<Computerrecht 2012/182>

<Artikelen>

Oprekking van het concept persoonsgegevens beperking van privacybescherming?

Colette Cuijpers en Paul Marcelis[1]

Uit een analyse van verschillende opinies van de Artikel 29-Werkgroep blijkt een steeds ruimere uitleg van het begrip persoonsgegevens. In dit artikel wordt vanuit twee perspectieven de vraag gesteld of een dergelijke ruime uitleg van het concept persoonsgegevens daadwerkelijk bijdraagt aan een betere bescherming van persoonsgegevens en privacy. In de eerste plaats vervaagt door een ruime uitleg de link tussen gegevensbescherming en privacy, wat vragen oproept omtrent het fundamentele karakter van het recht op gegevensbescherming en over de status van dit recht ten opzichte van het recht op privacy. In de tweede plaats is een ruime uitleg van het begrip persoonsgegevens praktisch moeilijk toe te passen, hetgeen geïllustreerd wordt aan de hand van voorbeelden betreffende het laagdrempelige gebruik van informatie beschikbaar op het internet. Dit artikel signaleert de problematiek van de steeds ruimere uitleg en is bedoeld als opmaat voor nader onderzoek naar oplossingen.

1. Inleiding

Sinds de inwerkingtreding van het Europese juridische kader betreffende persoonsgegevensverwerking zijn verschillende opinies verschenen van de Groep Gegevensbescherming Artikel 29 (Artikel 29-Werkgroep)[2] waarin het begrip

[1] Dr. C.M.K.C. Cuijpers is als senior onderzoeker verbonden aan TILT – Tilburg Institute for Law, Technology, and Society. Dhr. P. Marcelis volgt de research master van Tilburg University en is als junior onderzoeker verbonden aan TILT.

[2] Deze groep is opgericht op grond van art. 29 Richtlijn 95/46/EG. Het is een onafhankelijk Europees adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer, waarvan de taken zijn omschreven in art. 30 Richtlijn 95/46/EG en in art. 15 Richtlijn 2002/58/EG. Het secretariaat wordt verzorgd door directoraat C (Civiel recht, grondrechten en burgerschap) van het directoraat-generaal Justitie, vrijheid en veiligheid van de Europese Commissie, B-1049 Brussel, België, kamer LX-46 01/43. Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm. Alle in dit artikel vermelde internetbronnen zijn het laatst geraadpleegd op 20 juni 2012.

persoonsgegevens steeds ruimer wordt uitgelegd.[3] Hoewel deze ruime uitleg leidt tot een steeds breder toepassingsgebied, of dit ruime toepassingsgebied in ieder geval nadrukkelijk bevestigd, roept deze ruime uitleg vanuit twee perspectieven de vraag op of deze daadwerkelijk bijdraagt aan de bescherming van privacy. Enerzijds kan in dit verband gewezen worden op het conceptuele karakter van gegevensbescherming dat, mede door de oprekking van het concept persoonsgegevens, steeds verder afdwaalt van haar oorsprong, het recht op privacy. In de tweede plaats zet een steeds ruimere interpretatie van het concept persoonsgegevens de toepasselijkheid van het juridisch kader in de praktijk onder druk.

In dit artikel zal eerst een schets gegeven worden van het begrip persoonsgegevens. De wijze waarop de Artikel 29-Werkgroep het begrip persoonsgegevens uit Richtlijn 95/46/EG in meerdere opinies heeft uitgelegd, vormt hierbij het uitgangspunt. Uit deze analyse komt heel duidelijk een beeld naar voren dat steeds meer gegevens gevat kunnen worden onder het begrip persoonsgegevens. Door deze brede uitleg van het begrip persoonsgegevens vervaagt de link tussen de bescherming van persoonsgegevens en privacy. Dit roept vragen op omtrent het fundamentele karakter en de status van het recht op gegevensbescherming ten opzichte van het recht op privacy. Deze problematiek zal in de derde paragraaf nader worden besproken. In de vierde paragraaf zullen vraagtekens gezet worden bij de praktische toepasbaarheid van een steeds meer omvattend concept persoonsgegevens. Aan de hand van het voorbeeld van gebruik van informatie beschikbaar via sociale netwerksites zal de toepasselijkheid van een aantal kernconcepten uit de Wet bescherming persoonsgegevens ter discussie worden gesteld. Of het voorstel voor een nieuwe Verordening voor de bescherming van persoonsgegevens, welke naar verwachting in 2014 Richtlijn 95/46/EG zal vervangen, tegemoetkomt aan of verduidelijking geeft met betrekking tot de in paragraaf 3 en 4 gerezen punten wordt besproken in de vijfde paragraaf.

Het voorliggende artikel heeft niet als doel klip-en-klare antwoorden te geven met betrekking tot de beschreven problematiek. Dit vergt meer fundamenteel onderzoek. Het artikel is bedoeld als opmaat voor nader onderzoek naar de praktische toepasbaarheid van het EU juridisch kader betreffende privacy en gegevensbescherming op een specifiek terrein, datamining in open sources.[4] Aangezien bij dit vraagstuk de reikwijdte en interpretatie van het begrip persoonsgegevens een centrale rol speelt, zullen de inzichten van dit artikel in de conclusie bijdragen aan het scherp stellen van een onderzoeksagenda betreffende het gebruik van persoonsgegevens van en in open bronnen.

[3] Hoewel het juridisch kader meerdere Richtlijnen omvat richten wij ons op de algemene Richtlijn waarin het concept persoonsgegevens gedefinieerd is, Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. PbEG 1995, L 281/, 0031-0050.

[4] The work leading to this paper has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 242352 (VIRTUOSO).

2. De reikwijdte van het begrip persoonsgegeven

2.1 Inleiding

Sinds de inwerkingtreding van Richtlijn 95/46/EG zijn er vragen gerezen over de wijze waarop het begrip persoonsgegeven uitgelegd moet worden. Op 16 februari 2012 stond de reikwijdte van het concept persoonsgegevens nog centraal in een zaak voor de Rechtbank Amsterdam over gegevensverwerking in het kader van Google Maps en Google Street View.[5] In een andere recente zaak, 15 maart 2012, zijn door de Rechtbank Middelburg zelfs prejudiciële vragen gesteld over de strekking en de reikwijdte van het begrip persoonsgegevens.[6]

In Richtlijn 95/46/EG wordt het begrip in art. 2 (a) als volgt gedefinieerd:

"'persoonsgegevens', iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit".

Vooral de vraag wanneer iemand indirect geïdentificeerd kan worden roept vragen op. Zeker in een ´vernetwerkte´ informatiesamenleving,[7] waar de mogelijkheden om gegevens door middel van koppeling van verschillende databronnen te herleiden tot identificeerbare personen enorm zijn toegenomen.

2.2 Advies 4/2007 over het begrip persoonsgegeven

In 2007 heeft de Artikel 29-Werkgroep expliciet aandacht besteed aan de interpretatie van het concept persoonsgegevens.[8] In dit advies wijst de groep op enige onzekerheid bij de lidstaten over de toepassing van het begrip persoonsgegevens. Hier moet actie op ondernomen worden aangezien een van lidstaat tot lidstaat uiteenlopende toepassing van

[5] Rb. Amsterdam 16 februari 2012, nr. 506001/KG ZA 11-1962, *Computerrecht* 2012/122, m.nt. F. Van der Jagt.
[6] Rb. Middelburg 15 maart 2012, *LJN* BV8942, nr. 11/367. Inhoudelijk is deze zaak in het kader van deze bijdrage niet zo interessant. Het gaat in deze zaak om de vraag of een minuut bij een asielaanvraag persoonsgegevens betreft of dat het hier gaat om een juridische analyse. De criteria op grond waarvan het Hof van Justitie gaat beoordelen of er al dan niet sprake is van persoonsgegevens zijn wel interessant, maar daarvoor moeten we de uitspraak van het Hof afwachten.
[7] Een trend waar in het rapport *iOverheid* meerdere malen op gewezen wordt, WRR-rapport 86: *iOverheid*, Den Haag/Amsterdam: Amsterdam University Press 2011, o.a. p. 15, 33, 151.
[8] Groep Gegevensbescherming Artikel 29, Advies 4/2007 over het begrip persoonsgegeven, WP 136, 01248/07/NL, goedgekeurd op 20 juni 2007. Beschikbaar via: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_nl.pdf.

het begrip persoonsgegeven invloed kan hebben op het goed functioneren van gegevensbescherming in diverse contexten.[9] Daarom wordt beoogt richtsnoeren te geven voor de wijze waarop de nationale regelgeving voor gegevensbescherming moet worden toegepast.[10]

