatie en autorisatie steeds belangrijker in onze maatschappij. Uiteraard spelen persoonsgegevens in deze context een onmisbare rol.

Juist vanwege het grote belang van persoonsgegevens in het proces van identificatie, authenticatie en autorisatie, is de bescherming ervan essentieel. Wanneer persoonsgegevens, die gebruikt worden voor identificatie, authenticatie en autorisatie, in verkeerde handen vallen, kan dit verstrekkende gevolgen hebben voor degene op wie de gegevens betrekking hebben (denk bijvoorbeeld aan identiteitsdiefstal en ,-fraude).

Het belang dat door middel van het gegevensbeschermingsrecht wordt gewaarborgd is dus de veiligheid van de consument. Dit belang wordt gerealiseerd door het beperken van de verspreiding van persoonsgegevens naar (onbevoegde) derden.

5.3.3 (Economische) gelijkheid

Persoonsgegevens vertegenwoordigen veelal een substantiële waarde in het economisch verkeer. Deze waarde kan op verschillende manieren tot uitdrukking komen. Primair gaat het om de hoeveelheid kennis die bedrijven hebben over hun klanten en de economische macht die zij hieraan kunnen ontlenen. Verder spelen (persoons)gegevens mogelijk een rol in onderhandelingen tussen partijen (bijvoorbeeld bij sollicitaties).

Persoonsgegevens worden in het economisch verkeer primair gebruikt om klanten te identificeren en te classificeren aan de hand van aanvullende gegevens (transactionele

10 Het is van belang te vermelden dat de hier opgevoerde lijst van belangen niet uitputtend is.

data, koophistorie). Zo kunnen bedrijven op basis van een specifiek klantprofiel gerichte aanbiedingen doen of aanvullende voordelen bieden zoals betere service of interessante informatie. In deze context vertegenwoordigen de gegevens voor de bedrijven dus een economische waarde omdat deze informatie hen in staat stelt beter hun klanten te bedienen en te binden.

Omgekeerd vertegenwoordigt de persoonlijke informatie voor de consument ook een waarde. Consumenten hebben het recht om hun gegevens geheim te houden zodat bedrijven niet een betere economische machtspositie tegenover hen krijgen. Door het afschermen van persoonsgegevens wordt een situatie gecreëerd van economische gelijkwaardigheid. Naar mate bedrijven meer weten over consumenten, verschuift de economische machtsverhouding ten nadele van de consument.[11] Het gegevensbeschermingsrecht beschermt de consument in het economisch verkeer tegen ongeautoriseerd gebruik van zijn gegevens.[12]

Echter, consumenten kunnen er ook voor kiezen om hun gegevens in te zetten als 'ruilmiddel' om kortingen en betere service te bedingen. Consumenten zijn veelal bereid een stukje informationele privacy prijs te geven in ruil voor betere service of andere voordelen.

5.3.4 Het voorkomen van hinder

Ongewenste inmengingen in onze persoonlijke levenssfeer kunnen irritant of hinderlijk zijn en in het ergste geval zelfs bedreigend of beangstigend. Het recht op privacy stelt ons in staat personen en organisaties de toegang tot onze persoonlijke levenssfeer te ontzeggen. Privacy als het 'recht om alleen gelaten te worden', speelt als zodanig een belangrijke rol in het tegengaan van ongewenste inmengingen in de persoonlijke levenssfeer.

In de informatiemaatschappij zijn het niet langer alleen fysieke inmengingen die vervelend zijn, maar bijvoorbeeld ook ongewenste telefoontjes, faxen en emails. De verwerking van persoonsgegevens speelt bij het tegengaan van dergelijke hinderlijke inmengingen vaak een rol. Om deze reden wordt het gegevensbeschermingsrecht aangewend om hinderlijke inmengingen in de persoonlijke levenssfeer tegen te gaan. Een goed voorbeeld hiervan is het 'spamverbod' uit hoofdstuk 11 van de Telecommunicatiewet.

5.3.5 Waarborgen van vrijheid en autonomie

Een functie van het recht op privacy die steeds relevanter wordt naarmate de informatiemaatschappij zich verder ontwikkelt, is het waarborgen van de vrijheid en autonomie van individuen. Hoe meer informatie beschikbaar is over een persoon, hoe beter deze persoon te controleren (en zelfs te manipuleren) valt. Dit is wat sir Francis Bacon (1597) krachtig heeft samengevat in het adagium 'kennis is macht'.

Omgekeerd geldt dus: hoe minder informatie over een persoon beschikbaar is, hoe minder goed deze persoon te controleren valt. Omdat het recht op privacy informatie over personen kan verhullen, wordt het gebruikt als middel om de vrijheid en autonomie van het individu te garanderen. In deze hoedanigheid is privacy dus een middel om grondrechten als het recht op vrije meningsuiting, het recht op vrijheid van godsdienst, het recht op vergadering en het recht op betoging te garanderen. Hierbij valt een onderscheid te maken tussen vrijheid en autonomie in de publieke sector en in de private sector.

In de publieke sector functioneert het recht op privacy met name als rem op het handelen van de overheid wanneer dit handelen ingrijpt in de persoonlijke belangen van de burger. Enerzijds minimaliseert het recht op privacy zo overlast voor de burger, maar tegelijkertijd voorkomt het dat de machtsbalans tussen de overheid en de burger teveel in het nadeel van de laatste verschuift.

Ook in de private sfeer (de verhouding burger-bedrijfsleven) wordt het recht op privacy in het algemeen, en het gegevensbeschermingsrecht in het bijzonder, aangewend om de machtsbalans tussen de burger en het bedrijfsleven te bewaren. In de verhouding gaat het uiteraard meer om de economische machtsbalans, een onderwerp dat hierboven reeds is besproken.

11 In dit kader spreekt van den Hoven (1999) over 'informationele gelijkwaardigheid' tussen consumenten en bedrijven.

12 Informationele gelijkwaardigheid speelt ook een rol bij het voorkomen van discriminatie en het handhaven van sociale cohesie. Deze functie van het gegevensbeschermingsrecht zal echter in het kader van deze rapportage buiten beschouwing blijven.

5.4 Gegevensbescherming in consumentenperspectief

Wanneer we kijken naar het gegevensbeschermingsrecht als middel om de consument te beschermen dan zien we dat met name de volgende doelstellingen worden nagestreefd: zorgen voor 'economische equality of arms' tussen bedrijven en consumenten (doelstelling 3), het beschermen van de consument tegen overlast of hinder (doelstelling 4) en het beschermen van de consument tegen criminele gedragingen (doelstelling 5).

5.5 Juridisch kader nader bekeken

(Mede) om de in de voorgaande paragraaf genoemde belangen te beschermen is het recht op privacy in de Nederlandse Grondwet vastgelegd. Artikel 10 tot en met 13 van de Nederlandse Grondwet vormen de basis voor de bescherming van de privacy in Nederland.

Het gegevensbeschermingsrecht vormt een onderdeel van het recht op privacy en is op haar beurt vastgelegd in specifieke wetten zoals de Wet bescherming persoonsgegevens, de Telecommunicatiewet en enkele bepalingen uit de Wet Elektronische Handel en de Wet Verkoop op Afstand.

5.5.1 De Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) geeft nadere invulling aan het grondrecht op bescherming van de persoonlijke levenssfeer (artikel 10 Grondwet) en vloeit voort uit een aantal internationale beginselen voor de behoorlijke verwerking van persoonsgegevens.

De Wbp is de Nederlandse implementatie van Richtlijn 95/46/EG (Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens) en de opvolger van de Wet persoonsregistraties. Voornaamste doelstellingen van Richtlijn 95/46/EG zijn het niveau van de bescherming van de rechten en vrijheden van personen -met name het recht op bescherming van de persoonlijke levenssfeer- in alle Lidstaten gelijk te schakelen en een kader te bieden voor het vrije verkeer van persoonlijke data, teneinde te waarborgen dat bescherming van persoonsgegevens geen barrière vormt voor het functioneren van de interne markt.

De Wbp is van toepassing op verwerkingen van persoonsgegevens. Een persoonsgegeven is iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene). Als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

De belangrijkste uitgangspunten van de Wbp zijn:

- *Limitering van de gegevensverwerking (collection limitation principle)*

Deze bepaling stelt dat er een limiet is aan de hoeveelheid gegevens die over een persoon verzameld mogen worden en dat deze data op rechtmatige en eerlijke wijze verkregen moet worden, waar noodzakelijk met de wetenschap of toestemming van de betrokkene.

- *Kwalititeit van de gegevensverwerking (data quality principle)*

Deze bepaling stelt dat persoonsgegevens noodzakelijk moeten zijn voor het doel waartoe ze verwerkt worden en voor dit doel compleet, nauwkeurig en up-to-date moeten zijn.

- *Doelbindingscriterium (purpose specification principle)*

Deze bepaling stelt dat het doel waarvoor persoonsgegevens verzameld worden niet later vermeld dient te worden dan het moment van verkrijging, en dat de persoonsgegevens enkel en alleen mogen worden verwerkt ten behoeve van dit doel, of doelen die met het oorspronkelijke doel verenigbaar zijn.

- *Beperking gebruik gegevens (use limitation principle)*

Deze bepaling stelt dat persoonsgegevens niet openbaar mogen worden gemaakt, verstrekt of anderszins gebruikt anders dan in overeenstemming met het doelbindingscriterium. Een uitzondering op deze regel is alleen mogelijk met de toestemming van de betrokkene of in de gevallen die bij de wet zijn voorzien.

- *Veiligheid en vertrouwelijkheid gegevens (security safeguards principle)*

Deze bepaling stelt dat er adequate veilig-

heidsmaatregelen genomen dienen te worden om persoonsgegevens te beschermen tegen ongeoorloofde toegang, vernietiging, gebruik, aanpassing of openbaring.

- *Openheid en transparantie (openness principle)*

Deze bepaling stelt dat er een algemeen beleid van openheid dient te zijn met betrekking tot ontwikkelingen, toepassingen en beleidsvorming op het gebied van de verwerking van persoonsgegevens. Het moet in afdoende mate mogelijk zijn om het bestaan en de aard van persoonsgegevens vast te stellen, alsmede de doelen voor het gebruik van persoonsgegevens. Verder moet het mogelijk zijn om de vestigingsplaats en de identiteit van de verantwoordelijke voor de verwerking vast te stellen.

- *Verantwoordelijkheid (accountability principle)*

Deze bepaling stelt dat de verantwoordelijkheid voor de verwerking van gegevens ligt bij de persoon of organisatie die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Deze zogenoemde 'verantwoordelijke' moet er zorg voor dragen dat de verwerking in overeenstemming is met de wet.

- *Rechten van de betrokkenen*

Degene op wie de verwerking van gegevens betrekking heeft wordt de betrokkene genoemd. Deze betrokkene heeft een aantal rechten vanuit de wet, zoals een recht op inzage en een recht op correctie.

5.5.2 De telecommunicatiewet (hoofdstuk 11)

Om de privacy in de elektronische communicatiesector te beschermen is in 2002 door het Europees Parlement en de Raad Richtlijn 2002/58/EG aangenomen (richtlijn betreffende privacy en elektronische communicatie). Richtlijn 2002/58/EG is de opvolger 28 van Richtlijn 97/66/EG welke hetzelfde beoogde als de huidige richtlijn. Richtlijn 2002/58/EG is in mei 2004 in hoofdstuk 11 van de Telecommunicatiewet (TW) geïmplementeerd. Met het oog op de bescherming van de privacy is daarom met name hoofdstuk 11 van de Telecommunicatiewet van belang. Tot de inhoud van hoofdstuk 11 TW behoren onder andere de regelingen met betrekking tot verkeers- en locatiegegevens en het 'spam verbod'.

5.6 Tussenconclusie

Een aantal van de doelstellingen van het consumentenrecht wordt door middel van het gegevensbeschermingsrecht (en in mindere mate het telecommunicatierecht) gerealiseerd. Het gaat dan met name om het zorgen voor economische gelijkwaardigheid tussen consumenten en bedrijven (doelstelling 3), het beschermen tegen hinder en overlast (doelstelling 4) en het beschermen tegen criminele gedragingen (doelstelling 5).

Om deze doelstellingen te realiseren hanteert het gegevensbeschermingsrecht de volgende uitgangspunten en mechanismen: 1) limitering van het verzamelen van gegevens, 2) doelbinding en de daarbij behorende beperkingen van gebruik, 3) eisen omtrent de kwaliteit van gegevens, 4) eisen omtrent de beveiliging van gegevens en 5) openheid omtrent het verwerken van gegevens.