Het eerste punt waarop de Artikel 29-Werkgroep wijst is de keuze voor een brede definitie van het begrip persoonsgegeven waaraan in het gehele wetgevingsproces is vastgehouden.[11] In de tweede plaats wordt erop gewezen dat niet elke verwerking van persoonsgegevens binnen de reikwijdte van de Richtlijn valt. Bepaalde situaties vallen niet binnen de werkingssfeer van het Gemeenschapsrecht, of vallen buiten het bereik van de Richtlijn zoals de handmatige niet-gestructureerde verwerking van persoonsgegevens of verwerkingen in het kader van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden. Bij deze uitzonderingen kunnen echter drie belangrijke kanttekeningen worden geplaatst. In de eerste plaats is met het Verdrag van Lissabon de oorspronkelijke driepijlerstructuur vervallen waardoor de uitzondering betreffende de werkingssfeer van het Gemeenschapsrecht minder relevant geworden is.[12] Bovendien heeft het Hof bepaalt dat lidstaten de draagwijdte van de nationale wet ter implementatie van Richtlijn 95/46/EG uit mogen breiden tot niet binnen de werkingssfeer daarvan vallende gebieden, voor zover het gemeenschapsrecht hieraan niet in de weg staat.[13] In de tweede plaatse spelen handmatige niet gestructureerde verwerkingen van persoonsgegevens in de huidige informatiesamenleving nauwelijks een rol van betekenis. En in de derde plaats kan gewezen worden op de beperkte uitleg van het criterium '*uitsluitend persoonlijke of huishoudelijke doeleinden*', zeker in relatie tot het internet. In de zaak *Lindqvist* heeft het Hof van Justitie immers geoordeeld dat:

"Die uitzondering moet derhalve aldus worden uitgelegd, dat zij uitsluitend betrekking heeft op activiteiten die tot het persoonlijke of gezinsleven van particulieren behoren, hetgeen klaarblijkelijk niet het geval is met de verwerking van persoonsgegevens die bestaat in hun openbaarmaking op Internet waardoor die gegevens voor een onbepaald aantal personen toegankelijk worden gemaakt".[14]

De Artikel 29-Werkgroep bespreekt het concept persoonsgegevens aan de hand van de vier kernelementen uit de definitie, 'iedere informatie', 'betreffende', een 'geïdentificeerd of identificeerbaar', 'natuurlijke persoon'.[15] Identificeerbaarheid roept de meeste vragen op en is het meest relevant in het kader van dit artikel. De bespreking van de opinie is daarom beperkt tot dit kernelement.

[9] WP 136, p. 3.
[10] WP 136, p. 3.
[11] WP 136, p. 4.
[12] Zie uitgebreid over de wijzigingen die het Verdrag van Lissabon gebracht heeft R.H. Van Ooik & R.A. Wessel (red.), *De Europese Unie na het Verdrag van Lissabon*, Deventer: Kluwer 2009.
[13] Arrest van het HvJ 6 november 2003, nr. C-101/01, *Jur.* 2003, p. I-12971 (*Bodil Lindqvist*), r.o. 98.
[14] Bodil Lindqvist, r.o. 47.

2.2.1 Geïdentificeerd of identificeerbaar

Bij het kernelement *identificeren* gaat het om de vraag of een natuurlijke persoon van andere personen kan worden onderscheiden. Wanneer dit op het eerste gezicht niet mogelijk is met de beschikbare identificatiemiddelen, kan toch sprake zijn van 'identificeerbaarheid' doordat aan de hand van een combinatie met andere gegevens (die al dan niet bij de voor de verwerking verantwoordelijke berusten) de betrokkene van andere personen kan worden onderscheiden.[16]

In de conclusie bij het Advies 4/2007 stelt de Artikel 29-Werkgroep dat het bij 'geïdentificeerd of identificeerbaar' met name gaat om: '*de voorwaarden waarop een persoon als 'identificeerbaar' kan worden beschouwd*'. Hierbij wordt vooral gekeken naar de '*middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn*' en wordt gewezen op het belang van de specifieke context en omstandigheden van een geval die bij een analyse of sprake is van persoonsgegevens een belangrijke rol spelen.[17]

De Artikel 29-Werkgroep stelt dat een slechts hypothetische mogelijkheid om iemand te onderscheiden niet voldoende is om die persoon als 'identificeerbaar' te beschouwen. Echter, doordat overweging 26 aangeeft dat voor identificeerbaarheid in ogenschouw genomen worden: 'alle middelen waarvan mag worden aangenomen dat zij ***redelijkerwijs*** door degene die voor de verwerking verantwoordelijk is dan wel door ***enig ander persoon*** in te zetten zijn', lijkt met name door de toevoeging van *enig ander persoon* in zeer veel gevallen sprake te kunnen zijn van 'identificeerbaarheid'.

In bovenstaand citaat is het woord *redelijkerwijs* benadrukt om aan te geven dat dit een concept is dat zeer uiteenlopend beoordeeld kan worden. De nadruk op *enig ander persoon* is ingevoegd omdat dit de vraag oproept of sprake is van persoonsgegevens zodra *enig persoon* gegevens kan herleiden tot een individueel persoon. Dit is een erg brede lezing welke bijvoorbeeld geïllustreerd kan worden aan de hand van biometrische gegevens. Dergelijke gegevens zijn op een unieke wijze gekoppeld aan een specifieke persoon en kunnen dus bij uitstek gebruikt worden om een persoon te identificeren. Echter, het is maar een zeer beperkte groep mensen die daadwerkelijk een vingerafdruk aan een persoon kan linken, wat betreft kennis en vaardigheid, maar ook voor wat betreft geautoriseerde toegang tot databases waarin vingerafdruk en persoon aan elkaar gelinkt kunnen worden. Als wij nu, bijvoorbeeld ter illustratie bij een paper over biometrie, de vingerafdruk van enig persoon online plaatsen, is dit dan een persoonsgegeven omdat er mogelijk enig persoon is die deze vingerafdruk kan herleiden tot een identificeerbaar persoon?

---

[15] WP 136, p. 6.
[16] WP 136, p. 6.
[17] WP 136, p. 27.

Volgens de Artikel 29-Werkgroep moet bij identificatie rekening gehouden worden met alle relevante factoren zoals kosten van identificatie, het beoogde doel, de wijze waarop de verwerking is gestructureerd, het voordeel dat de voor de verwerking verantwoordelijke ervan verwacht, de belangen die voor de betrokken personen op het spel staan, het risico van organisatorische tekortkomingen (bijv. inbreuken op de vertrouwelijkheidsplicht) en technische storingen.[18] Bovendien moet er rekening gehouden worden met de stand van de technologie. Hierbij moet de duur van verwerking en opslag van gegevens in de beoordeling betrokken worden. Wat nu nog niet mogelijk is op het vlak van identificatie, is over vijf jaar technisch gezien wellicht dusdanig eenvoudig dat hoewel nu geen sprake is van persoonsgegevens, deze gegevens na verloop van tijd dit mogelijk wel worden. De Artikel 29-Werkgroep stelt dat het systeem zich moet kunnen aanpassen wanneer dergelijke ontwikkelingen zich voordoen en moet zorgen dat tijdig passende technische en organisatorische maatregelen worden genomen.[19]

2.3 Ruime uitleg bij onzekerheid

Hoewel de hierboven beschreven opinie dateert uit 2007, is de uitleg die gegeven is aan het concept persoonsgegevens door de jaren heen nauwelijks gewijzigd. De trend waarbij het concept persoonsgegevens wordt opgerekt tot die gegevens waarvan niet met zekerheid is vast te stellen of zij al dan niet herleidbaar zijn tot een identificeerbaar persoon, en dat dan *dus* uitgegaan moet worden van persoonsgegevens, wordt in latere opinies bevestigd. Deze redenering is in de eerste plaats gevolgd in relatie tot IP-adressen uitgegeven aan een internetcafé. In een dergelijke situatie is het voor internetdienstverleners niet altijd mogelijk om te weten of het IP-adres in kwestie identificatie mogelijk maakt. Hier is de conclusie aan verbonden dat de aan deze IP-adressen gekoppelde gegevens op dezelfde wijze behandeld moeten worden als informatie die gekoppeld is aan IP-adressen van geregistreerde en identificeerbare gebruikers. Dit tenzij de internetdienstverlener met absolute zekerheid gegevens van niet-identificeerbare gebruikers kan onderscheiden. Zo niet zal hij alle IP-informatie voor de zekerheid als persoonsgegevens moeten behandelen.[20]

In het voorbeeld over IP-adressen wordt uitdrukkelijk uitgegaan van identificeerbaarheid door internetaanbieders '*internetaanbieders en beheerders van lokale netwerken [kunnen] zonder veel moeite internetgebruikers identificeren aan wie ze IP-adressen hebben verstrekt*'.[21] In een voorbeeld over camerabewaking lijkt dit perspectief afgezwakt te worden. In die context wordt door verantwoordelijken vaak aangevoerd dat slechts voor een gering percentage van het verzamelde materiaal identificatie plaats zal vinden, en dat er dus

[18] WP 136, p. 16.
[19] WP 136, p. 6.
[20] WP 136, p. 18. Onder verwijzing naar het document 'Privacy on the Internet' – An integrated EU Approach to On-line Data Protection, WP 37. Beschikbaar via: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2000_en.htm.
[21] WP 136, p. 17.

vóór die identificatie, geen sprake is van verwerking van persoonsgegevens. Het doel van videobewaking is echter de identificatie van de personen die op de videobeelden te zien zijn, in alle gevallen dat de voor de verwerking verantwoordelijke dat nodig acht. Het hele proces moet dan ook worden beschouwd als de verwerking van gegevens over identificeerbare personen, ook als sommige personen in de praktijk niet identificeerbaar zijn.[22]

In een advies over gegevensbescherming en zoekmachines, heeft de Artikel 29-Werkgroep bevestigd dat IP-adressen, maar ook cookies, in de meeste gevallen als persoonsgegevens dienen te worden beschouwd:

"Wanneer een cookie een unieke gebruikersidentificatiecode bevat, vormt deze code duidelijk een persoonsgegeven. Door het gebruik van permanente cookies of soortgelijke middelen met een unieke gebruikersidentificatiecode kunnen gebruikers van een bepaalde computer zelfs worden getraceerd wanneer zij zich bedienen van dynamische IP adressen. Met de door deze middelen gegenereerde gedragsgegevens kunnen de persoonlijke kenmerken van de betrokkene nog specifieker in beeld worden gebracht."[23]

Een vergelijkbare redenering, waarbij de onmogelijkheid van het onderscheiden van identificerende en niet-identificerende gegevens moet leiden tot het aanmerken van alle gegevens als persoonsgegevens, kan gevonden worden in een meer recente opinie over geolocatiegegevens.[24] Hierin wordt met betrekking tot Wi-Fi-toegangspunten het volgende gesteld:

"The fact that in some cases the owner of the device currently cannot be identified without unreasonable effort, does not stand in the way of the general conclusion that the combination of a MAC address of a WiFi access point with its calculated location, should be treated as personal data. Under these circumstances and taking into account that it is unlikely that the data controller is able to distinguish between those cases where the owner of the WiFi access point is identifiable and those that he/she is not, the data controller should treat all data about WiFi routers as personal data".[25]

In deze opinie wijst de Artikel 29-Werkgroep zelf op de ontwikkeling dat gegeven het feit dat mensen steeds meer informatie vrijgeven via bijvoorbeeld sociale netwerksites, er steeds

[22] WP 136, p. 17.
[23] Groep Gegevensbescherming Artikel 29, Advies 1/2008 over gegevensbescherming en zoekmachines, WP 148, 00737/NL, goedgekeurd op 4 april 2008, p. 9.
[24] Groep Gegevensbescherming Artikel 29, Opinion 13/2011 on Geolocation services on smart mobile devices (alleen nog beschikbaar in het Engels) WP 185, 881/11/EN, goedgekeurd op 16 mei 2011. Beschikbaar via: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.
[25] WP 185, p. 11.

vaker sprake kan zijn van identificeerbaarheid.[26] Tevens wordt er duidelijk op gewezen dat het voor identificeerbaarheid zeker niet noodzakelijk is dat de naam van de betrokkene bekend is. Het gaat erom dat: '*(…) a user can be "singled out" even if his/her real name is not known*'.[27]

2.4 Ruime uitleg en het internet?

Wanneer we nu deze uitleg van het begrip persoonsgegevens ´loslaten´ op open bronnen, meer in het bijzonder op het internet, dan blijkt dat vrijwel elk gegeven op het internet dat op de een of andere wijze een link heeft met een persoon, hoe zwak deze link ook is, als persoonsgegeven beschouwd moet worden. De kans dat er enig ander persoon is die op basis van slechts een stukje informatie, hoe triviaal ook, in combinatie met andere gegevens een persoon kan identificeren is immers groot. Dit, in combinatie met de uitleg dat wanneer het niet mogelijk is om met zekerheid te zeggen of in een bepaald geval wel of geen sprake zal zijn van identificeerbaarheid alle gegevens als persoonsgegevens behandeld moeten worden, leidt tot een situatie waarin de hele oceaan aan potentieel identificeerbare gegevens op internet binnen het bereik van het recht op gegevensbescherming valt. In veel gevallen zal identificatie echter helemaal geen doel zijn, zal er ook geen sprake zijn van identificatie bij degene die de gegevens verwerkt, en is het enkel twijfelachtig of enig ander persoon deze data ooit zal gebruiken ter identificatie. Dit alles met betrekking tot een datasubject dat geen enkele clou heeft van het gebruik van hem betreffende data, dan wel mogelijke identificeerbaarheid van hem als persoon op basis van deze data. Hoewel juist dit aspect – de onwetendheid en het gebrek aan transparantie voor datasubjecten – een van de grondslagen vormt voor het recht op gegevensbescherming, dwaalt deze situatie anderzijds erg ver af van de oorspronkelijke juridische basis waarop het recht op gegevensbescherming gestoeld is, het recht op privacy.

Alvorens in paragraaf 3 nader in te gaan op de – onduidelijkheden in – de relatie tussen privacy en gegevensverwerking, mede aan de hand van jurisprudentie van het Hof van Justitie (HvJ), heeft ook de Artikel 29-Werkgroep in de in deze paragraaf besproken opinie aandacht besteed aan de relatie tussen privacy en gegevensbescherming. De Artikel 29-Werkgroep wijst erop dat bij de verwerking van persoonsgegevens tevens de bescherming van het recht op een persoonlijke levenssfeer gewaarborgd moet worden.

"Het kan een aanzienlijke rol spelen bij de vaststelling hoe de bepalingen van de Richtlijn moeten worden toegepast op sommige situaties waarbij geen risico bestaat voor de fundamentele rechten van personen".[28]

[26] WP 185, p. 10.
[27] WP 185, p. 11.
[28] WP 136, p. 4.

Vervolgens stelt de Artikel 29-Werkgroep: '*(…) dat een ruime interpretatie van het begrip persoonsgegeven gecombineerd moet worden met een passend evenwicht bij de toepassing van de bepalingen van de Richtlijn*'.[29]

Deze citaten lijken een benadering voor te staan waarbij een daadwerkelijke inmenging in het privéleven van betrokkenen van invloed is op de toepasselijkheid van het recht op gegevensbescherming. Later in de opinie lijkt deze benadering echter weer grotendeels teniet te worden gedaan door te benadrukken dat art. 8 van het Handvest van de Grondrechten van de Europese Unie een autonoom recht is, naast en afzonderlijk van het recht op eerbiediging van het privéleven en het familie- en gezinsleven in art. 7 Handvest. Hierbij wijst de Artikel 29-Werkgroep erop dat de Richtlijn afzonderlijk verwijst naar de verwerking van persoonsgegevens in contexten buiten de sfeer van de woning en het familie- en gezinsleven.[30]

In de volgende paragraaf wordt ingegaan op de wijze waarop het Hof van Justitie omgaat met het onderscheid tussen privacy en gegevensverwerking. Deze paragraaf beoogd duidelijk te maken dat de vraag naar het fundamentele karakter van gegevensbescherming, hoewel positief beantwoord met het Verdrag van Lissabon, nog steeds relevant is in het licht van de wenselijkheid van de oprekking van de reikwijdte van het begrip persoonsgegevens.

3. Privacy en de verwerking van persoonsgegevens

3.1 Vóór en na Lissabon

Hoewel privacy en gegevensbescherming veelal in één adem genoemd worden, is het van belang om hier kort stil te staan bij het onderscheid en de onderlinge relatie tussen beide rechten. Het recht op gegevensbescherming is van oudsher een onderdeel van het meer omvattende recht op privacy.[31] Het recht op privacy kan gezien worden als een 'paraplurecht' met verschillende dimensies. Het huisrecht, het recht op lichamelijke integriteit, het recht om zelf te mogen kiezen met wie al dan niet relaties aan te gaan en het recht op gegevensbescherming. Vanuit dit perspectief kan er sprake zijn van een schending van privacy, zonder dat er persoonsgegevens in het geding zijn, bijvoorbeeld bij het onrechtmatige binnentreden van een woning. Anderzijds houdt dit ook in dat er sprake kan zijn van een verwerking van persoonsgegevens, zonder dat er sprake is van een aantasting van privacy. Blok heeft het concept privacy tot in detail onderzocht en komt tot de conclusie

[29] WP 136, p. 6.
[30] WP 136, p. 8.
[31] Voor Nederland verankerd in art. 10 Gw, welk artikel wordt uitgelegd in het licht van art. 8 EVRM. Beschikbaar op: www.echr.coe.int/NR/rdonlyres/655FDBCF-1D46-4B36-9DAB-99F4CB59863C/0/DutchN%C3%A9erlandais.pdf.

dat het bij privacy in de kern gaat om: bescherming tegen bemoeienis van buitenaf met betrekking tot de eigen woning, de vertrouwelijke communicatie, het intieme leven en het lichaam.[32] In veel gevallen zal de verwerking van persoonsgegevens niet plaatsvinden in het kader van vertrouwelijke communicatie, en in heel veel gevallen zullen persoonsgegevens die verwerkt worden niet raken aan het intieme leven van de betrokkene. Voordat, via het Verdrag van Lissabon, het Handvest van de Grondrechten van de Europese Unie gelding kreeg, was de vraag dan ook legitiem of het recht op gegevensverwerking in alle gevallen te kwalificeren was als een mensenrecht. Het antwoord voor die tijd was naar onze mening nee. Niet elke verwerking van persoonsgegevens raakt de kern waar het bij het recht op privacy om gaat. De Europese regulering van het recht op gegevensbescherming is duidelijk niet alleen ingegeven door het mensenrecht op privacy, maar ook door het vrij verkeer van persoonsgegevens. Regels betreffende de verwerking van persoonsgegevens kunnen immers een remmend effect op de handel hebben als deze regels binnen de EU niet geharmoniseerd zijn. Het is ook niet het mensenrecht, maar deze economische overweging die de rechtsbasis vormt voor Richtlijn 95/46/EG aangezien deze gebaseerd is op wat nu is art. 114 EU-Verdrag. Hoewel vanuit deze rechtsbasis het belang van geharmoniseerde wetgeving te verklaren is, volgt hieruit niet per definitie dat sprake moet zijn van een zeer hoog beschermingsniveau, danwel een zeer brede werkingssfeer van het recht op gegevensbescherming. Sterker nog, een breed toepassingsbereik zal de grensoverschrijdende verwerking van gegevens eerder bemoeilijken dan vergemakkelijken. Geredeneerd vanuit de optiek van de bescherming van het individu kan de vraag gesteld worden in hoeverre deze bescherming nog gestoeld kan worden op de achterliggende gedachte van bescherming van de persoonlijke levenssfeer, als de brede werkingssfeer van het recht op gegevensbescherming ook zeer strikte voorwaarden voor de verwerking van persoonsgegevens oplegt wanneer helemaal geen sprake is van een (mogelijke) inbreuk op het privéleven.