Ambient intelligence technologie zal een fundamentele invloed hebben op het leven van mensen en hun positie als consument. Daarom is ook een fundamentele discussie omtrent de uitgangspunten en mechanismen voor de bescherming van persoonsgegevens noodzakelijk. Met het oog op het vertrouwen in ambient intelligence is het met name noodzakelijk om te analyseren hoe de komst van ambient intelligence de verwerking van persoonsgegevens gaat beïnvloeden en welke gevolgen dit heeft voor het waarborgen van de uitgangspunten van het gegevensbeschermingsrecht. In dit kader is het met name van belang te kijken hoe de technologie het recht beïnvloedt en hoe het recht de technologie zou moeten beïnvloeden. Hierbij moet eenzelfde (of indien mogelijk hoger) niveau van bescherming van de consument uitgangspunt zijn.

6 Persoonsgegevens en consumentenbescherming in ambient intelligence

6.1 Algemeen

Technologische ontwikkelingen voltrekken zich in een hoog, nagenoeg exponentieel, tempo. Zat tussen de ontwikkeling van de landbouw en de uitvinding van het wiel nog een periode van 4000 jaar, in onze huidige informatiemaatschappij zien wij dagelijks nieuwe uitvindingen. De invloed van technologie op onze maatschappij is aanzienlijk. Nieuwe technologieën, met name als zij een breuk met traditionele methoden vormen, roepen allerlei maatschappelijke vragen op en beïnvloeden de werking van ons rechtssysteem.

De technologische ontwikkelingen die zich momenteel voltrekken zullen binnen enkele jaren samenkomen in de ambient intelligence visie. Met het oog op het onderwerp van deze rapportage is de belangrijkste trend binnen deze toekomstvisie op de informatiemaatschappij de vergaande integratie van de fysieke wereld en de virtuele wereld (cyberspace) en de invloed die dit heeft op de verwerking van (persoons)gegevens.

Om het leven in de moderne informatiemaatschappij mogelijk te maken, worden in toenemende mate gegevens vastgelegd over communicatie, transacties en andere vormen van interactie. Zo moeten telecommunicatiebedrijven en ISP's verkeersgegevens registreren om het gebruik van telecommunicatiediensten in rekening te kunnen brengen en moeten webwinkeliers gegevens registreren om online verkopen mogelijk te maken.

Door het gebruik van identificatie,- en sensortechnologieën en het daaropvolgende vastleggen van gegevens, ontstaat er een steeds duidelijkere koppeling tussen de fysieke wereld en cyberspace. Dit heeft tot gevolg dat wanneer een persoon of een goed door de fysieke wereld beweegt, informatiesporen achtergelaten worden in cyberspace. Deze 'digitale voetstappen' kunnen met behulp van onder andere kunstmatige intelligentie technologieën eenvoudig worden verzameld, geanalyseerd en verder worden verwerkt.

6.2 Ambient intelligence en de bescherming van persoonsgegevens

Nieuwe technologieën kunnen een substantiële invloed hebben op economische, juridische en sociale verhoudingen binnen onze maatschappij. In deze paragraaf wordt de invloed van ambient intelligence op het beschermen van gegevens verkend. Specifiek wordt gekeken naar de rol van het gegevensbeschermingsrecht als middel om de consument te beschermen. In deze paragraaf wordt met name gekeken hoe de technologische ontwikkelingen op het gebied van ambient intelligence de bescherming van persoonsgegevens onder druk kan zetten.

6.2.1 Schaalvergroting

Omdat op steeds meer plaatsen identificatie- en sensortechnologie zal worden toegepast neemt het aantal punten waar gegevens kunnen worden verzameld steeds verder toe. Het voornaamste effect dat ambient intelligence dan ook zal hebben op de bescherming van persoonsgegevens is de toename van het aantal verwerkte gegevens.

Naast de hoeveelheid (persoons)gegevens die verwerkt worden, zal ook de context waarin gegevens worden verzameld steeds helderder worden. Dit is het gevolg van de toename in de verwerking van zogenaamde 'event data'. Het gaat hierbij om gegevens die gerelateerd zijn aan een bepaalde (fysieke) context. Als we een voorbeeld nemen uit het ambient intelligence scenario van hoofdstuk 2: wanneer Mark zijn AC tegen het OV-poortje op het station houdt wordt geregistreerd waar hij op welk tijdstip is. Al deze event data wordt bijgehouden in achterliggende databases.

De schaalvergroting die zal optreden door de komst van het ambient intelligence tijdperk heeft diverse gevolgen. Het voornaamste gevolg is dat de informatie die kan worden verkregen over personen completer wordt. Een ander effect is dat het gegevensbeschermingsrecht op steeds meer plaatsen ingezet zal moeten worden, om de simpele reden dat er op meer plaatsen gegevens worden verwerkt.

6.2.2 Profiling en personalisatie

Naarmate meer gegevens over personen beschikbaar komen, wordt het steeds beter mogelijk om uitgebreide profielen over deze personen op te stellen. Deze profielen kunnen voor diverse doeleinden worden gebruikt. Wanneer we kijken naar de verhouding tussen consumenten en het bedrijfsleven zien we dat bedrijven primair geïnteresseerd zijn in het opstellen van profielen om een beter inzicht te krijgen in hun klanten.

Hoe meer bedrijven weten van consumenten hoe beter zij hun aanbod kunnen toespitsen op de consument en hoe beter zij in staat zijn het gedrag van de consument te voorspellen of zelfs te sturen. Om deze reden zijn (persoons)gegevens van grote waarde voor bedrijven.

Hoewel accurate klantprofielen voordelen kunnen opleveren voor de consument (zoals een verbeterde service en lagere prijzen), kunnen zij ook diens economische positie nadelig beïnvloeden. Een voorbeeld hiervan is prijsdifferentiatie: wanneer een bedrijf weet uit het profiel van een consument dat deze zeer geneigd is om een bepaald type product te kopen, dan kan de verkoper de prijs van dit product voor de consument iets lager (of hoger) maken dan voor andere consumenten.

Een ander mogelijk nadelig gevolg van de toename in de profilering van consumenten is de zogenoemde 'panoptische schifting' (Marx 1985). Door uitgebreide profielen zijn consumenten via het proces van identificatie, beoordeling en classificatie steeds beter in te delen in economische of maatschappelijke klassen. Dit maakt het insluiten of juist uitsluiten van consumenten voor bepaalde goederen of diensten mogelijk.

6.2.3 Gebrek aan transparantie

Een van de uitgangspunten van de Wet bescherming persoonsgegevens is dat de verwerking van persoonsgegevens transparant moet zijn voor de betrokkenen. Met andere woorden, het moet voor de persoon wiens gegevens worden verwerkt duidelijk zijn wie zijn gegevens verwerkt en met welk doel dit gebeurt.

Het is momenteel al nagenoeg onmogelijk voor een consument te beoordelen waar, wanneer en waarom zijn persoonsgegevens worden verwerkt. Het ambient intelligence tijdperk zal deze situatie niet verbeteren. Deze ontwikkeling is inherent aan de achterliggende gedachte bij ambient intelligence. Om de interactie met de intelligente omgeving zo prettig mogelijk te maken is het expliciet een designdoel van ambient intelligence dat de computer naar de achtergrond van ons leven verdwijnt. De omgeving moet intelligent genoeg zijn om op ons te reageren en met ons te interacteren, maar gebruiksvriendelijk en onopvallend genoeg om niet op de voorgrond te treden. Daarom moet de technologische infrastructuur van de ambient intelligence omgeving haast per definitie onopvallend of onzichtbaar zijn voor de gebruiker. Daarnaast moet de werking van de omgeving voor de gebruiker een 'blackbox' zijn: de omgeving moet de gebruiker immers enkel tot dienst zijn.

Hoewel deze eigenschappen bijdragen aan een eenvoudige, intuïtieve, en prettige gebruikerservaring hebben zij ook tot gevolg dat het voor de gebruiker steeds minder duidelijk wordt waar, wanneer en waarom (persoons)gegevens worden verwerkt en wie daarvoor verantwoordelijk is.

Dit gebrek aan transparantie voor de consument heeft als belangrijkste nadeel dat deze de controle over zijn gegevens (nog verder) kwijtraakt. Het risico van deze ontwikkeling is een toenemende 'informatie-ongelijkheid' tussen consumenten en de gebruikers en beheerders van de ambient intelligence infrastructuur. Ook wordt het voor consumenten steeds moeilijker om fouten in hun gegevensverwerking op te sporen en te herstellen.

Daarnaast ondermijnt het verlies aan controle over de eigen gegevensverwerking het vertrouwen in ambient intelligence technologie en in de organisaties die gebruik maken van de ambient intelligence infrastructuur.

6.2.4 Systeemdwang en keuzevrijheid

Een achterliggend idee bij ambient intelligence is dat het alomtegenwoordig ('ubiquitous') en 'always on' is. Door de alomtegenwoordigheid en het 'always on' karakter van de ambient intelligence infrastructuur zal het moeilijk tot onmogelijk worden voor personen om zich te ontrekken aan deze infrastructuur. Daarnaast zal voor veel handelingen en transacties in de ambient intelligente wereld de verwerking van persoonsgegevens noodzakelijk zijn.
Dit kan tot gevolg hebben dat burgers onderworpen worden aan gegevensverwerkingen waar zij weinig tot geen invloed op uit kunnen oefenen. De technologie 'dwingt' burgers aldus om gegevens prijs te geven. Wanneer het systeem 'eist' dat er persoonsgegevens worden verwerkt (omdat het systeem zonder deze gegevens weigert te werken) dan is er sprake van een systeemdwang.[13]

De vraag is in hoeverre de keuzevrijheid van de consument om te beslissen al dan niet zijn

gegevens prijs te geven dan nog bestaat. Maar zelfs als het systeem de consument niet direct dwingt, kan er sprake zijn van systeemdwang. Wanneer het alternatief voor het niet verwerken van gegevens dusdanig onvriendelijk is, of duurder, is er sprake van 'zachte' systeemdwang.

In dit kader speelt ook de discussie rondom opt-in (vrijwillige deelname aan een systeem na expliciete toestemming) en opt-out (impliciete toestemming, slechts weigering na expliciete mededeling) een voorname rol.

6.2.5 Sfeerovergang

Een belangrijk effect van de voortschrijdende ontwikkeling van informatietechnologie is dat het 'sfeerovergang' vergemakkelijkt (function creep).

In ons leven begeven wij ons in diverse 'sferen'. Voorbeelden zijn de familiesfeer, de werksfeer, de medische sfeer, de religieuze sfeer en de economische sfeer. Binnen deze diverse sferen vervullen we bepaalde rollen, interacteren wij met bepaalde personen en instanties en geven wij informatie aan deze personen en instanties prijs. Wat we binnen de ene sfeer wel vrijwillig prijsgeven, willen we in een andere sfeer soms liever niet prijsgeven. Binnen diverse sferen hanteren we dus allerlei 'deelidentiteiten'.

Voor de komst van de informatiemaatschappij konden we redelijk ongestoord onszelf zijn en informatie prijsgeven binnen één bepaalde sfeer omdat deze verschillende sferen min of meer van elkaar gescheiden bleven. Wat zich binnen de gezinssfeer afspeelde kwam bijvoorbeeld zonder ons medeweten of toedoen niet in de werksfeer terecht. Door informatietechnologie wordt echter steeds meer informatie permanent vastgelegd. Omdat digitale informatie zo makkelijk te verveelvoudigen en te verspreiden is, ontstaat het risico dat informatie die in een bepaalde sfeer (vrijwillig) openbaar is gemaakt, ook in een andere sfeer bekend wordt. David Lyon (2001) spreekt in dit kader ook wel over 'lekkende containers'. Wat informatietechnologie dus mogelijk maakt, is dat deze op zichzelf staande, autonome sferen steeds verder in elkaar overlopen en vervagen omdat informatie makkelijk van de ene sfeer naar de andere sfeer vloeit.

Zo delen wij bijvoorbeeld graag informatie omtrent onze gezondheid met een arts, maar willen wij niet altijd dat deze informatie bekend wordt in onze vriendenkring en willen wij al helemaal niet dat deze informatie zich een weg vindt naar de economische sfeer waar het gebruikt kan worden door bedrijven of onze werkgever.

De verwachting is dat (ongewilde) sfeerovergangen sterker worden naarmate de middelen om informatie vast te leggen beter en alomvattender worden. Met de komst van de ambient intelligente wereld zal het dus nog moeilijker worden om de diverse autonome sferen te scheiden.