Sinds de inwerkingtreding van het Verdrag van Lissabon heeft het Handvest van de Grondrechten van de Europese Unie dezelfde rechtskracht verkregen als de Unie Verdragen. Hierdoor wordt het Handvest juridisch bindend voor de instellingen van de Unie en voor de lidstaten, voor zover deze uitvoering geven aan Uniewetgeving. Tevens is met het Verdrag van Lissabon de mogelijkheid gecreëerd voor toetreding van de Europese Unie tot het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).[33] Een zaak kan pas aanhangig worden gemaakt voor het Europees Hof voor de Rechten van de Mens (EHRM) als alle nationale rechtsmiddelen zijn uitgeput. Voor de Europese Unie houdt dit in dat bij schending van het EVRM eerst een beroep gedaan moet worden op het Europees Hof van Justitie (HvJ). Dit Hof zal het recht uit moeten leggen in overeenstemming met de rechtspraak van het EHRM. Hetzelfde geldt voor de uitleg van de rechten verankerd in het Handvest. Een afwijkende uitleg zou immers in strijd komen met

[32] Peter Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlands en Amerikaans recht*, Den Haag: Boom Juridische Uitgevers 2002.
[33] Zie voor actuele ontwikkelingen hieromtrent: www.eerstekamer.nl/eu/thema/toetreding_van_de_eu_tot_het.

het EVRM. Particulieren kunnen zich in hun onderlinge relaties niet direct op het Handvest beroepen, maar een nationale rechter is bij de uitleg van een Uniehandeling in een geschil tussen twee particulieren wel gehouden de Uniehandeling uit te leggen met inachtneming van het Handvest en in geval van onduidelijkheid zal de nationale rechter prejudiciële vragen dienen te stellen aan het HvJ. Met het Verdrag van Lissabon is het recht op gegevensverwerking dus verankerd als fundamenteel recht. Uit onderstaande bespreking van enkele rechterlijke uitspraken van het HvJ blijkt echter dat de verhouding tussen het recht op privacy en het recht op gegevensbescherming nog altijd niet geheel duidelijk is.

3.2 Uitleg van het Hof van Justitie

Uit rechtspraak die dateert van vóór het Verdrag van Lissabon blijkt dat het HvJ worstelt met de relatie tussen het recht op privacy en het recht op gegevensverwerking en bovendien met de status van het recht op gegevensverwerking.[34] In zaken als *Österreichischer Rundfunk*[35] en *Promusicae*[36] lijkt het Hof de concepten door elkaar te halen en in de zaak *Österreichischer Rundfunk* gaat het Hof zelfs geheel voorbij aan het feit dat er een specifiek juridisch kader voor gegevensverwerking is. Met betrekking tot de status van gegevensbescherming kan in de eerste plaats gewezen worden op de zaak *Satamedia*[37] waarin het Hof gegevensbescherming van lagere orde acht dan het recht op vrijheid van meningsuiting. Hetzelfde lijkt het geval te zijn in de zaak *Bavarian Lager* waar toegang tot gegevens mogelijk wordt geacht aangezien het vrijgeven van deze gegevens aldus de rechter niet strijdig is met het recht op privacy.[38] Hier volgt het Hof de redenering dat aangezien het recht op privacy niet geschonden wordt, de regels betreffende gegevensbescherming niet toepasselijk zijn.[39] In de genoemde zaken bevreemd niet alleen de wijze waarop het Hof omgaat met de concepten privacy en gegevensbescherming, maar ook de tegenstrijdigheid met de algemene uitleg dat mensenrechten gelijk zijn en er dus geen rangorde bestaat tussen dergelijke rechten.[40]

Na de inwerkingtreding van het Verdrag van Lissabon wordt in hoger beroep de *Bavarian Lager*-zaak alsnog in het voordeel van het recht op gegevensbescherming beslecht en wordt onderkend dat de vraag of sprake is van een schending van privacy geen rol speelt. Zodra sprake is van de verwerking van persoonsgegevens, is het regime betreffende

[34] Meer uitgebreid over dit onderwerp Orla Lynskey, *From Market-Making Tool to Fundamental Right; Data Protection's Identity Crisis*. Paper presented at the 2012 CPDP Conference Brussels Belgium.
[35] HvJ 2003, nr. C-139/01, ECR I-4989 (*Österreichischer Rundfunk en anderen*).
[36] HvJ 2008, nr. C-275/06, ECR I-271 (*Productores de Música de España (Promusicae)/Telefónica de España*).
[37] HvJ 2008, nr. C-73/07, ECR-I 09831 (*Tietosuojavaltuutettu/Satakunnan Markkinapörssi OY, Satamedia*).
[38] HvJ 2007, nr. T-194/04, ECR II-3201 (*Bavarian Lager/Commissie*).
[39] Onder verwijzing naar art. 4 lid 1 onder b Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie, PbEG, L 145/43.
[40] Zie bijv. M. Kuitenbrouwer & M. Leenders (red.), *Geschiedenis van de mensenrechten. Bouwstenen voor een interdisciplinaire benadering*, Hilversum: Verloren 2000, p. 77.

gegevensbescherming toepasselijk en moet dit dus nageleefd worden.[41] In een andere post *Lissabon*-zaak wordt duidelijk dat het Hof het recht op gegevensbescherming niet langer lager in rangorde plaatst dan andere grondrechten. In de zaak *Volker* ging het om het vergroten van transparantie rondom het toekennen van communautaire financiële middelen — op zich een legitiem streven — door het publiek toegankelijk maken van informatie over de begunstigden van deze middelen.[42] Op basis van een uitgebreid gemotiveerde proportionaliteits- en subsidiariteitstoets komt het Hof tot de conclusie dat het doel, het vergroten van transparantie rondom het gebruik van communautaire middelen, ook bereikt kan worden op een wijze die minder inbreuk maakt op de privacy van betrokkenen. De wijze waarop het Hof tot deze conclusie komt geeft echter nog steeds blijk van onduidelijkheid omtrent de relatie tussen, en daarmee de uitleg van, het recht op privacy en het recht op gegevensverwerking. Eerst stelt het Hof dat art. 8 lid 1 Handvest, het fundamentele recht betreffende bescherming van persoonsgegevens, nauw verband houdt met het in art. 7 Handvest neergelegde recht op eerbiediging van het privéleven.[43] Vervolgens, onder verwijzing naar de zaak *Schmidberger*, wijst het Hof op de niet absolute gelding van het recht op bescherming van persoonsgegevens.[44] In rechtsoverweging 80 van het arrest *Schmidberger* stelt het Hof met betrekking tot rechten die geen absolute gelding hebben dat deze*: '(…) in relatie tot hun functie in de maatschappij moeten worden beschouwd. Bijgevolg kan de uitoefening van die rechten aan beperkingen worden onderworpen, mits die beperkingen daadwerkelijk beantwoorden aan doeleinden van algemeen belang en, het door dergelijke beperkingen nagestreefde doel in aanmerking genomen, niet zijn te beschouwen als een onevenredige en onduldbare ingreep waardoor de beschermde rechten in hun kern zouden worden aangetast'.*[45]

Terugkerend naar het arrest *Volker* stelt het Hof in rechtsoverweging 52:

"In deze omstandigheden dient enerzijds te worden vastgesteld dat de eerbiediging van het in de artikelen 7 en 8 van het Handvest erkende recht op persoonlijke levenssfeer bij de verwerking van persoonsgegevens gelijk welke informatie betreft aangaande een geïdentificeerde of identificeerbare natuurlijke persoon en, anderzijds, dat de beperkingen

[41] HvJ 2010, nr. C-28/08, ECR I-6055 (*Europese Commissie/Bavarian Lager*).
[42] Arrest van het HvJ 9 november 2010 (Grote kamer), nr. C-92/09 (*Volker und Markus Schecke GbR*) en nr. C-93/09 (*Hartmut Eifert/Land Hessen*). Het gaat om informatie over besteding van gelden uit het Europees Landbouwgarantiefonds (ELGF) en het Europees Landbouwfonds voor Plattelandsontwikkeling (ELFPO). De problematiek rondom toepasselijkheid van het gegevensverwerkingsrecht had te maken met verschillen tussen natuurlijke personen, rechtspersonen en rechtspersonen waarbij uit de officiële naam de identiteit van een of meerdere natuurlijke personen blijkt. Zie voor een heldere beschrijving van deze zaak Margriet Overkleeft-Verburg in *Jurisprudentie Bestuursrecht* 2011-1.
[43] R.o. 47.
[44] HvJ 2003, nr. C‑112/00, ECR I-05659 (*Schmidberger*), punt 80.
[45] Onder verwijzing naar de arresten 8 april 1992, nr. C-62/90, *Jur.* p. I-2575, punt 23 (*Commissie/Duitsland*), en 5 oktober 1994, nr. C-404/92 P, Jur. p. I-4737, punt 18 (*X/Commissie*).

die mogen worden gesteld aan het recht op bescherming van de persoonsgegevens, overeenkomen met die welke worden toegelaten in het kader van artikel 8 EVRM".[46]

Het gedeelte na anderzijds roept de vraag op of deze uitleg correct is, en niet juist voor de bescherming van persoonsgegevens het gedetailleerde juridische raamwerk dat met name Richtlijn 95/46/EG voorschrijft als toetsingskader gevolgd moet worden.

Bovendien wordt er op verschillende plaatsen in het arrest gesproken over eerbiediging van privéleven in het algemeen en op de bescherming van hun persoonsgegevens in het bijzonder.[47] Dit roept de vraag op of de zaak op een andere wijze beoordeeld zou zijn als geen sprake zou zijn geweest van een aantasting van het privéleven, maar enkel van een verwerking in strijd met het recht op gegevensbescherming.

3.3 Schwartz en Solove

Dat niet alleen door het Hof, maar ook in de literatuur, geworsteld wordt met het uitdijende concept persoonsgegevens in relatie tot privacy en gegevensbescherming blijkt bijvoorbeeld uit een artikel van Schwartz en Solove.[48] Hoewel dit artikel overwegend vanuit Amerikaans perspectief is geschreven, bevat het ook een vergelijking met het Europese wettelijke kader. Schwartz en Solove gaan in op de problemen die bestaan met betrekking tot de definiëring van wat zij noemen PII, *Personally Identifiable Information*. Zij verklaren de complexiteit in het duiden van het concept PII vanuit het perspectief van de huidige informatiemaatschappij waarin het steeds moeilijker is om gegevens te anonimiseren. Bovendien, door een constante aanwas van gegevens alsmede technologische ontwikkelingen, kunnen gegevens die vandaag de dag niet identificeerbaar zijn, dit morgen ineens wel zijn. Het concept is dus niet alleen technologie afhankelijk, maar ook context afhankelijk.[49]

Ondanks de problemen met definiëring, pleiten Schwarz en Solove voor het behoud van het concept PII, zij het met de nodige aanpassing. In dit verband stellen zij de problematiek rond het concept PII als volgt scherp:

"Abandoning PII is problematic, however, because the concept serves a crucial function: it establishes the boundaries of privacy regulation. Without some concept of PII, there would be no limits on the scope of privacy law. In a world overflowing with information, the law cannot possibly regulate all of it. Yet, without adequate boundaries on regulation, privacy rights would expand to protect a nearly infinite array of information, including practically

[46] Onder verwijzing naar EHRM, arresten *Amann/Zwitserland* van 16 februari 2000, Recueil des arrêts et décisions 2000-II, § 65, en *Rotaru/Roemenië* van 4 mei 2000, Recueil des arrêts et décisions 2000-V, § 43.
[47] Arrest *Volker*, r.o. 77, 78 en 81.
[48] Paul M. Schwartz & Daniel J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information', *New York University Law Review* December 5, 2011, Vol. 86, p. 1814 (hierna: Schwartz & Solove 2011); UC Berkeley Public Law Research Paper No. 1909366; GWU Legal Studies Research Paper No. 584; GWU Law School Public Law Research Paper No. 584. Beschikbaar via: http://ssrn.com/abstract=1909366.
[49] Schwartz & Solove 2011, p. 1836.

every piece of statistical or demographic data. The law would encompass nearly every fact about human behavior, no matter how generalized".[50]

Dit zou leiden tot een '*cumbersome and unworkable regulation of nearly all information*'.[51] Daarom stellen zij dat: '*Privacy law must have coherent boundaries, which adequately protect privacy and which can be flexible and evolving*'.[52]

Vanuit deze overwegingen zou aansluiting bij het concept privacy – in de zin van privéleven zoals uitgelegd door het Hof van Justitie – om te komen tot een definiëring van het concept PII in lijn der verwachting liggen. Echter, Schwartz en Solove sturen aan op een onderverdeling binnen het concept PII op basis van het risico van identificatie:

"Our model places information on a continuum that begins with no risk of identification at one end, and ends with identified individuals at the other. We divide this spectrum into three categories, each with its own regulatory regime: under the PII 2.0 model, information can be about an (1) identified, (2) identifiable, or (3) non-identifiable person. Our three categories divide up this spectrum and provide different regimes of regulation for each. Because these categories do not have hard boundaries, we define them in terms of standards. (…) In our reconceptualized notion of PII, the key is to think about identification in terms of risk level."[53]

Hoewel deze benadering naar onze mening zeker kan bijdragen aan een meer praktijkgerichte en realistische invulling van het recht op gegevensbescherming, en zeker meegenomen moet worden in de herzieningsronden met betrekking tot de nieuwe Privacyverordening, lost deze benadering de kloof tussen beschermingsdoel – persoonlijke levenssfeer en vrij verkeer gegevens – en beschermingsobject – elk gegeven dat een persoon *kan* identificeren – niet op. Het is immers maar de vraag of in alle situaties waarin iemand identificeerbaar is, ook sprake is van het in het gedrang komen van de persoonlijke levenssfeer.

3.4 Het doel voorbij?

Als we kijken naar de ratio achter de nadere regulering van de verwerking van persoonsgegevens, welke mooi beschreven is in de titel van Richtlijn 95/46/EG, doemt sterk de vraag op of het middel het doel inmiddels niet voorbijschiet. De Richtlijn beoogt de *bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens* en betreffende het *vrije verkeer van die gegevens*.
Dat met het eerste zinsdeel uitdrukkelijk gedoeld wordt op een link met privacy, blijkt uit overweging 10 van de Preambule van Richtlijn 95/46/EG:

[50] Schwartz & Solove 2011, p. 1866.
[51] Schwartz & Solove 2011, p. 1827.
[52] Schwartz & Solove 2011, p. 1836.
[53] Schwartz & Solove 2011, p. 1877 and 1879.

"Overwegende dat (…)de eerbiediging moet worden gewaarborgd van de fundamentele rechten en vrijheden, en met name van het recht op bescherming van de persoonlijke levenssfeer, dat tevens in artikel 8 van het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en in de algemene beginselen van het Gemeenschapsrecht is erkend (…)."

Door de oprekking van de reikwijdte van het begrip persoonsgegevens is er echter een beschermingsregime ontstaan waarbij ook zonder enige dreiging voor de persoonlijke levenssfeer, persoonsgegevens vallen binnen het strikte beschermingsregime van Richtlijn 95/46/EG. Het is zeer discutabel of dit brede toepassingsgebied vervolgens bijdraagt aan het tweede belang achter Richtlijn 95/46/EG, het vrije verkeer van gegevens.

In de volgende paragraaf wordt besproken hoe de praktische toepasbaarheid van het recht op gegevensbescherming door de brede uitleg van het begrip persoonsgegevens een stuk gecompliceerder is geworden.

4. Praktische toepasbaarheid van het concept persoonsgegevens

Met de nog immer stijgende toegang tot het internet[54] en de steeds meer centrale rol die het internet speelt als communicatiemiddel[55] groeit de zorg om de bescherming van data. De hierboven beschreven tendens om het concept persoonsgegevens ruim uit te leggen, en daarmee het recht op gegevensbescherming snel van toepassing te achten, is wat dat betreft een schijnbaar logische reactie om voor betere bescherming te zorgen. De vraag is echter wat de betekenis van deze bescherming is wanneer deze niet meer handhaafbaar is vanwege de grote discrepantie met wat er in de praktijk gebeurt en zelfs of deze ruimere uitleg in combinatie met een gebrekkige handhaving niet averechts kan werken. Immers, regelgeving waarmee zeer gemakkelijk in strijd gehandeld wordt, zelfs door 'normaal' te handelen, nodigt niet direct uit tot strikte naleving.

4.1 Hoedanigheid van de verwerker: twee illustraties

Zoals in de introductie aangegeven zal het probleem, dat ondanks – of juist dankzij? – de ruimere uitleg van het recht op gegevensbescherming dit recht zeer snel en daarmee veelvuldig geschonden wordt, geïllustreerd worden aan de hand van een voorbeeld. Neem

[54] Volgens het CBS had in 2006 80% van alle Nederlandse huishoudens internettoegang, tegen 94% in 2011. Zie: http://statline.cbs.nl/StatWeb/publication/default.aspx?VW=T&DM=SLNL&PA=71102ned&D1=3-4%2c11-17&D2=0-10&D3=a&HD=080424-1708&HDR=T&STB=G1%2cG2.