6.2.6 Misbruik van ambient intelligence

Nog meer dan nu zal ICT in de nabije toekomst een centrale plaats in ons leven innemen. Dit heeft onherroepelijk tot gevolg dat naarmate de ambient intelligence visie meer gestalte krijgt, er een toename zal zijn in de verwerking van (persoons)gegevens. Ook ligt het in de lijn der verwachting dat het belang van deze gegevensverwerkingen groter wordt en dat onze afhankelijkheid ervan toeneemt. Dit maakt dat misbruik van de ambient intelligence infrastructuur en dienstverlening interessant(er) wordt voor criminelen of anderszins kwaadwillenden.

6.3 Tussenconclusie

De algemene indruk uit dit hoofdstuk is dat naarmate de ambient intelligence visie completer wordt, de verwerking van (persoons)gegevens omvangrijker en belangrijker wordt. Dit heeft zijn weerslag op de bescherming van consumenten. Hoewel de komst van het ambient intelligence tijdperk ontegenzeggelijk voordelen heeft voor de consument, kunnen de in dit hoofdstuk genoemde risico's negatieve gevolgen hebben voor hem. Zo kunnen als gevolg van profiling, systeemdwang, en sfeerovergangen de belangen die het juridisch kader tracht te beschermen aangetast worden. De vraag is in hoeverre het juridisch kader in de toekomst weerstand kan bieden aan de in dit hoofdstuk genoemde risico's. Deze analyse vormt het onderwerp van het volgende hoofdstuk.

13 Systeemdwang kan ook betekenen dat de burger door het systeem gedwongen wordt om een bepaalde handeling te verrichten omdat het systeem mogelijke alternatieven uitsluit.

7 Juridisch kader in het licht van ambient intelligence

In het voorgaande hoofdstuk hebben we gezien dat de ontwikkeling van ambient intelligence de belangen kan aantasten die het juridisch kader voor de bescherming van persoonsgegevens tracht te beschermen. Gegeven het feit dat de principes en mechanismen die ten grondslag liggen aan het huidige juridische kader voor de bescherming van persoonsgegevens zijn opgesteld in het databasetijdperk (grofweg de jaren zestig/zeventig van de vorige eeuw), is het noodzakelijk om te kijken in hoeverre technologische ontwikkelingen deze grondslagen en mechanismen beïnvloeden.

7.1 Uitgangspunten: een adequate basis

Wanneer we de uitgangspunten van het huidige gegevensbeschermingsrecht (zoals transparantie, doelbinding enzovoorts) in ogenschouw nemen, kan geconcludeerd worden dat deze uitgangspunten technologie onafhankelijk geformuleerd zijn. De uitgangspunten die voortvloeien uit de *OECD Guidelines on Privacy* en *Fair Information Practice Principles* lijken de toets der tijd goed te doorstaan. Zowel de Europese Commissie als de European Data Protection Supervisor zijn eenzelfde mening toegedaan.[14]

De grootste uitdaging voor de wetgever zit hem in de balans tussen technologie-onafhankelijkheid van de wet en de concrete toepasbaarheid ervan. De wetgever ontkomt er vaak niet aan om voor de duidelijkheid van de wettelijke bepalingen aan te sluiten bij de heersende stand van de techniek. Technologieafhankelijkheid vergroot in dit geval de rechtszekerheid (hoe concreter de bepalingen, hoe beter deze te begrijpen zijn). Anderzijds neemt de rechtszekerheid af door technologieafhankelijke wetgeving, omdat elke verandering in de technologie tot gevolg heeft dat de wet aangepast moet worden.[15] Met het oog op de rechtszekerheid is het dus zaak een balans te vinden tussen technologie onafhankelijkheid en concrete toepasbaarheid.

Mogelijke knelpunten voor de toekomst bevinden zich in dit spanningsveld. De knelpunten zullen dan ook niet zozeer liggen in de uitgangspunten van het gegevensbeschermingsrecht, maar eerder in de concrete invulling van deze uitgangspunten. Hierbij speelt allereerst de vraag hoe de binnen het juridisch kader gekozen mechanismen (met name het begrippenkader en de invulling van de plichten die voortvloeien uit het juridisch kader) zich in de toekomst houden. Ten tweede speelt de vraag hoe de technologie zich naar de uitgangspunten van het gegegevensbeschermingsrecht kan en moet schikken.

7.2 Mogelijke knelpunten richting de toekomst

Hoewel de wetgever waar mogelijk technologieneutrale wetgeving opstelt, hebben de snelle technologische ontwikkelingen hun weerslag op de houdbaarheid van het juridisch kader. In deze paragraaf wordt geanalyseerd welke knelpunten het juridisch kader voor de bescherming van persoonsgegevens in de toekomst mogelijk tegen gaat komen.

7.2.1 Begrippenkader

Een mogelijk toekomstig knelpunt bij de bescherming van persoonsgegevens betreft het begrippenkader van de Wet bescherming persoonsgegevens, de Telecommunicatiewet en aanverwante wetten. Diverse auteurs geven aan dat begrippen uit de Wet bescherming persoonsgegevens zoals 'verantwoordelijke', 'bestand' en 'persoonsgegeven' nu al in de praktijk voor problemen zorgen (Zwenne *et al.* 2007, p. 62). Het valt te verwachten dat deze problematiek in het ambient intelligence tijdperk verder zal toenemen. Met name de definitie en de reikwijdte van het begrip 'persoonsgegeven' is omstreden.

Definitie persoonsgegeven
Zoals gezegd zijn de principes, mechanismen en begrippen die ten grondslag liggen aan het huidig juridisch kader opgesteld in het databasetijdperk. Databases zijn opgebouwd uit velden met daarin informatie. Wanneer in een database informatie staat die terug te voeren is op een identificeerbare natuurlijke

14 Zie hiervoor: *Mededeling van de Commissie aan het Europees Parlementen en de Raad over de de follow-up van het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming* (COM(2007)87, Brussel 7 maart 2007)) en *Advies van de Europese Toezichthouder voor gegevensbescherming inzake de mededeling van de Commissie aan het Europees Parlement en de Raad over de follow-up can het werkprogramma voor een betere toepassing van de richtlijn gegevensbescherming* (SN3750/07)

15 In het kader van privacy en de bescherming van persoonsgegevens kan bijvoorbeeld worden gewezen op de diverse wijzigingen in de Telecommunicatiewet.

persoon, dan is er sprake van persoonsgegevens. Echter, met de komst van het ambient intelligence tijdperk zien we dat de term 'persoonsgegeven' een steeds moeilijker hanteerbaar begrip wordt. Is een RFID-tag bijvoorbeeld per definitie een persoonsgegeven? Of is het slechts een persoonsgegeven wanneer in een achterliggende database NAW-gegevens aan deze tag te verbinden zijn? En, hoe zit het met de (verkeers)-gegevens die intelligente apparaten in hun communicatie met elkaar achterlaten?

De Artikel 29 Werkgroep heeft aangegeven dat gegevens iemand betreffen wanneer zij:

"verwijzen naar de identiteit, de kenmerken of het gedrag van een persoon of indien dergelijke informatie wordt gebruikt om de wijze waarop die persoon wordt behandeld of beoordeeld te bepalen of te beïnvloeden."[16]

Door de komst van ambient intelligence worden gegevens op meer plaatsen vastgelegd. Deze gegevens zullen in veel gevallen slechts indirect gerelateerd zijn aan een persoon. RFID-tags kunnen bijvoorbeeld volledig geanonimiseerd zijn (geen persoonsgegeven), maar wanneer via een bewakingscamera, gekoppeld aan een RFID-leesapparaat, te zien is wie de tag bij zich draagt, dan kan er alsnog sprake zijn van een persoonsgegeven. Dergelijke indirecte koppelingen en samenstellingen van verschillende soorten (anonieme) gegevens zullen in het ambient intelligence tijdperk steeds vaker voorkomen.

Afhankelijk van de ruimte die wordt genomen bij de interpretatie van het begrip persoonsgegeven, wordt de reikwijdte van de wet bepaald. De Artikel 29 Werkgroep heeft in een advies uit juni 2007 gepleit voor een ruime interpretatie van het begrip persoonsgegeven.[17] Dit heeft tot voordeel dat de meeste situaties waarin gegevens worden verwerkt onder het bereik van de Wbp worden gebracht en er dus geen 'witte vlekken' ontstaan in de rechtsbescherming van de betrokkenen. Keerzijde van de medaille is dat een groot aantal verwerkingen die geen invloed hebben op de positie van de consument (en dus ook niet aan de doelstellingen die worden nagestreefd met het gegevensbeschermingsrecht), wel onder het regime van de Wbp worden geplaatst. Dit betekent dat aan de diverse administratieve verplichtingen uit de wet moet worden voldaan, ook als dit niet noodzakelijkerwijs bijdraagt aan de bescherming van de consument.

Uiteindelijk gaat het dus om een antwoord op de vraag wanneer wordt aangenomen dat een gegeven naar iemand verwijst (met andere woorden: wanneer gegevens naar iemand herleidbaar zijn). Bij een ruime interpretatie van het begrip persoonsgegeven zal sneller worden aangenomen dat gegevens verwijzen naar een natuurlijk persoon. Voor veel gegevens zal in het ambient intelligence tijdperk moeilijk op voorhand vast te stellen zijn of het een persoonsgegeven betreft, of dat het dit in combinatie met andere gegevens kan worden.

Een aantal wetenschappers is van mening dat daarom het begrip persoonsgegeven in een groeiend aantal situaties niet meer zal aansluiten bij de technische en maatschappelijke werkelijkheid. De huidige trend is om op basis van allerlei soorten gegevens (persoonsgegevens, anonieme gegevens) een profiel over iemand samen te stellen. Naast het beschermen van de 'bouwstenen' (de persoonsgegevens) waarop een oordeel over iemands (deel)identiteit wordt gebaseerd, zal in toenemende mate aandacht moeten worden besteed aan de bescherming van deze (deel)identiteiten binnen een concrete context.

Terstegge (2005) spreekt daarom liever van 'digitale voetsporen'. Deze digitale voetsporen krijgen pas betekenis als zij gecombineerd worden en in een bepaalde context worden geplaatst. Als vervolgens misbruik van deze informatie wordt gemaakt, dan kan er ex-post op gereageerd worden via sancties. Daar zet hij tegenover dat er maatregelen moeten worden genomen om het vertrouwen in de technologie te verhogen, bijvoorbeeld door het aantal digitale voetsporen tot een minimum te beperken of de consument de technische mogelijkheid te geven om gebruik ervan te controleren (privacy by design). Prins (2004) ziet ook meer in de bescherming van identiteiten dan enkel in de bescherming van persoonsgegevens. Het is dus de vraag of het verwerken van 'persoonsgegevens' richting de toekomst nog wel het enige criterium moet zijn om te

16 Groep Gegevensbescherming Artikel 29 , *Werkdocument inzake problemen op het gebied van gegevensbescherming die verband houden met de RFID-technologie.* 19 januari 2005, WP 105 blz. 8.

17 Groep Gegevensbescherming Artikel 29, *Advies 4/2007 over het begrip persoonsgegeven.* 01248/07/NL WP 136

beslissen of het verwerken van gegevens al dan niet rechtmatig is. Vooralsnog biedt de wet geen duidelijke aanknopingspunten voor bescherming van gegevensverwerkingen die niet direct aan te merken zijn als het verwerken van persoonsgegevens.

Begrippenkader Telecommunicatiewet
Wanneer we kijken naar de Telecommunicatiewet zien we dat de structuur van de wet (en het bijbehorende begrippenapparaat) problematisch wordt richting de toekomst (Schermer 2004). De in de Telecommunicatiewet gebruikte definities met betrekking tot elektronische communicatienetwerken en -diensten zijn in belangrijke mate gebaseerd op de verhoudingen zoals die gelden in de telecommunicatiesector (vast, mobiel en internet). In deze sector is er over het algemeen sprake van een telecommunicatieaanbieder die een openbare telecommunicatiedienst aanbiedt welke afgenomen wordt door een gebruiker. Maar wanneer we kijken naar de inrichting van de ambient intelligence omgeving zien we dat de verhoudingen heel anders kunnen liggen. De inrichting van de ambient intelligence omgeving verschilt dusdanig van de inrichting van een (openbaar) elektronisch communicatienetwerk dat het bijna onmogelijk is om invulling te geven aan de bepalingen uit hoofdstuk 11 van de Telecommunicatiewet zonder een andere interpretatie van de begrippen uit die wet.