[55] Zo ook de aankondiging dat de Belastingdienst van papier wil overstappen naar berichtgeving via internet; *NOS*, 'Blauwe brief gaat verdwijnen'. Beschikbaar via: http://nos.nl/artikel/337730-blauwe-brief-gaat-verdwijnen.html.

het googelen van personen, oftewel het zoeken op internet naar informatie over iemand. Door de wijde verspreiding van sociale media is er over bijna iedereen wel informatie op internet beschikbaar, op internet geplaatst door de betreffende persoon zelf, dan wel door anderen.[56] Zonder twijfel is zowel het plaatsen als het zoeken aan te merken als een verwerking van persoonsgegevens in de zin van Richtlijn 95/46/EG, en daarmee ook in de zin van de Nederlandse Wet bescherming persoonsgegevens (Wbp). Het gaat hier immers om informatie betreffende een geïdentificeerd persoon[57] en '*elke handeling (...) met betrekking tot persoonsgegevens*' geldt als verwerking.[58] Als de zoektocht geheel in een privésituatie plaatsvindt is desondanks de Wbp niet van toepassing.[59] Echter zoals hierboven onder 2.2 aangegeven moet deze uitzondering beperkt uitgelegd worden volgens het Hof van Justitie, dus is de zoeker bijvoorbeeld een werkgever die een potentiële werknemer googelt dan geldt deze uitzondering niet.[60] Gezien de toepasselijkheid van de Wbp op de zoekactie door de werkgever, zijn er een beperkt aantal verwerkingsgronden die een rechtvaardiging bieden om deze gegevensverwerking te mogen uitvoeren.[61] De gronden die hierop mogelijk van toepassing zouden zijn, zijn expliciete toestemming van de begoogelde of de grond dat de belangen van de ´googelaar´ (in de zin van de Wbp de verantwoordelijke) zwaarder wegen dan de fundamentele belangen van de begoogelde. Het is natuurlijk zeer waarschijnlijk dat deze toestemming in de meeste gevallen niet eerst verkregen is, aangezien het *even googelen* nu juist een laagdrempelige en goedkope manier is om een eerste beeld te vormen van – in dit geval – de potentiële werknemer. De belangenafweging is per definitie een genuanceerder verhaal – het betreft immers een afweging –, maar feit is dat de werkgever geen noodzaak heeft de gegevens te verwerken, zoals art. 8 onder f Wbp wel vereist. De werkgever heeft immers nu juist de sollicitatieprocedure tot zijn beschikking om alles dat noodzakelijk is te weten te komen over de potentiële werknemer. Er is dus vermoedelijk sprake van strijd met het recht op gegevensbescherming wanneer de informatie wordt bekeken in de hoedanigheid van werkgever, ook al is dezelfde persoon wel vrij deze informatie te bekijken als privépersoon.

Dit is een sterk voorbeeld van de discrepantie tussen regelgeving en praktijk wat betreft gegevensbescherming, omdat hoogstwaarschijnlijk iedereen die dit leest zal erkennen wel eens iemand te hebben gegoogeld en mogelijk ook een groot aantal lezers dit hebben gedaan anders dan '*ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden*'.[62] Voor deze laatste categorie is het misschien een verrassing dat zij iets deden dat waarschijnlijk niet toegestaan is; de informatie die zij zochten is toch

[56] CBS, 'Nederlandse jongeren zeer actief op sociale netwerken'. Beschikbaar via: www.cbs.nl/nl-NL/menu/themas/dossiers/jongeren/publicaties/artikelen/archief/2011/2011-3296-wm.htm.
[57] Art. 1 onder a Wbp.
[58] Art. 1 onder b Wbp.
[59] Art. 2 lid 2 onder a Wbp.
[60] Dat dit een reëel probleem is werd eerder al vastgesteld, zie bijv. J.E.J. Prins, 'Googlende werkgevers', *NJB* 2008/677, afl. 13, jrg. 83, 28 maart 2008, p. 780-781.
[61] Art. 8 Wbp.
[62] Art.2 lid 2 onder a Wbp.

immers ‘vrij’ op internet verkrijgbaar? Het is ook zeer de vraag of de werkgevers die dit lezen vanaf nu besluiten geen informatie meer over sollicitanten op te zoeken, of het nu toegestaan is of niet.[63]

Hoewel het buiten het bereik van dit artikel valt om uitgebreid de theorieën over naleving uit de doeken te doen, kan hier het onderscheid tussen *mala in se* – een inherent immorele handeling zoals bijvoorbeeld moord – en *mala in prohibitum* – een handeling die verboden is zonder noodzakelijkerwijs op zichzelf immoreel te zijn zoals te hard rijden op een compleet lege weg – hier verduidelijking bieden. Waar men in het algemeen bij handelingen die als een *mala in se* ervaren worden dit uit eigen beweging probeert niet te doen, geldt voor *mala in prohibitum* juist dat dit vaak grotendeels afhangt van de pakkans en eventuele sanctie.[64] Omdat het zoeken naar ‘vrije informatie’ op zich niet als immoreel zal worden ervaren, is het waarschijnlijk dat juist de handhaving een grote rol speelt in de naleving van het recht op gegevensbescherming. Zoals aangegeven is dit een heikel punt omdat handhaving op een dusdanig grote schaal niet mogelijk is. En dit kan op den duur weer problematisch zijn, omdat het stelselmatig niet-naleven van de regelgeving de betekenis hiervan mogelijk uitholt.

Het zojuist gegeven voorbeeld betreft de relatie tussen werkgevers en werknemers, iets dat zeer veel mensen raakt. Zeer vergelijkbaar is echter de situatie wanneer verzekeraars op sociale media kijken om te onderzoeken of hun klanten niet frauderen.[65] Ook hier wordt vanuit een professionele hoedanigheid gezocht naar persoonsgegevens, dus opnieuw is de Wbp van toepassing en zijn er dus slechts een beperkt aantal verwerkingsgronden die deze gegevensverwerking rechtvaardigen. Expliciete toestemming vragen aan de van fraude verdachte verzekerde om diens gegevens in te zien is vanzelfsprekend onzinnig aangezien in een daadwerkelijk geval van fraude deze toestemming simpelweg geweigerd kan worden of de verdachte naar aanleiding van dit verzoek het eventuele bewijs van de fraude zoek kan maken. Een afweging tussen de belangen van de verzekeraar om effectief fraude te kunnen bestrijden enerzijds en het recht op privacy van de verzekerde anderzijds, zou mogelijk wel in het voordeel van de verzekeraar kunnen uitvallen en zodoende een rechtvaardiging voor de gegevensverwerking kunnen vormen.[66] In deze situatie is er echter ook nog de reële kans dat het bijzondere persoonsgegevens betreft, zoals wanneer een verzekeraar een

---

[63] In die geest, de reactie onder een artikel van prof. Prins waarin zij betoogt dat werkgevers niet zomaar sollicitanten mogen googlen; ‘Totaal wereldvreemd en dan (of dus) hoogleraar. Waarom niet verbieden om überhaupt een vraag te stellen.’ Beschikbaar via: www.elsevier.nl/web/10210357/Nieuws/Internet-Gadgets/Werkgever-mag-sollicitant-niet-zomaar-googlen.htm?forum=190469&showall=true#599406.

[64] C.A. Sanderson & J.M. Darley, ‘"I Am Moral, But You Are Deterred": Differential Attributions About Why People Obey the Law’, *Journal of applied social psychology* 2002, vol. 32, nr. 2, p. 375-405.

[65] Bijv. verzekeraar Aegon geeft toe op de Facebook-pagina van klanten te kijken bij vermoedens van fraude. Zie in dit verband: www.rtl.nl/(/actueel/rtlnieuws/binnenland/)/components/actueel/rtlnieuws/2011/11_november/07/binnenland/verzekeraars-checken-facebook-hyves-aegon-controle.xml.

[66] Art. 8 onder f Wbp. Voor enkele voorbeelden het belang van verzekeraars bij toegang tot persoonsgegevens: http://stopfraude.blogspot.com/2004/12/fraudebestrijding-gebaat-bij-betere.html, http://stopfraude.blogspot.com/2005/05/tijd-rijp-voor-aanpak.html.

zorgverzekeringsclaim onderzoekt door na te gaan of de verzekerde inderdaad de geclaimde gezondheidsproblemen heeft. Bijzondere gegevens zijn namelijk een gelimiteerd aantal type gegevens, welke als extra gevoelig beschouwd worden en gegevens betreffende iemands gezondheid vallen hier ook onder.[67] Het regime is strikter voor dit type gegevens in die zin dat het in principe verboden is deze gegevens te verwerken[68] tenzij een wettelijke uitzondering van toepassing is. In het voorbeeld van de verzekeraar is hier sprake van wanneer de gegevensverwerking *noodzakelijk* is voor de uitvoering van de overeenkomst tussen verzekeraar en verzekerde.[69] Deze afweging zal per geval natuurlijk verschillen, maar opnieuw geldt dat juist vanwege het laagdrempelige karakter van het zoeken van informatie over iemand op het internet, het de vraag is of dit – bijzondere persoonsgegevens verwerkende – middel pas wordt ingezet wanneer dit echt noodzakelijk en dus gerechtvaardigd is.