7.2.2 Verantwoordelijkheid voor de verwerking van gegevens

Een ander mogelijk knelpunt in het huidige juridische kader betreft de verantwoordelijkheid voor de verwerking van gegevens. Momenteel liggen de verhoudingen bij het verwerken van gegevens relatief eenvoudig: organisaties (bedrijven en overheden) verzamelen gegevens en zijn aldus 'verantwoordelijke' in de zin van de Wbp. Natuurlijke personen (met andere woorden burgers, consumenten, patiënten, werknemers) zijn 'betrokkene' in de zin van de Wbp. Echter in het ambient intelligence tijdperk zullen deze verhoudingen minder duidelijk komen te liggen. Door de alomtegenwoordigheid van ICT zal informatie makkelijker van organisatie naar organisatie vloeien. Ook zullen steeds meer partijen samenwerkingsverbanden aangaan, databases koppelen en/of 'managed services' aanbieden. Hierdoor wordt het steeds lastiger om de verantwoordelijke voor de (volledige) gegevensverwerking te definiëren.

Maar naast organisaties zullen consumenten zelf ook steeds meer informatie over elkaar verwerken. Neem het voorbeeld van de kledingkast in het ambient intelligence scenario uit hoofdstuk 2. In dit voorbeeld verschafte Mark de computer van de winkelier toegang tot de gegevensverzameling van zijn vrouw. In dit scenario wordt het lastig aan te geven wie de verantwoordelijke voor de gegevensverzameling is. Is dit Mark's vrouw Helena (het is haar kleding), is het Mark (hij verschaft de toegang), of is het de winkelier (die de data gebruikt)? Het antwoord op deze vraag is niet direct duidelijk. Eenzelfde ontwikkeling zien we online (Web 2.0). Door de vele verschillende participerende (content aanbieders, gebruikers) en faciliterende partijen (ISP's, Videosites, Fotosites, Social Networking sites, veilingsites) wordt het steeds minder duidelijk wie nu de verantwoordelijke in de zin van de Wbp is.

De hierboven gesignaleerde 'horizontalisering' van gegevensverwerkingen betekent een nieuwe uitdaging voor het mechanisme van de Wbp.

7.2.3 Systeemdwang en vrije keuze

Voor het verwerken van persoonsgegevens is een rechtmatige grondslag noodzakelijk. De wettelijke grondslagen voor de verwerking van persoonsgegevens zijn vastgelegd in artikel 8 van de Wbp. Eén van de grondslagen voor de verwerking van persoonsgegevens is de ondubbelzinnige toestemming van de betrokkene. Het is deze grondslag die in het kader van ambient intelligence steeds problematischer wordt.

De toestemming van de betrokkene moet gebaseerd zijn op een ondubbelzinnige, specifieke, uitdrukkelijke en vrije keuze. Het is de vraag in hoeverre deze in de toekomst nog te maken valt. Met betrekking tot de vrije keuze van de consument valt een aantal knelpunten te signaleren.

Een eerste knelpunt betreft het informeren van de consument. Voor het efficiënt functioneren van een ambient intelligente omgeving is de verwerking van gegevens veelal noodzakelijk. Deze gegevens worden verzameld via deels onzichtbare sensoren. Dit betekent dat op tal van punten gegevens, waaronder persoonsgegevens, verwerkt worden zonder dat dit direct voor de betrokkene duidelijk is. Echter, wil er sprake zijn van een ondubbel-

zinnige toestemming in de zin van de Wbp, dan moet de betrokkene over de noodzakelijke informatie beschikken om tot toestemmingsverlening te kunnen komen. De betrokkene dient daarom voldoende en begrijpelijk geïnformeerd te worden over de verschillende aspecten van de gegevensverwerking die voor hem van belang zijn (Artz 1999). Het is nog maar de vraag in hoeverre deze informatie ter beschikking kan worden gesteld in een omgeving waar *overal* gegevens worden verzameld en verwerkt.

Een tweede knelpunt betreft het bewust maken van een keuze over het toestaan van de verwerking. Wil er sprake zijn van toestemming in de zin van de Wbp, dan moet deze toestemming ondubbelzinnig zijn geuit door de betrokkene. Maar in een ambient intelligente omgeving zou dit betekenen dat de consument nagenoeg constant geconfronteerd zou worden met vragen over de verwerking van zijn gegevens, hetgeen indruist tegen de ambient intelligence visie en ook nog eens hinderlijk is voor de consument. Voorts is het de vraag of de consument kan overzien wat de potentiële gevolgen zijn van het geven van toestemming binnen een ambient intelligente omgeving (informed consent). Dwaling ligt op de loer.[18] Hoewel het informeren van de consument van cruciaal belang blijft voor diens rechtsbescherming, is het zaak te zoeken naar een mechanisme dat de consument afdoende informeert zonder dat dit afbreuk doet aan de gebruiksvriendelijkheid van de ambient intelligence infrastructuur.

Een derde knelpunt heeft betrekking op de daadwerkelijke vrijheid van de keuze van de consument met betrekking tot het al dan niet prijsgeven van persoonsgegevens. Wanneer door systeemdwang de keuze voor het prijsgeven van persoonsgegevens *de facto* niet meer vrij is (bijvoorbeeld omdat men dan niet meer met goed fatsoen van de dienstverlening gebruik kan maken), dan komt de grondslag voor de verwerking van de gegevens in feite op losse schroeven te staan.

Bij de aanleg van de ambient intelligence infrastructuur en het gebruik van ambient intelligence diensten moet dus, meer nog dan nu, een actieve afweging worden gemaakt tussen het belang van de verwerking van de gegevens en de gerechtvaardigde belangen van de betrokkene. De keuzevrijheid van de consument impliceert ook dat de consument de mogelijkheid moet hebben om zich te ontrekken aan de ambient intelligence infrastructuur. Als er effectieve mogelijkheden zijn voor de consument om zich aan de ambient intelligente infrastructuur te ontrekken of zijn interactie daarmee te controleren (consumer-in-control) dan zou uit het feit dat hij er geen gebruik van heeft gemaakt, kunnen worden afgeleid dat hij instemt met de verwerking van zijn gegevens (consent-by-participation).

7.2.4 Transparantie

De Wet bescherming persoonsgegevens heeft als uitgangspunt dat de verwerking van gegevens open en transparant moet zijn voor zowel de betrokkene als de toezichthouder. Op deze manier is er goede controle mogelijk op de verwerking van gegevens en de bij de keuze voor de manier van gegevensverwerking gemaakte belangenafweging. De wetgever legt de verantwoordelijke twee belangrijke *a priori* verplichtingen op met betrekking tot het verwerken van gegevens: de informatieplicht en de meldplicht. Deze plichten beogen de transparantie van de verwerkingen te vergroten, maar het is de vraag hoe deze plichten vervuld dienen te worden in een ambient intelligence tijdperk.

Informatieplichten

De verantwoordelijke dient voorafgaand aan de gegevensverwerking de betrokkenen te informeren over tenminste zijn identiteit en het doel van de verwerking. Het is waarschijnlijk dat door de komst van ambient intelligence deze informatieplicht moeilijker gestalte valt te geven. Het is immers moeilijk op alle plaatsen waar sensoren hangen aan te geven wat de verwerking inhoudt en wat voor doelstellingen hiermee worden nagestreefd. Het is dus de vraag of de informatieplichten in hun huidige vorm goed toepasbaar zijn in ambient intelligente omgeving (Zwenne *et al.*, 2007, p. 106). Hoewel als uitgangspunt het informeren van de consument dus van onverminderd belang is, moet richting het ambient intelligence tijdperk gezocht worden naar alternatieve methoden om de informatieplichten zo goed mogelijk in te vullen.

18 Op deze plek gaan wij niet in op de andere civielrechtelijke problemen die verbonden zijn aan toestemming zoals toestemming door minderjarigen, wilsgebreken en de juridische gevolgen van intrekking van de toestemming. Zie daarvoor: Terstegge 2002.

Meldingsplicht

Om de transparantie en controleerbaarheid van gegevensverwerkingen te vergroten bestaat er in Nederland een meldplicht met betrekking tot het verwerken van gegevens. Er is hierbij gekozen voor een 'genormeerde vrijstelling'. Dit betekent dat alle gegevensverwerkingen moeten worden aangemeld tenzij deze zijn vrijgesteld via het zogenoemde vrijstellingsbesluit. De Europese Commissie onderstreept het belang dat de meldplicht speelt bij het beschermen van de betrokkene.[19] Diverse stakeholders en wetenschappers hebben echter kritiek geuit op het systeem van de genormeerde vrijstelling omdat het niet de beoogde transparantie oplevert en daarnaast voor veel administratieve lasten zorgt.[20]

Wanneer we de genormeerde vrijstelling bekijken in het licht van de ambient intelligence visie, zien we dat er door een toenemend aantal verwerkingen ook een toenemend aantal meldingen zal zijn. Dit zullen in veel gevallen ook verwerkingen zijn die verder geen invloed hebben op de betrokkene. Zo kan het uitlezen van een RFID-tag met daarin persoonsgegevens worden aangemerkt als het verwerken van persoonsgegevens, ook wanneer er niks met deze gegevens wordt gedaan en de reader ze direct wist na het lezen. Desondanks zou in dergelijke gevallen melding moeten worden gemaakt of een vrijstelling moeten worden gecreëerd. Het lijkt richting de toekomst zinvol om te onderzoeken hoe het systeem van genormeerde vrijstellingen verbeterd kan worden, waarbij de rechtsbeschermende functie voor de betrokkene intact blijft, zonder dat dit tot onnodige administratieve lasten voor de aanbieders en gebruikers van de ambient intelligence infrastructuur leidt.

7.2.5 Globalisering

Wereldwijd bestaan er verschillende privacyregimes. Hoewel de Wbp een implementatie is van een Europese richtlijn, beperkt de Wbp zich qua bereik in principe tot Nederland. Knelpunten die als gevolg hiervan in de evaluatie van de Wbp worden gesignaleerd zijn dat op verantwoordelijken met vestigingen in meerdere lidstaten verschillende nationale privacywetten van toepassing zijn en de omstandigheid dat de Wbp enerzijds van toepassing kan zijn op verwerkingen die weinig verband houden met Nederland, terwijl anderzijds de wet niet van toepassing kan zijn op verwerkingen die wel specifiek verband houden met Nederland (Zwenne et al. 2007, p. 70). De Europese Commissie en de EDPS onderkennen deze problematiek en geven aan dat verdere harmonisatie van de verschillende Europese juridische kaders noodzakelijk is. Deze harmonisatie is mogelijk zonder dat hiervoor Richtlijn 95/46/EG op de schop hoeft.

Naast de Europese situatie, welke door harmonisatie van wetgeving sterk verbeterd kan worden, vormt ook de mondiale situatie een aandachtspunt. De globalisering van de wereldhandel, en daarmee ook de ICT-dienstverlening, zal in de komende jaren ongetwijfeld voortduren. De bovengenoemde knelpunten zullen daarom in het kader van ambient intelligence naar alle waarschijnlijkheid relevanter worden, zeker als organisaties hun dienstverlening verder 'internationaliseren'. Het is waarschijnlijk dat in het kader van ambient intelligence partijen 'managed services' aanbieden, waardoor gebruikers niet zelf een eigen IT infrastructuur hoeven aan te leggen en te onderhouden. Bij dergelijke managed services kunnen diverse processen ook in het buitenland worden ondergebracht, terwijl de dienstverlening in Nederland plaatsvindt. Hierdoor ontstaan jurisdictieproblemen en neemt het belang van uitgangspunten en mechanismen die wereldwijd gedeeld worden toe.

7.2.6 Veranderende verhoudingen

Wanneer we spreken over het verwerken van gegevens dan zien we dat dit momenteel primair geschiedt in de verhouding tussen een organisatie (bedrijf, overheid et cetera) en een individu (consument, patiënt, burger et cetera). Als zodanig is de inrichting van het gegevensbeschermingsrecht ook primair geënt op deze verhoudingen. Het valt echter te verwachten dat in toenemende mate persoonsgegevens verwerkt zullen worden door individuen. Hoewel deze situatie in principe door de wet gedekt wordt, is de vraag in hoeverre de praktische uitvoering van de wet met deze veranderende verhoudingen om zal kunnen gaan.

7.2.7 Handhaving

Handhaving van het gegevensbeschermingsrecht is cruciaal voor de rechtsbescherming van de betrokkenen. Echter, door de explosie-

19 COM(2007)87, Brussel 7 maart 2007
20 Zie voor een beknopt overzicht: Zwenne *et al.*, 2007, p. 82

ve stijging van het aantal verwerkingen in de laatste jaren, wordt een effectieve handhaving van de wet steeds lastiger. Door het toenemende belang van ICT in onze samenleving en het daarmee samenhangende groeiende aantal verwerkingen van persoonsgegevens wordt het werkterrein van de Wbp en de Telecommunicatiewet steeds verder uitgebreid. Hierdoor krijgt de Wbp het karakter van een omnibuswet: een wet die op steeds meer verschillende situaties van toepassing is. Omdat de wet op steeds meer situaties van toepassing is of wordt verklaard, groeit ook de noodzaak tot handhaving in deze situaties. In de rapportage aangaande de eerste fase van de evaluatie van de Wet bescherming persoonsgegevens worden (mede) als gevolg van deze ontwikkeling diverse knelpunten in de handhaving van het gegevensbeschermingsrecht gesignaleerd (Zwenne *et al*., 2007, p. 83). Onbekendheid met de wet en capaciteitsproblemen bij de handhaving komen hierbij als belangrijke knelpunten naar boven.

Een probleem in het huidige gegevensbeschermingsrecht is dat veel verantwoordelijken zich onvoldoende bewust zijn van de verplichtingen uit de Wbp en de rol van de toezichthouder bij de handhaving hiervan. Ditzelfde geldt voor de betrokkenen waarvan maar weinigen aangeven dat wanneer zij problemen hebben met de verwerkingen van hun persoonsgegevens zij zich tot de toezichthouder wenden. Dit kan er op duiden dat de zorgvuldige omgang met gegevens - enkel op basis van een wettelijke plicht - voor weinig verantwoordelijken een prioriteit vormt. Naarmate het aantal verwerkingen stijgt zullen deze problemen groter worden.

De handhaving van het gegevensbeschermingsrecht in Nederland ligt primair bij het College bescherming persoonsgegevens, een zelfstandig bestuursorgaan dat aangewezen is in de Wet bescherming persoonsgegevens als toezichthouder. Naarmate het aantal verwerkingen van persoonsgegevens stijgt, wordt ook de taak van het College bescherming persoonsgegevens omvangrijker. Hierdoor ontstaat het risico dat de opdracht van de wetgever aan de toezichthouder (een doelmatige en doeltreffende handhaving) op bepaalde punten niet meer naar volle omvang kan worden uitgevoerd.

7.3 Tussenconclusie

Wanneer we de uitgangspunten van het huidige juridisch kader voor de bescherming van persoonsgegevens tegen het licht houden, dan kunnen we constateren dat de principes van het gegevensbeschermingsrecht onverminderd van belang zijn in het ambient intelligence tijdperk. Sterker nog, het belang van de principes van het gegevensbeschermingsrecht zoals onder andere vastgelegd in de *Fair Information Practice Principles*, de *OECD Guidelines on Privacy* en onze eigen Wet bescherming persoonsgegevens, zullen met het oog op de mogelijke risico's voor de bescherming van persoonsgegevens, die ambient intelligence met zich mee kan brengen, alleen maar relevanter worden.

Op basis van de in dit hoofdstuk aangestipte knelpunten kan echter wel tentatief geconstateerd worden dat het gegevensbeschermingsrecht in haar huidige hoedanigheid in de toekomst niet langer optimaal de beoogde functies kan vervullen.

Hoewel de Wbp technologie-onafhankelijk tracht te zijn, zal in de toekomst de structuur en het begrippenkader alsmede het formele karakter van de wet veelal knellen met de technische en organisatorische werkelijkheid van het ambient intelligence tijdperk. De evaluatie van de Wbp komt tot een vergelijkbare conclusie (Zwenne *et al.* 2007, p. 175). Met andere woorden, hoewel de uitgangspunten van de wet hun waarde behouden, zullen een aantal van de in de wet gekozen mechanismen in de toekomst steeds minder toereikend zijn. Een soortgelijke conclusie kan getrokken worden voor de Telecommunicatiewet, omdat deze gebaseerd is op de huidige technologische en organisatorische verhoudingen binnen de telecommunicatiesector. Ook deze verhoudingen zullen als gevolg van het ambient intelligence tijdperk veranderen.

Tot op heden is het met name het recht op informationele privacy geweest dat werd ingeroepen om de bescherming van de consument gestalte te geven. Op basis van de conclusies uit dit hoofdstuk blijkt het huidige juridisch instrumentarium richting de toekomst niet in haar zelfstandigheid optimaal geschikt om de consument te beschermen. Aanpassingen aan het juridisch instrumentarium (en de implementatie daarvan), alsmede het complementair inzetten van andere (juridische) mechanismen, lijken in de toekomst onvermijdelijk.

8 Oplossingsrichtingen

In hoofdstuk 6 zijn een aantal risico's besproken die de ontwikkeling van ambient intelligence in het kader van gegevensverwerking mogelijk met zich meebrengt. In hoofdstuk 7 hebben we gezien dat het huidige juridisch kader voor de bescherming van persoonsgegevens op een aantal punten in de toekomst gaat knellen. Het valt het te betwijfelen of het juridisch kader (in de huidige vorm) zelfstandig weerstand kan bieden aan de risico's van ambient intelligence. Hoewel tot op heden het juridisch instrumentarium het primaire mechanisme is voor de bescherming van de consument, lijkt het er op dat richting de toekomst een breder instrumentarium ingezet dient te worden.[21] In dit hoofdstuk bespreken wij een aantal mogelijke oplossingsrichtingen.

8.1 Gebruiker in controle

Om de consument meer vertrouwen te geven in zijn slimme omgeving en de partijen die hem via deze omgeving diensten aanbieden, dient de consument middelen in handen te krijgen waarmee hij controle kan uitoefenen op de verwerking van zijn gegevens. Deze gedachte staat bekend als 'user-centric privacy' en 'gebruiker in controle'. Om de gebruiker meer controle te geven zijn een aantal middelen voorhanden die in deze paragraaf besproken worden.

8.1.1 Vergroten bewustzijn

Wil een gebruiker effectief controle kunnen uitoefenen over de slimme omgeving en het gebruik van zijn gegevens daarbinnen, dan moet hij zich allereerst bewust zijn van de manier waarop de omgeving werkt en welke rol de verwerking van gegevens daarbinnen speelt. Het voorlichten van de gebruiker over de mogelijkheden, onmogelijkheden en werking van ambient intelligence is hiervoor noodzakelijk. Deze voorlichting betreft een gedeelde verantwoordelijkheid van het bedrijfsleven, de overheid en consumentenorganisaties.

8.1.2 Informeren gebruiker

Juist omdat de ambient intelligence omgeving het mogelijk maakt om ongemerkt gegevens te verzamelen en te verwerken is het noodzakelijk dat de gebruiker geïnformeerd wordt over het feit dat zijn gegevens verwerkt worden. Dit kan onder andere door duidelijk te maken in de fysieke ruimte dat er systemen aanwezig zijn die gegevens verwerken. Een uniform systeem van logo's of merktekens lijkt hiervoor het meest geschikt. Echter zoals aangegeven in hoofdstuk 7, kent deze aanpak zijn beperkingen, omdat een visuele/fysieke melding niet altijd het meest geschikt of gebruiksvriendelijk is. Mogelijke oplossingsrichtingen liggen bijvoorbeeld in het delegeren van beslissingen omtrent informeren en accepteren aan de technologie zelf (bijvoorbeeld met behulp van intelligente software agenten). De consument zelf geeft in dit geval een bepaald profiel aan en de technologie zorgt voor de handhaving van de voorwaarden die in het profiel zijn gesteld. Zie voor een verdere bespreking van dit onderwerp paragraaf 8.2.

8.1.3 Voorkomen systeemdwang

Wil er daadwerkelijk sprake zijn van een gebruiker in controle, dan moeten de keuzes van de gebruiker vrij zijn. Wanneer de mogelijkheden van de gebruiker worden ingeperkt door de inrichting van het ICT-systeem, dan is er sprake van systeemdwang en is de keuze dus niét vrij. Aanbieders van ambient intelligence systemen moeten dus bij het design en de inrichting van de slimme omgeving rekening houden met dit gegeven en trachten systeemdwang zoveel mogelijk uit te sluiten.

8.1.4 Voorkomen vervreemding

Wanneer de inrichting en de werking van de ambient intelligence omgeving niet intuïtief, inzichtelijk, en gebruiksvriendelijk is voor de consument, dan kan dat het vertrouwen van de consument in de technologie zelf schaden. In het ergste geval kan de consument vervreemden van de technologie. Dit kan twee negatieve gevolgen hebben: de consument verzet zich tegen het gebruik van de technologie of de consument accepteert gelaten de technologie met het idee dat hij er toch geen invloed op kan uitoefenen. Om vervreemding te voorkomen is het ontwerp van goede, intuïtieve user interfaces die de consument het gevoel van controle geven van belang. Voorts is van belang dat de uit-

21 Zie onder andere COM(2007) 228, Brussel 2 mei 2007

komsten van het systeem voorspelbaar en consistent zijn. Dit is met name van belang voor adaptieve systemen die zich op basis van nieuwe informatie telkens aanpassen.

8.1.5 Versterken recht op inzage

De consument heeft vanuit het huidige gegevensbeschermingsrecht reeds het recht op inzage in de verwerking van zijn gegevens. In de praktijk blijkt dit recht op inzage echter grotendeels een wassen neus te zijn. Dit komt allereerst door de onbekendheid van de consument met de wet en de rechten die hier voor hem uit voortvloeien. Verder is de praktische invulling van het recht op inzage momenteel voor de gemiddelde consument te omslachtig, tijdrovend en te duur. Een oplossing zou wellicht liggen in een geautomatiseerd systeem van inzage in gegevensverwerkingen. Hoe een dergelijk systeem vormgegeven zou moeten worden is vooralsnog onduidelijk.

8.1.6 Vergemakkelijken mogelijkheden tot verhaal

Het idee van de gebruiker in controle impliceert niet alleen dat de gebruiker de toegang tot zijn gegevens kan ontzeggen of inzage moet krijgen in de verwerking van zijn gegevens, maar ook dat deze actiever kan optreden tegen mogelijke misstanden. In lijn met de doelstellingen van het consumentenrecht betekent dit dus het vergroten van de mogelijkheden tot adequate manieren van verhaal en geschillenbeslechting. Door meer nadruk te leggen op de mogelijkheden tot verhaal die de consument heeft via bijvoorbeeld het burgerlijk recht, kan de positie van de consument worden verstevigd. Daarbij mag de internationale dimensie niet uit het oog verloren worden.

8.2 Technologische regulering

Met betrekking tot de problemen in het auteursrecht stelde Charles Clark reeds in 1995: *"the answer to the machine is in the machine"* (Clark 1995). Met andere woorden, de uitdagingen waarvoor onze technologie ons stelt kunnen ook worden opgelost vanuit de technologie. Omdat de architectuur en inrichting van de technologie de mogelijkheden en de toepassing ervan dicteren, is de meest effectieve manier om (het gebruik van) technologie te reguleren, de technologie zelf. Dit is door Lessig (1999) kernachtig samengevat in de frase *"Code as Code"*. Met het oog op de bescherming van privacy en persoonsgegevens in relatie tot ambient intelligence gaat dit principe ook op.

8.2.1 Privacy by design

In het kader van ambient intelligence zijn er een aantal manieren om de technologie dusdanig te reguleren dat er minder risico's ontstaan voor de privacy van de consument. Het denken over het waarborgen van privacy via die technologie is te vangen onder de noemer 'privacy by design'.[22]

De achterliggende gedachte bij 'privacy by design' is dat reeds in de ontwerpfase van de technologie rekening moet worden gehouden met privacyvraagstukken. Het idee is dat de privacy beschermd wordt doordat het gebruik van gegevens waar mogelijk wordt afgeschermd, verminderd, of geëlimineerd. De uitgangspunten van het gegevensbeschermingsrecht worden daarvoor vertaald in de volgende ontwerpprincipes: *notice* (openheid en kennisgeving), *choice and consent* (keuzevrijheid en toestemming), *proximity and locality* (maximale afstand van verwerking), *anonimity and pseudonimity* (anonimiteit en pseudonimiteit), *security* (beveiliging) en *access and recourse* (recht op inzage en mogelijkheden tot verhaal) (Langheinrich 2001). Deze principes hebben niet alleen betrekking op het ontwerp van de technologie door aanbieders, maar ook op de uiteindelijke inrichting van het systeem door toepassers.