Deze voorbeelden laten treffend zien hoe de ruime uitleg het begrip persoonsgegevens er mogelijk toe leidt dat gangbare handelingen binnen de reikwijdte van het recht op gegevensbescherming vallen. Tegelijkertijd is de illustratie aan de hand van deze specifieke voorbeelden ook een indicatie dat de beoordeling van wat nu precies wel en niet onder het recht op gegevensbescherming valt erg afhangt van de omstandigheden van het geval. Onduidelijkheid over de precieze reikwijdte terzijde, door de laagdrempeligheid van de betreffende handelingen en de onmogelijkheid van dekkend toezicht en handhaving is het de vraag of er geen – te – groot verschil ontstaat tussen de regelgeving en de praktijk. De eisen die nu worden gesteld zijn mogelijk naar verhouding tot de schending te zwaar; denk aan het moeten verkrijgen van expliciete toestemming alvorens iemand te mogen opzoeken via Google wanneer het niet puur huishoudelijk gebruik betreft. Dit kan op zijn beurt weer in de weg staan aan het voldoen aan andere waarden voortvloeiend uit de Wbp, zoals transparantie. De verwerker zal immers niet staan te springen om transparant te zijn over een gegevensverwerking waarvoor hij niet de vereiste toestemming heeft verkregen. De hier opgeworpen vraag is dus of door het stellen van te zware eisen aan relatief ingeburgerd gedrag, niet de kans bestaat dat ook aan lichtere eisen die voor dit gedrag gesteld worden niet meer voldaan wordt? Indien deze vraag bevestigend beantwoord wordt, zou dit kunnen betekenen dat de ruimere toepasselijkheid van het recht op gegevensbescherming in feite de betekenis ervan kan uithollen.

[67] Art. 16 Wbp: 'godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging' en 'strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.'
[68] Art. 16 Wbp.
[69] Art. 21 lid 1 onder b 2° Wbp.

4.2 De (on)mogelijkheid van anonimisering

Er is nog een punt waar regelgeving en praktijk niet – meer – in de pas lopen. Richtlijn 95/46/EG[70] en de Wbp[71] zijn namelijk niet van toepassing indien gegevens dusdanig zijn geanonimiseerd dat de persoon waarop deze gegevens betrekking hebben niet meer identificeerbaar is. Hierdoor is immers niet langer sprake van persoonsgegevens in de zin van de Wbp en is het gegevensbeschermingsregime dus niet van toepassing op de verwerking van dergelijke geanonimiseerde gegevens. Effectieve anonimisering *kan* dus de reikwijdte van het begrip persoonsgegevens verkleinen.

De praktijk, en dan met name enkele grote schandalen, laat echter zien dat het haast niet mogelijk is gegevens effectief te anonimiseren, omdat deze relatief gemakkelijk toch te herleiden zijn tot een identificeerbare persoon. In zijn artikel over de tekortkoming van anonimisering van data bespreekt Paul Ohm enkele van deze zaken alsook onderzoek naar hoeveel verschillende gegevens ervoor nodig zijn om iemand te kunnen identificeren.[72]

In de *AOL*-zaak betrof het een zoekmachine die ten behoeve van onderzoek drie maanden zoekactiviteit van haar gebruikers vrijgaf. Het betrof ongeveer 20 miljoen zoekopdrachten van zo'n 650.000 gebruikers, waarbij de namen en IP-adressen vervangen waren door een uniek nummer. Al binnen enkele dagen bleek dat door kritisch naar de zoekopdrachten te kijken men zeer gemakkelijk de identiteit achter een uniek nummer kon achterhalen. Hierbij ging het zeker niet alleen om zogenaamde 'vanity searches' – het zoeken naar de eigen naam – maar bijvoorbeeld ook over het combineren van enkele zoekopdrachten, waarbij elke zoekopdracht steeds het aantal mogelijke zoekers verder terugbracht totdat uiteindelijk één of enkele individuen overbleven.[73, 74]

Een mogelijk nog minder waarschijnlijk voorbeeld van hoe gemakkelijk iemand te identificeren is met behulp van zeer geringe data is de *Netflix*-zaak.[75] Netflix, een verhuurder van films, schreef een wedstrijd uit met als doel een beter systeem te ontwikkelen om op basis van de voorkeuren van huurders films te kunnen aanbevelen. Om deelnemers aan deze wedstrijd te helpen dit te ontwikkelen, gaf Netflix ongeveer 100 miljoen beoordelingen van films door 500.000 gebruikers vrij. Deze beoordelingen bestonden uit de naam van de film, de concrete beoordeling van deze film door de gebruiker, de datum van de beoordeling en een uniek gebruikersidentificatienummer welke de gebruikersnaam verving. Binnen twee

[70] 95/46/EG, r.o. 26.
[71] Art. 10 lid 1 Wbp.
[72] P. Ohm, 'Broken Promises Of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review* 2010, nr. 57, p. 1701-1777. Beschikbaar via: http://ssrn.com/abstract=1450006 (hierna: Ohm 2010).
[73] Ohm 2010, p. 1717.
[74] Binnen 6 dagen na het vrijgeven van de gegevens door AOL hadden 2 journalisten van de *New York Times* door het kritisch bekijken van zoekopdrachten de identiteit achter een zogenaamd 'anoniem' nummer achterhaald. Zie: M.Barbaro & T. Zeller, 'A Face Is Exposed for AOL Searcher No. 4417749', *New York Times* 9 augustus 2006. Beschikbaar via: www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all.
[75] Zie voor een uitgebreide bespreking van deze zaak Ohm 2010, p. 1720-1722.

weken na het vrijgeven van deze gegevens werd ook hier aangetoond dat met minimale gegevens de data terug te koppelen was aan geïdentificeerde personen. Slechts de wetenschap wanneer – met een precisie van ongeveer twee weken – iemand een zestal films beoordeeld had, bleek in 99% van de gevallen al genoeg om te achterhalen welk uniek gebruikersidentificatienummer er bij deze persoon hoorde. Neem daarbij het gegeven dat veel filmliefhebbers naast beoordelingen binnen het – in principe – gesloten Netflix-systeem mogelijk ook beoordelingen plaatsen op openbare websites zoals IMDb[76] en het is duidelijk dat de gegevens die benodigd zijn om een Netflix-nummer te koppelen aan een persoon zeer gemakkelijk te vinden kunnen zijn.[77] Met als gevolg dat de zogenaamd anonieme gegevens die Netflix vrijgegeven had, weer gekoppeld konden worden aan geïdentificeerde personen, en dus kwalificeerden als persoonsgegevens.[78]

Het punt wat in beide bovenstaande zaken zeer belangrijk is, is dat ondanks dat op het eerste gezicht persoonsgegevens relatief gemakkelijk geanonimiseerd kunnen worden, de combinatie van enkele op zichzelf niet-identificerende gegevens al snel voldoende kan zijn om deze gegevens alsnog tot één persoon terug te leiden. Ohm bespreekt een onderzoek en de herhaling daarvan waaruit blijkt dat respectievelijk 87,1% dan wel 61% van de burgers van de V.S. geïdentificeerd kan worden met behulp van niet meer dan hun 5-cijferige ZIP-code, geboortedatum en geslacht.[79] Het feit dat deze basale gegevens – waar te pas en te onpas naar gevraagd wordt bij bijvoorbeeld aankopen op internet– gecombineerd al genoeg zijn om een persoon te identificeren, laat zien hoe moeilijk het is gegevens *effectief* te anonimiseren, zonder risico op de-anonimisering. Ohm stelt zelfs dat bovenstaande als geheel suggereert dat misschien alles 'Personal Identifiable Information' is voor diegene die de juiste externe informatie heeft om het mee te combineren.[80]

In verband met de kritische blik die hier op de oprekking van het begrip persoonsgegeven geworpen wordt, betekent dit dat een zeer ruime uitleg van dit begrip niet gecompenseerd dan wel ondervangen kan worden door gebruik te maken van anonimisatie, aangezien dit zeer wel een illusie lijkt te zijn.

---

[76] The InternetMovie Database, <www.imdb.com>.
[77] Ohm 2010, p. 1720.
[78] Hoe het openbaar worden van deze schijnbaar onschuldige informatie wel degelijk grote gevolgen kan hebben blijkt uit de hier beschreven zaak: R. Singel, 'Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims'. Beschikbaar via: www.wired.com/threatlevel/2009/12/netflix-privacy-lawsuit/. *Doe/Netflix, Inc.*, 2009 WL 6305245. Beschikbaar via: www.wired.com/images_blogs/threatlevel/2009/12/doe-v-netflix.pdf.
[79] Ohm 2010, p. 1719.
[80] Ohm 2010, p. 1723.