Openheid en kennisgeving
Gezien het feit dat - in tegenstelling tot de huidige stand van de technologie - het in de toekomst veel beter mogelijk wordt om ongemerkt informatie te verzamelen, moet er in de technologie een mogelijkheid tot kennisgeving worden ingebouwd. Dit betekent bijvoorbeeld dat wanneer de ambient intelligente omgeving voornemens is om informatie te verwerken over een persoon in deze ruimte, deze persoon hiervan op de hoogte gesteld wordt. In het geschetste ambient intelligence scenario zou dit bijvoorbeeld betekenen dat Mark een bericht krijgt op zijn AC wanneer een verwerking van zijn gege-

22 De auteur schaart de Privacy Enhancing Technologies ook onder de noemer Privacy by Design.

vens plaatsvindt of plaats gaat vinden. Een dergelijke kennisgeving is de 'virtuele tegenhanger' van een fysiek logo-systeem.

Keuzevrijheid en toestemming
In veel gevallen is de simpele kennisgeving dat een verwerking plaats gaat vinden niet genoeg, omdat de expliciete toestemming van de consument (de betrokkene) noodzakelijk is. In dergelijke gevallen moet het systeem de mogelijkheid bieden om aan deze toestemming uitdrukking te geven. In dit kader speelt ook de notie van systeemdwang een rol: wanneer een systeem door de inrichting geen vrije keuze laat aan de gebruiker, dan heeft het vragen om toestemming ook geen zin. Bij de bouw en inrichting van een systeem dient hier dus rekening mee te worden gehouden.

Anonimiteit en pseudonimiteit
Waar mogelijk moet een systeem mogelijkheden bieden voor anoniem gebruik. Een goed voorbeeld hiervan is de anonieme OV-chipkaart. Daarnaast moet, waar dit kan, het ook mogelijk worden gemaakt om via pseudoniemen (deelidentiteiten) gebruik te maken van het systeem. Anonieme en pseudonieme toegang tot de slimme omgeving moet niet nodeloos duurder of ingewikkelder zijn voor de consument.

Maximale afstand van verwerking
In de ambient intelligence omgeving zal veel informatie draadloos, over afstand, worden verwerkt. Door het bereik van RFID, sensoren en andere communicatiemiddelen te beperken tot de maximaal noodzakelijke afstand, kunnen veel onnodige privacyinbreuken worden voorkomen en risico's worden beperkt. Daarnaast geeft het vaststellen van een maximale afstand voor de verwerking van gegevens meer inhoud aan de vrije keuze en toestemming van de consument. In het ambient intelligence scenario bijvoorbeeld kan het 'aanraken' van de reclameposter worden opgevat als een vorm van toestemming.

Beveiliging
Het spreekt voor zich dat de adequate beveiliging van ICT-systemen een absolute noodzakelijkheid is voor de betrouwbaarheid ervan. In het kader van ambient intelligence zijn met name identificatie,-, authenticatie,- en autorisatiemechanismen van groot belang. Het voorbeeld uit de zorgsfeer zoals omschreven in het ambient intelligence scenario vormt hier een goed voorbeeld van.

Recht op inzage en mogelijkheden tot verhaal
Zoals eerder aangegeven in paragraaf 8.1 is het voor de notie van de gebruiker in controle noodzakelijk dat de consument invulling kan geven aan zijn recht op inzage en zijn mogelijkheden tot verhaal. Waar mogelijk dient hier bij het ontwerpen van systemen (met name databases) rekening te worden gehouden.

Privacy by design wordt inmiddels breed gedragen als een belangrijk mechanisme voor de bescherming van persoonsgegevens.[23] Tot op heden is het ontwerpen van producten en diensten via de privacy by design gedachte geen harde eis. Een mogelijkheid om ontwerpers, fabrikanten en gebruikers van het belang van privacy by design te doordringen is om het onderdeel te maken van de kwaliteitseisen die aan een product of dienst mogen worden gesteld.

8.2.2 'Privacy Aware Technologies'

Om nadere invulling te geven aan het concept van privacy by design en het idee van de gebruiker in controle is het van belang dat de technologie zich 'bewust' wordt van de privacyeisen van de gebruiker. Met andere woorden: de slimme omgeving moet weten wat de privacywensen en -eisen van de gebruiker zijn.

Een mogelijke benadering is dat de slimme omgeving voor elke verwerking van gegevens de gebruiker benadert en diens privacywensen inventariseert (en indien noodzakelijk toestemming vraagt). Een dergelijke benadering is echter niet bijzonder gebruiksvriendelijk, omdat de gebruiker in deze benadering nagenoeg constant geconfronteerd wordt met verzoeken en kennisgevingen.

Een praktischer benadering is de kennisgevingen en verzoeken tot het verwerken van gegevens over te laten aan een stuk technologie dat in dienst staat van de gebruiker. In het ambient intelligence scenario, zou dit de Ambient Communicator zijn.[24] De slimme

23 Zie onder andere: EU RFID Policy Outlook 2007 en Beugelsdijk 2007
24 In het kader van RFID technologie wordt reeds gewerkt aan een 'RFID guardian' die op basis van de privacyvoorkeuren van de gebruiker al dan niet toestaat dat RFID tags van de gebruiker worden uitgelezen (zie: http://www.rfidguardian.org)

omgeving richt zich tot de Ambient Communicator en deze beslist op basis van door de gebruiker vooraf gedefinieerde voorkeuren of profielen of de gegevens van de gebruiker al dan niet verwerkt mogen worden. Een voorbeeld van het gebruik is terug te vinden in het ambient intelligence scenario als Mark het winkelcentrum binnenloopt.

Om dit tweede concept haalbaar te maken, moeten de 'privacyvoorkeuren' van de gebruiker duidelijk zijn voor de technologie. Hiervoor is een ontologie van privacybegrippen nodig en een systematiek voor het beheren van (deel)identiteiten. Het Platform for Privacy Preferences (P3P) biedt een dergelijke ontologie reeds voor internetbrowsers.[25] Binnen het EU project PRIME wordt gewerkt aan identitymanagementsystemen die een soortgelijke functie moeten gaan vervullen, maar zich niet beperken tot internetbrowsers.[26]

Identitymanagementsystemen sluiten beter aan bij de contextgevoeligheid van het ambient intelligence tijdperk (afhankelijk van de context of de sfeer waarin de gebruiker zich bevindt mogen gegevens al dan niet verzameld/verwerkt worden). Daarnaast sluit het ook beter aan bij de beleving van de consument. Een identiteit of (deel)identiteit (werknemer, consument, patiënt, familielid) en het belang daarvan is een tastbaarder concept voor de consument dan een enkel persoonsgegeven.

8.3 Juridische regulering

Naast het idee van de gebruiker in controle en de technologische regulering van ambient intelligence, blijft de juridische regulering van ambient intelligence een belangrijke pijler voor de bescherming van de consument. In deze paragraaf worden aantal punten naar voren gebracht die het juridisch kader richting de toekomst moeten versterken.

8.3.1 Technologie onafhankelijkheid en rechtszekerheid

Uit de knelpunten gesignaleerd in hoofdstuk 7 blijkt dat het juridisch kader in de toekomst op bepaalde punten kan gaan wringen. Hoewel de uitgangspunten van het gegevensbeschermingsrecht relatief technologie-onafhankelijk zijn, zijn het begrippenkader en de daaraan gekoppelde structuur van de wet dit op bepaalde punten in mindere mate. Dit betekent dat het juridisch kader in de toekomst wellicht aanpassingen behoeft. Deze aanpassingen zullen niet zozeer van principiële aard zijn (de uitgangspunten van de Wbp doorstaan immers goed de toets der tijd), maar liggen veeleer in aanpassingen van de mechanismen die worden gebruikt om invulling te geven aan de uitgangspunten waarop de wet is gebaseerd. Zo is er bijvoorbeeld geen discussie omtrent het uitgangspunt van een transparante gegevensverwerking, maar wel omtrent het beste mechanisme om dit in te vullen (bijvoorbeeld via de meldplicht).

De kern van de discussie omtrent de houdbaarheid van het juridisch kader ligt in de technologie-onafhankelijkheid van de wetgeving en daarmee samenhangend het toepassingsbereik van de wetgeving. Het huidige gegevensbeschermingsrecht heeft zoals eerder geconstateerd het karakter van een 'omnibuswet'. Dit is grotendeels toe te schrijven aan de ruime interpretatie van de begrippen 'verwerken' en 'persoonsgegeven'. Voordeel van deze ruime interpretatie is dat de Wet bescherming persoonsgegevens relatief technologie-onafhankelijk is (immers nieuwe vormen van verwerken en nieuwe typen gegevens worden automatisch onder het bereik van de wet gebracht) en niet aan constante herziening onderworpen is. Dit komt de rechtsbescherming van de consument ten goede en verhoogt de rechtszekerheid. Aan de andere kant is dit ook direct een nadeel van de wet. Omdat de wet op zoveel situaties van toepassing is (ook in situaties waar de mechanismen van de wet niet optimaal werken), wordt het toepassingsbereik onduidelijker alsmede de voorwaarden waaronder de wet toegepast dient te worden. Deze onduidelijkheid ondergraaft de rechtszekerheid en brengt (administratieve) lasten mee voor de toepassers van ambient intelligence technologie. Er moet dus in de toekomst een balans worden gezocht tussen de houdbaarheid van de wet (deze moet niet constant aangepast te hoeven worden) en de werkbaarheid en concreetheid van de wet.

25 http://www.p3p.org. Gemeld dient te worden dat het P3P platform niet kan rekenen op substantiële steun van de browsermakers en om deze reden haar werk heeft gestaakt.
26 http://www.prime-project.eu

Een mogelijk aanknopingspunt voor de toekomst is het verleggen van de nadruk op de bescherming van losse persoonsgegevens naar de nadruk op het gebruik van gegevens binnen een bepaalde context. Op deze manier worden moeilijke discussies omtrent wat nu exact een persoonsgegeven is vermeden en wordt het gebruik van gegevens aan een specifieke context gerelateerd. Hierdoor kan er beter geconstateerd worden of er al dan niet een bedreiging is voor de privacy van consumenten en zo ja, wat deze bedreiging inhoudt. Deze verschuiving van persoonsgegevens naar het beheer van (deel)identiteiten die opgebouwd zijn uit tal van gegevens, kan een aanknopingspunt bieden voor een verdere discussie over de toekomst van de gegevensbescherming (Prins 2004, Terstegge 2005, Schermer 2007a).

8.3.2 Internationale focus

De toenemende globalisering vraagt om een internationale focus op de verwerking van gegevens. In Europees verband dienen met name procedurele belemmeringen weggenomen te worden (verschillende methoden voor meldingen van verwerkingen enzovoorts), terwijl op mondiaal niveau gestreefd zou moeten worden naar harmonisering van verschillende privacyregimes. Het ziet er echter sterk naar uit dat een 'privacyverdrag' op mondiaal niveau vooralsnog een brug te ver is. Het probleem van mondialisering van privacyvraagstukken is echter niet specifiek voor ambient intelligence en dient in een breder perspectief geadresseerd te worden.

8.3.3 Gedifferentieerd systeem van toezicht en handhaving

Zoals geconstateerd in hoofdstuk 7 is het onduidelijk of in de toekomst het misbruik van gegevens, of de onzorgvuldige omgang daarmee, in voldoende mate bestreden kan worden via alleen het gegevensbeschermingsrecht en het daarbij behorende handhavingsregime. Het feit dat de Wet bescherming persoonsgegevens een omnibuswet is, speelt hierbij een belangrijke rol. Zoals eerder aangegeven heeft het karakter van de Wbp als omnibuswet tot voordeel dat de consument in een zo groot mogelijk aantal situaties recht heeft op bescherming. Echter, het nadeel is dat deze bescherming door het karakter als omnibuswet vaak niet optimaal geboden wordt.

Deze constatering impliceert dat een bredere waaier aan beschermings- en handhavingsmechanismen nodig is. Deze beschermingsmechanismen kunnen juridisch van aard zijn (bijvoorbeeld handhaving via het strafrecht of het burgerlijk recht), technisch van aard (zie paragraaf 8.2) of organisatorisch (via met name zelfregulering). Met het oog op de inhoud van deze paragraaf wordt de nadruk gelegd op de differentiatie van juridische handhavingsmechanismen.

Het gegevensbeschermingsrecht in haar huidige vorm heeft een geschiedenis van grofweg veertig jaar. Met name door de opkomst van de computer en het internet heeft het een sterke groei meegemaakt en sterk aan belang gewonnen. Echter, door de explosieve groei van het aantal verwerkingen wordt handhaving steeds problematischer. Daarnaast veranderen ook de verhoudingen tussen verwerkende partijen. Waar vroeger de meeste privacyvraagstukken speelden in de verhouding bedrijfsleven-consument, zien we nu ook steeds vaker privacyvraagstukken tussen consumenten/burgers onderling. De vraag is daarom of niet, naast de handhavingsmechanismen uit het gegevensbeschermingsrecht (publiekrechtelijke handhaving via een toezichthouder), meer nadruk gelegd dient te worden op andere regulatieve instrumenten zoals het burgerlijk recht en het strafrecht.

Burgerlijk recht

In tegenstelling tot het gegevensbeschermingsrecht kent het burgerlijk recht een geschiedenis van meer dan 2000 jaar. In deze tijd bleek het burgerlijk recht wonderbaarlijk goed mee te kunnen met de voortschrijdende stand van de technologie. Het lijkt daarom logisch om naast het gegevensbeschermingsrecht beter aan te sluiten bij de juridische instrumenten uit het Burgerlijk Wetboek. Hierbij kan met name worden gedacht aan onrechtmatige daadsacties.

Bij de overgang van de Wet Persoonsregistraties naar de Wet bescherming persoonsgegevens is gekozen voor de voortzetting van publiekrechtelijke handhaving van het recht op (informationele) privacy. Echter naast deze publiekrechtelijke taak zou in de toekomst ook een aanvullende rol weggelegd kunnen zijn voor het burgerlijk recht. Dit biedt niet alleen een grotere flexibiliteit met betrekking tot de context van de gegevensverwerking, maar vergroot ook de mogelijk-

heden tot civielrechtelijke afdoening (Cuijpers 2004). Een dergelijke benadering kan ook bijdragen aan de bewustwording en de 'sense of urgency' bij verantwoordelijken (Cuijpers 2004, p. 378). De dreiging van bijvoorbeeld 'class action suits' van gedupeerde consumenten kan door bedrijven wel eens als groter worden ervaren dan die van een bestuurlijke boete of een strafrechtelijke sanctie. De gerichte protesten van consumenten tegen onder andere Benetton en Facebook en de reacties van de bedrijven hierop lijken deze conclusie te ondersteunen.[27]

Een argument dat tegen deze benadering pleit, is de moeilijkheid waarmee is vast te stellen wat de schade is die wordt geleden door het verkeerd gebruik of misbruik van persoonsgegevens. Daarnaast hebben grote organisaties over het algemeen een langere juridische adem dan de consument, hetgeen consumenten af kan schrikken bij het zoeken van verhaal.

Strafrecht

Het belang van informatie wordt in onze informatiesamenleving steeds groter. Ook de schade die kan ontstaan door misbruik van, of onzorgvuldige omgang met, gegevens wordt steeds groter. Onder andere Nouwt (2006) heeft daarom geopperd om het misbruik van gegevens in de toekomst in toenemende mate te sanctioneren via het strafrecht. Voor wat betreft delicten als fraude en oplichting, die worden gepleegd door het misbruiken van gegevens, kan reeds worden aangesloten bij de strafbepalingen uit het commune strafrecht.[28] Ook het overtreden van het spam-verbod van artikel 11.7 Telecommunicatiewet is reeds ondergebracht in het bijzonder strafrecht (Wet op de economische delicten). Nouwt pleit er echter voor om voor de handhaving van de bepalingen uit de Wet bescherming persoonsgegevens zelf, ook in toenemende mate het strafrecht te gebruiken. Niet alleen omdat het strafrecht potentieel zwaardere straffen mogelijk maakt, maar ook omdat het strafrecht volgens Nouwt als middel beter aansluit bij het belang van de bescherming van (persoons)gegevens. Met betrekking tot het toenemende belang van gegevensverwerkingen in het ambient intelligence tijdperk verdient deze overweging zeker nader onderzoek.

8.3.4 Zelfregulering

Naast de formele wetgeving op het gebied van privacy en consumentenbescherming dient ook zelfregulering blijvende aandacht te krijgen in de toekomst. Het belang van privacy en de bescherming van persoonsgegevens wordt voor bedrijven steeds evidenter. Niet alleen omdat het voor hen een wettelijke verplichting is, maar ook omdat zij in toenemende mate door hun klanten op de vingers worden getikt. Zoals eerder aangegeven zijn Benetton en Facebook hier goede voorbeelden van.

Mede gezien de sterke afhankelijkheid van context in een ambient intelligence omgeving kan het juridisch kader zonder nadere interpretatie nooit afdoende concrete houvast bieden. Via zelfregulerende initiatieven kan sectorale invulling worden gegeven aan de algemene en abstracte eisen uit de Wbp en recht worden gedaan aan het contextuele karakter van ambient intelligence.

8.3.5 Van bescherming persoonsgegevens naar identity management

In de ambient intelligence visie is de context bepalend voor de manier waarop de mens omgaat met zijn intelligente omgeving en de manier waarop de intelligente omgeving omgaat met de mens. Hoe meer gegevens ter beschikking staan aan de intelligente omgeving, hoe beter de omgeving in staat is om de gebruiker adequaat tot dienst te zijn. In de toekomst zal profilering en personalisatie dus steeds belangrijker worden. De consument zal steeds vaker op basis van zijn eigen identiteit (of een deelidentiteit) interacteren met maatschappelijke actoren (Prins 2004). Het beschermen (en afschermen) van deze (deel)identiteiten en het voorkomen van sfeerovergangen is de primaire uitdaging bin-

27 Zie onder andere: http://www.boycottbenetton.com/ ; http://www.wired.com/politics/security/commentary/securitymatters/2006/09/71815 en http://www.zdnet.be/news.cfm?id=76792

28 Hierbij dient met het oog op de toekomst nog wel onderzocht te worden in hoeverre het huidige commune strafrecht (met name de bepalingen rondom cybercrime) nog actueel en toereikend zijn. De vraag of in het commune strafrecht aanvullende bepalingen opgenomen dienen te worden die het misbruik van gegevens moeten sanctioneren verdient daarom nader onderzoek.

nen het ambient intelligence tijdperk. Meer nog dan het beschermen van de bouwstenen van iemands identiteit (de persoonsgegevens) zal gekeken moeten worden naar het gebruik en de interpretatie van de identiteit zelf. Op deze manier komen ook de belangen die aan het recht op (informationele) privacy ten grondslag liggen beter tot hun recht.

8.4 Opmaat voor discussie

De ontwikkeling van ambient intelligence is een fundamentele technologische ontwikkeling waarvan de eerste tekenen nu wereldwijd zichtbaar worden. De ontwikkeling van ambient intelligence gaat naar alle waarschijnlijkheid ook een fundamentele invloed hebben op de ontwikkeling van privacy en het gegevensbeschermingsrecht. Dit betekent dat richting de toekomst diverse mechanismen ingezet dienen te worden van technische, juridische en organisatorische aard. De uitwerking van concepten als gebruiker in controle en privacy by design moeten in de toekomst de bescherming van gegevens verstevigen.

Het is hierbij goed mogelijk dat bestaande juridische constructies en begrippen met het oog op veranderende technologische en maatschappelijke verhoudingen gewijzigd dienen te worden. Vooralsnog lijkt een aanpassing van de wet op dit moment niet nodig en niet zinvol, maar het is van belang om reeds in dit stadium een fundamentele discussie te voeren over de ontwikkeling van het gegevensbeschermingsrecht.

9 Conclusies

De ontwikkeling van nieuwe technologieën verloopt in een razendsnel tempo. Met name op het gebied van informatie- en communicatietechnologieën volgen de ontwikkelingen elkaar in sneltreinvaart op. Onze samenleving is in zo'n twintig tot dertig jaar verworden van een industriële samenleving tot een 'informatiemaatschappij' waarin technologieën zoals internet en de personal computer centraal staan. Echter, hier stoppen de technologische ontwikkelingen niet. Wij begeven ons inmiddels richting de volgende stap in de evolutie van onze informatiemaatschappij: ambient intelligence. In de ambient intelligence visie wordt de mens omringd door een onzichtbaar netwerk van intelligente computers, sensoren en andere ICT-middelen. Deze intelligente, onzichtbare ICT-infrastructuur is zich 'bewust' van de personen in de omgeving en kan anticiperen en reageren al naar gelang de wensen en de behoeften van de personen. De eerste tekenen van deze ontwikkeling zijn inmiddels zichtbaar in de vorm van RFID-toepassingen, intelligente camera's en sensornetwerken.

Hoewel de ambient intelligence visie ontegenzeggelijk veel voordelen zal hebben voor de consument, zal de ontwikkeling ervan ook onzekerheden en risico's opleveren. Wil de consument deze onzekerheden en risico's accepteren, dan moet hij een gerechtvaardigd vertrouwen hebben in de technologie en de partijen die van deze technologische infrastructuur gebruik maken. Door het nemen van bepaalde maatregelen kan de mate van risico en onzekerheid worden teruggebracht en het vertrouwen in de technologie worden vergroot. Het is belangrijk om een onderscheid te maken tussen 1) het vertrouwen in de technologie zelf (het systeem) en 2) het vertrouwen in de achterliggende actoren die de technologie aanbieden of gebruiken.

Wanneer wij de risico's van ambient intelligence inventariseren dan zien wij dat de risico's en onzekerheden primair gerelateerd zijn aan de uitwisseling van (persoonlijke) gegevens. De vraag die zich opdringt is de volgende:

Hoe kan de bescherming van gegevens over burgers/consumenten in een ambient intelligente wereld adequaat worden gewaarborgd terwijl tegelijkertijd de economische en maatschappelijke kansen van ambient intelligence worden benut?

9.1 De bescherming van persoonsgegevens

De eerste deelvraag uit dit rapport luidt:

Biedt het huidige instrumentarium voor de bescherming van persoonsgegevens genoeg handvatten voor een gerechtvaardigd vertrouwen in ambient intelligence?

De bescherming van persoonsgegevens krijgt op aantal manieren gestalte. Twee belangrijke elementen zijn: 1) de *technische* bescherming van gegevens (met andere woorden de beveiliging)[29] en 2) de *juridische* bescherming van gegevens.

Wanneer wij kijken naar de bescherming van persoonsgegevens dan zien wij dat het juridische kader (het recht op privacy) de boventoon voert in de discussies rondom ambient intelligence en consumentenvertrouwen. Met het recht op privacy, meer specifiek de bescherming van persoonsgegevens, worden diverse doelen nagestreefd, waarvan een aantal onder de bredere noemer van de consumentenbescherming kunnen worden geplaatst. Het gaat hoofdzakelijk om: 1) het zorgen voor economische gelijkwaardigheid tussen consumenten en bedrijven, 2) het beschermen van de consument tegen hinder en overlast en 3) het beschermen van de consument tegen criminele gedragingen.

Om deze doelstelllingen te realiseren hanteert het gegevensbeschermingsrecht de volgende uitgangspunten en mechanismen: 1) limitering van het verzamelen van gegevens, 2) doelbinding en de daarbij behorende beperkingen van gebruik, 3) eisen omtrent de kwaliteit van gegevens, 4) eisen omtrent de beveiliging van gegevens en 5) openheid omtrent het verwerken van gegevens.

Deze beginselen van het gegevensbeschermingsrecht lijken de toets der tijd goed te kunnen doorstaan. In samenhang met technische maatregelen moet het huidige instrumentarium voor de bescherming van persoonsgegevens dus voldoende aanknopingspunten bieden in de toekomst.

29 Een bespreking omtrent informatiebeveiliging in het kader van ambient intelligence vormt geen onderdeel van dit rapport.

De eerste deelvraag kan dus met een *ja* worden beantwoord. Het huidige instrumentarium biedt voldoende handvatten om tot een gerechtvaardigd vertrouwen in ambient intelligence te komen. Met name als ethisch-juridisch richtsnoer biedt het huidige instrumentarium voldoende handvatten voor de toekomst. De vraag is wel in hoeverre het juridisch instrumentarium in de toekomst doelmatig en doeltreffend blijft.

9.2 Gegevensbescherming in het licht van ambient intelligence

De tweede deelvraag uit dit rapport luidt als volgt:

Is het huidige juridische kader voor de bescherming van persoonsgegevens afdoende de toegerust om om te gaan met de gevolgen van ambient intelligence?

De ambient intelligence omgeving gaat naast veiligheid, gemak en efficiëntie ook nieuwe onzekerheden en risico's opleveren. Deze onzekerheden en risico's zijn primair gerelateerd aan de verwerking van (persoons)gegevens. Hierbij kan gedacht worden aan schaalvergroting, profilering en personalisatie, sfeerovergangen, systeemdwang en misbruik van de ambient intelligence infrastructuur.

Gezien het feit dat de geconstateerde risico's primair raken aan de bescherming van (persoons)gegevens wordt over het algemeen het recht op (informationele) privacy gezien als het instrument bij uitstek om deze risico's te beperken. Immers, hoe minder gegevens over een persoon bekend zijn, hoe minder risico's er kunnen ontstaan.

Het huidige juridische kader dat de informationele privacy waarborgt bestaat primair uit de Wet bescherming persoonsgegevens en de Telecommunicatiewet. In hoofdstuk 7 kwam naar voren dat deze wetten in de toekomst op een aantal punten gaan knellen. Mogelijke knelpunten vloeien voort uit de (onbewuste) techniekafhankelijkheid van de wet. De achterliggende reden is dat de Wet bescherming persoonsgegevens als impliciet uitgangspunt computers en databases neemt en de Telecommunicatiewet uitgaat van de huidige verhoudingen binnen de telecommunicatiesector. De vertrekpunten van de huidige wetgeving zullen met het oog op de toekomst in toenemende mate afwijken van de technische en organisatorische werkelijkheid. Mogelijke knelpunten richting de toekomst zijn 1) het huidige begrippenkader, 2) vragen omtrent de verantwoordelijke voor de verwerking van gegevens, 3) het moeilijk tegen kunnen gaan van systeemdwang en vrije keuze, 4) verminderde effectiviteit van de methoden om transparantie en openheid te garanderen, 5) onvoldoende aandacht voor de globalisering van de wereldhandel, 6) veranderende verhoudingen tussen bij gegevensverwerking betrokken partijen en 7) moeilijkheden met de handhaving van de wet.

Hoewel de uitgangspunten van het juridisch kader dus ook richting de toekomst relevant en adequaat zijn, moet wel geconcludeerd worden dat de juridische structuur en het begrippenkader op bepaalde punten waarschijnlijk gaat knellen. Dit geldt met name voor de mechanismen die invulling moeten geven aan de uitgangspunten van het gegevensbeschermingsrecht. Geconcludeerd kan worden dat het huidige juridische kader voor de bescherming van gegevens (de Wet bescherming persoonsgegevens en de Telecommunicatiewet) in de toekomst, zonder aanpassingen zelfstandig niet afdoende toegerust is om om te gaan met de veranderingen die ambient intelligence met zich mee zal brengen.

Het strekt tot aanbeveling om een brede, maatschappelijk gedragen discussie te voeren over de mogelijkheden om het gegevensbeschermingsrecht met het oog op de ontwikkeling van ambient intelligence te versterken. Hierbij moeten ook alternatieve technologische, organisatorische en juridische mechanismen (privacy by design, gebruiker in controle, zelfregulering en een gedifferentieerd systeem van handhaving), die flankerend aan het gegevensbeschermingsrecht aanvullende bescherming kunnen bieden, in ogenschouw worden genomen.

9.3 Aanvullende mechanismen

De laatste deelvraag uit dit rapport luidt:

Welke instrumenten kunnen in de toekomst bijdragen aan het vergroten van het vertrouwen in ambient intelligence?

Tot op heden ligt bij de bescherming van persoonsgegevens sterk de nadruk op het

juridisch kader en de handhaving daarvan door de toezichthouder. Hoewel dit ook in de toekomst een onmisbaar instrument blijft voor het waarborgen van de privacy en het vertrouwen van de consument, zal gezien technologische en organisatorische/ institutionele veranderingen die het ambient intelligence tijdperk teweeg brengt, het juridisch kader niet zelfstandig in staat blijken om de privacy en het vertrouwen van de consument te garanderen. Daarom moet gezocht worden naar alternatieve mechanismen die aanvullende bescherming kunnen bieden naast het juridisch kader.

Zonder in technologisch determinisme te willen vervallen kan voorzichtig geconcludeerd worden dat door de voortschrijdende ontwikkeling van ambient intelligence technologieën de privacy van de consument steeds moeilijker te handhaven zal zijn. Binnen deze technologische werkelijkheid moeten diverse mechanismen in gezamenlijkheid opereren om invullling te geven aan de bescherming van de consument in zijn algemeen en de bescherming van diens gegevens in het bijzonder.

In dit rapport zijn een tweetal aanvullende mechanismen besproken, te weten: het verbeteren van de controle die de gebruiker zelf heeft over zijn gegevens (gebruiker in controle) en regulering van het gebruik van gegevens door de technologie zelf (privacy by design).

Gebruiker in controle

De toenemende alomtegenwoordigheid, onzichtbaarheid en complexiteit van de technologie vergen een beter inzicht van de consument in de werking van de technologie en de mogelijke risico's die een onzorgvuldige omgang met gegevens met zich mee kan brengen. Een genuanceerde, kritische en bewuste houding van de consument ten opzichte van de verwerking van gegevens is een noodzakelijke voorwaarde voor de bescherming van persoonsgegevens. Via algemene voorlichting, gerichte informatieverstrekking op toepassingsniveau en met ondersteuning van technologische middelen moet de gebruiker zich meer bewust worden van zijn ambient intelligente omgeving. Alleen dan kan er op een realistische manier worden gesproken over de 'gebruiker in controle'.

Privacy by design

De meest effectieve regulering van de ambient intelligence omgeving is via de technologie zelf (Code as Code). Door nadruk te leggen op het belang van privacy by design (bijvoorbeeld via het stimuleren van onderzoek naar privacy enhancing technologies of door het onderdeel te maken van de productveiligheid) kunnen veel privacyrisico's worden vermeden.

Daarnaast kan privacy met instrumenten als privacy enhancing technologies, identitymanagement, en privacyfilters beter worden aangepast aan de concrete situatie waarin een consument zich bevindt. Op deze manier wordt privacy 'contextueler'. Dit sluit beter aan bij de beleving van de consument (welke afhankelijk is van de situatie) en heeft voor bedrijven als voordeel dat zij veel administratieve lasten kunnen voorkomen (bijvoorbeeld door het overbodig maken van verplichte meldingen).

10 Literatuurlijst

Aarts, E., Marzano, S. (2003), *The new everyday view on ambient intelligence*, Rotterdam: Uitgeverij 010

Artz, M. J. T. (1999), Koning Klant, het gebruik van klantgegevens voor marketingdoeleinden, *Achtergrondstudies en Verkenningen 14*, Den Haag: Registratiekamer

Berkvens, J.M.A. (2004). Ontvreemde privacy, in: *Rechtsgeleerd Magazijn Themis*, 2004, 5, 267-269.

Blok, P. (2002). *Het Recht op Privacy*, Boom Juridische Uitgevers.

Beugelsdijk, R. (2006). *RFID, veelbelovend of onverantwoord. Bijdrage aan de maatschappelijke discussie over RFID.* College bescherming persoonsgegevens, oktober 2006. Achtergrondstudies en Verkenningen 29

Clark C. (1995), The Answer to the Machine is in the Machine, in: P. Bernt Hugenholtz (ed.), *The Future of Copyright in a Digital Environment*, Den Haag: Kluwer Law International, p. 139

Cuijpers, C. (2004). *Privacyrecht of privaatrecht, een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn*. Den Haag: SDU Uitgevers.

Diamond, J. (1999). *Guns, Germs, and Steel: the Fates of Human Societies*, New York: W. W. Norton and Company

De Vries, P. (2004). *Trust in systems: Effects of direct and indirect information*. Universiteit Eindhoven

Etzioni, A. (1999). *The Limits of Privacy*, New York: Basic Books

Franken, H., Arnbak, J., Bovens, M.A.P., Donner, J.P.H, Gerritsma, A.M., Kummeling, H.R.B.M., Prins, J.E.J., de Ru, H.J., Snellen, I. Th. M., Vogelzang, P. (2000). *Rapport van de Commissie Grondrechten in het Digitale Tijdperk*. Rotterdam: Phoenix & Den Oudsten

Gutwirth, S. (1998). *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Amsterdam: Otto Cramwinckel Uitgevers

Haggerty, K. D., Ericson, R. V. (2000). The Surveillant Assemblage, in: *The British Journal of Sociology*, Vol. 51 Issue 4 605 December 2000, p. 605-622

Hof, C., van 't (2007), *RFID and identity management in everyday life*, Brussels: European Community

Hof, C., van 't, *et al.* (2007), RFID: helderheid over opsporing verzocht, Den Haag: Rathenau Instituut, (Bericht aan het parlement; oktober 2007)

Hof, C., van 't, Est, R., van (2007) RFID: meer keuze, gemak en controle in de digitale publieke ruimte, Den Haag: Rathenau Instituut

Hustinx, P. J. (2004). Bescherming van Persoonsgegevens op Koers, in: *Rechtsgeleerd Magazijn Themis*, 2004, 5

International Telecommunication Union (2005). *The Internet of Things*, ITU Reports 2005

Kurzweil, R. (2005). *The Singularity Is Near: When Humans Transcend Biology*, Viking Adult

Langheinrich, M. (2001). Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In: Gregory D. Abowd, Barry Brumitt, Steven A. Shafer (Eds.): *Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001).* LNCS No. 2201, Springer-Verlag, pp. 273-291, Atlanta 2001.

Lyon, D. (2001). *Surveillance Society, Monitoring everyday life*, Buckingham: Open University Press

Lyon, D. (2003a). *Surveillance as Social Sorting, Privacy, Risk and Digital Discrimination*, New York: Routledge

Lyon, D. (2003b). *Surveillance after September 11*, Cambridge: Polity Press

Ména, J. (2004). *Homeland Security: Techniques and Technologies*, Charles River Media: Hingham, MA

Nieuwenhuis, A.J. (2001). *Tussen privacy en persoonlijkheidsrecht, een grondrechtelijk en rechtsvergelijkend onderzoek*, Nijmegen: Ars Aequi Libri

Nouwt (2006). Tijd voor een nieuw punitief sluitstuk in de WBP, *Privacy & Informatie* 2005/6, pp. 253-258

OECD (1980), *Guidelines governing the protection of privacy and transborders flows of personal data*.

Prins, J. E. J. (2004). Technologie en de nieuwe dilemma's rond identificatie, anonimiteit en privacy, *Justitiële Verkenningen*, 2004-8, p. 34-47

Prins, J. E. J. (2007). Doeltreffend Privacytoezicht, in: *Nederlands Juristenblad*, nr. 28, p. 727

Schermer, B.W. (2007a), *Software Agents, Surveillance, and the Right to Privacy: a Legislative Framework for Agent-Enabled Surveillance*. Leiden: Leiden University Press (dissertatie)

Schermer, B. W. (2007b), *RFID en Mobility in Japan*, verslag studiereis Japan 2007, TWA Tokyo, Rathenau Instituut, RFID Platform Nederland.

Schuurman et al. (2007), *Ambient Intelligence: toekomst van de zorg of zorg van de toekomst?*, Den Haag: Rathenau Instituut, 2007 (Studie; 50)

Spivack, N. (2006). *The Third Generation Web is Coming*. www.kurzweilAI.net (laatste bezoek 20 maart 2007)

Terstegge, J. H. J. (2002), Wilt u hier even tekenen...? Betekenis van toestemming in het privacyrecht, in: *Privacy & Informatie*, nr.4, augustus 2002.

Terstegge, J. H. J. (2005), Toepassingen en toekomst van RFID, in G-J. Zwenne & B. Schermer (red.) *Privacy en andere juridische aspecten van RFID*, Den Haag 2005

Warren S. D., Brandeis L. D. (1890). The Right to Privacy: the Implicit Made Explicit, in: *Harvard Law Review*, p. 193-220.

United States Department of Health, Education, and Welfare (1973). *Secretary's Adisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens*.

Vedder, A. et al. (2007) *Van privacyparadijs tot controlestaat?*, Den Haag: Rathenau Instituut (Studie; 49)

Westin, A. F. (1967). *Privacy and Freedom*, New York: Atheneum Press

Wooldridge, M. (2002), *An Introduction to Multi-agent Systems*, West Sussex: John Wiley & Sons Ltd.

Wright, D. Gutwirth, S. Friedewald, M., Vildjiounaite, Punie, Y. (eds.) (2008), *Safeguards in a World of Ambient Intelligence*, Springer: The International Library of Ethics, Law and Technology

Zwenne G. J., Duthler A. W., Groothuis M., Kielman, H., Koelewijn W.,Mommers, L. (2007). *Eerste fase evaluatie Wet bescherming persoonsgegevens: Literatuuronderzoek en knelpuntenanalyse*, Leiden: Universiteit Leiden

e omslag =