5. Voorstel ter vervanging van Richtlijn 95/46/EG door een Verordening[81]

Op 25 januari 2012, op *Data Protection Day*, is een 'ingrijpende hervorming' van de Europese regelgeving betreffende de verwerking van persoonsgegevens aangekondigd.[82] Het meest opvallend is dat de Richtlijn uit 1995 nu vervangen wordt door een Verordening. Als reden geeft de preambule bij de Verordening dat dit rechtsinstrument beter geschikt is dan een Richtlijn vanwege de directe werking wat minder juridische fragmentatie en daardoor betere harmonisatie met zich brengt.[83]

5.1 Definitie persoonsgegevens in Verordening

Relevant vanuit het perspectief van dit artikel is of deze 'ingrijpende hervorming' ook wat gaat veranderen aan de – brede – uitleg van het begrip persoonsgegevens. Kijkend naar art. 4 waarin de definities van de in de Verordening gebruikte begrippen worden gegeven, lijkt dit op het eerste gezicht het geval. Wanneer we hier eerst de definitie van persoonsgegevens uit de Richtlijn en vervolgens de definitie uit de Verordening neerzetten, lijkt de nieuwe definitie namelijk nog ruimer:

"persoonsgegevens, iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon, hierna 'betrokkene' te noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit;"[84]

Dit wordt vervangen door:

"persoonsgegevens: iedere informatie betreffende een betrokkene;"

Deze versimpeling van de definitie lijkt op het eerste oog een verruiming van het begrip in te houden. Dit blijkt echter schijn als we de nieuwe – apart in art. 4 lid 1 Verordening gedefinieerde – term *betrokkene* in ogenschouw nemen:

"betrokkene: een geïdentificeerde natuurlijke persoon of een natuurlijke persoon die direct of indirect, met behulp van middelen waarvan mag worden aangenomen dat zij

[81] COM(2012)11 (def.). Beschikbaar via: https://zoek.officielebekendmakingen.nl/blg-168656.pdf.
[82] Commission proposes a comprehensive reform of the data protection rules. Beschikbaar via: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
[83] COM(2012)11 (def.), p. 6.
[84] Art. 2 onder a Richtlijn 95/46/EG.

redelijkerwijs door de voor de verwerking verantwoordelijke dan wel door een andere natuurlijke of rechtspersoon in te zetten zijn, kan worden geïdentificeerd, met name aan de hand van een identificatienummer, gegevens over de verblijfplaats, een online-identificatiemiddel of een of meer specifieke elementen die kenmerkend zijn voor zijn fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit."[85]

Nadere lezing van beide bovenstaande definities laat zien dat de 'oude' definitie van persoonsgegeven slechts opgesplitst is in een simpele en korte definitie van persoonsgegeven en een meer uitgebreide definitie van betrokkene. Met dit verschil dat nu verduidelijkt is dat ook *gegevens over de verblijfplaats en een online-identificatiemiddel* kunnen bijdragen aan identificatie, alsmede genetische (niet in de Richtlijn genoemd) en mentale (in de Richtlijn psychische) kenmerken. Ook de zinsnede over de redelijkerwijs in te zetten middelen is niet nieuw gezien overweging 26 van Richtlijn 95/46/EG: '*alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is dan wel door enig ander persoon in te zetten zijn om genoemde persoon te identificeren.*' In deze zin, welke letterlijk is overgenomen in de Verordening, is het naar onze mening overigens vreemd dat het woord ´redelijkerwijs´ ziet op het inzetten van de middelen, en niet op de identificeerbaarheid.

Nader beschouwd is er wat betreft de definitie van persoonsgegevens – op wat verschuivingen van woorden daargelaten – dus niets veranderd in de Verordening ten opzichte van de Richtlijn. Het moment van hervorming is dus niet gegrepen om het begrip op papier strakker af te bakenen en de ruime uitleg zodoende in te dammen.

5.2 'Artikel 64-Werkgroep'

In informatieve documenten van de Europese Commissie over het waarom van de voorgestelde Verordening, worden – in lijn met de eerder besproken ruime uitleg door het Hof van Justitie – persoonsgegevens zelfs gedefinieerd als '*alle gegevens over een persoon die betrekking hebben op zijn of haar privé-, beroeps- of publieke leven.*'[86] Hoewel deze documenten formeel geen onderdeel uitmaken van de Verordening zelf, is het een indicatie van de zo mogelijk nog ruimere uitleg die met de nieuwe regelgeving gevolgd zal worden. Gezien de in feite ongewijzigde definitie van het begrip persoonsgegevens, is een volgende relevante vraag dan ook of er mogelijk wel wijzigingen plaats gaan vinden wat betreft de uitleg van dit begrip. De artikelsgewijze toelichting bij de Verordening geeft hier geen blijk van. Wel wordt gesproken over de vervanging van de Artikel 29-Werkgroep door een

[85] Art. 4 lid 2 Verordening.

[86] Europese Commissie, 'Waarom moeten we de EU-regels over gegevensbescherming hervormen?', Beschikbaar via: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_nl.pdf. Zie ook: MEMO/12/41, 'Data protection reform: Frequently asked questions', 25 januari 2012. Beschikbaar via: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=HTML&aged=0&language=EN&guiLanguage=en.

Europees Comité voor Gegevensbescherming (hierna ECvG), op te richten op grond van art. 64 Verordening. Aangezien de Werkgroep steeds een grote rol heeft gespeeld in de uitleg van het begrip persoonsgegevens zou deze vernieuwing een grote rol *kunnen* spelen in de toekomstige interpretatie van het begrip persoonsgegevens. Of dit ook het geval zal zijn valt echter nog te bezien. In de artikelsgewijze toelichting bij de Verordening[87] wordt aangegeven dat de taken van het ECvG gebaseerd zijn op art. 30 Richtlijn 95/46/EG, dat de taken van de Artikel 29-Werkgroep bepaalt. Daarnaast zal het ECvG zijn samengesteld uit steeds één vertegenwoordiger van de toezichthoudende autoriteit van elke lidstaat, een vertegenwoordiger van de Europese Toezichthouder en een vertegenwoordiger van de Commissie, net zoals de Artikel 29-Werkgroep is samengesteld. Gezien deze grote overeenkomsten tussen de Artikel 29-Werkgroep en het Comité zowel in taken als in samenstelling, lijkt het niet waarschijnlijk dat plotsklaps de uitleg van de kernbegrippen uit de regelgeving betreffende de verwerking van persoonsgegevens drastisch zal veranderen.

5.3 Toch een meer beperkte uitleg?

In het bovenstaande geschetste beeld van status-quo, is er één vreemde eend in de bijt. In overweging 24 van de Verordening wordt namelijk aangegeven dat het gebruik van onlinediensten sporen achter kan laten die kunnen worden gebruikt om profielen op te stellen en om personen te herkennen. Vervolgens wordt gesteld:

"Identificatienummers, locatiegegevens, online-identificatiemiddelen en andere specifieke factoren hoeven **dus** niet onder alle omstandigheden als persoonsgegevens te worden beschouwd." [nadruk toegevoegd]

Deze overweging staat in schril contrast met de opstelling van de Artikel 29-Werkgroep zoals hierboven beschreven. Waar in de opinie van de Artikel 29-Werkgroep nog gesteld werd dat bij onzekerheid over de herleidbaarheid van gegevens tot een identificeerbaar persoon er *dus* uitgegaan moet worden van persoonsgegevens, wordt hier gesteld dat deze gegevens die tot identificatie *kunnen* leiden, *dus* niet altijd persoonsgegevens zijn. Deze tegenstelling is ook de Werkgroep zelf opgevallen, want in zijn opinie ten aanzien van de Verordening[88] geeft hij aan dat overweging 24 van de Verordening te restrictief is wat betreft het begrip persoonsgegevens en verwijst hierbij naar zijn eerdere opinie over persoonsgegevens.[89] Ook in Opinie 08/2012 waarin de Artikel 29-Werkgroep nadere input geeft voor de discussie over de herziening van juridisch raamwerk betreffende persoonsgegevensbescherming wordt de

[87] COM(2012)11 (def.), onder 3.4.7.3, p. 15.
[88] Groep Gegevensbescherming Artikel 29, Opinion 01/2012 on the data protection reform proposals, 23 Maart 2012, WP 191, p. 9. Beschikbaar via: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.
[89] WP 136, p. 16.

noodzaak van een ruim concept persoonsgegevens benadrukt.[90] Ook in deze opinie suggereert de Artikel 29-Werkgroep dat als algemene regel geldt dat identificatienummers, locatiegegevens, online-identificatiemiddelen en andere specifieke factoren beschouwd moeten worden als persoonsgegevens. Het valt dus te bezien of overweging 24 van de voorgestelde Verordening in de herzieningsronden overeind blijft. Zelfs als dit het geval is moet nog bezien worden of dit daadwerkelijk de deur op een kiertje zet om meer tegemoet te komen aan de praktijk waar het onlinediensten betreft. Zowel het Europees Parlement als de Raad kunnen in eerste lezing, en later ook in tweede lezing, immers nog met wijzigingsvoorstellen komen, of het voorstel in de laatste lezing zelfs geheel blokkeren.[91]

6. Conclusies

De steeds ruimere uitleg van het begrip persoonsgegevens lijkt te zijn ingegeven door het idee van adequate bescherming van persoonsgegevens. Bij nadere bestudering roept deze ruime uitleg echter zowel vanuit conceptueel als vanuit praktisch perspectief de vraag op of dit doel daadwerkelijk wordt bereikt. Door een ruime uitleg van het begrip persoonsgegevens komt in de eerste plaats de ratio achter het recht op gegevensbescherming – de bescherming van fundamentele vrijheden en het waarborgen van een vrij verkeer van persoonsgegevens – in het gedrang. Niet alleen is het regime inmiddels van toepassing wanneer er helemaal geen sprake is van een inmenging in het privéleven, waardoor de relatie met privacy verloren is gegaan. Ook is het zeer waarschijnlijk dat een ruime toepasselijkheid van het recht op gegevensbescherming het vrije verkeer van deze gegevens eerder bemoeilijkt dan vereenvoudigd. In de tweede plaats blijkt de ruime uitleg van het begrip persoonsgegevens praktisch te leiden tot een situatie waarin wet en werkelijkheid niet meer stroken.

Door een ruim concept persoonsgegevens vallen ook gebruikelijke alledaagse handelingen onder het strikte beschermingsregime. Echter, doordat eenvoudig in strijd gehandeld wordt met het recht op gegevensbescherming gaat de geloofwaardigheid hiervan achteruit en is de kans aanwezig dat ook makkelijk na te leven principes in het gedrang komen. Het is een misvatting dat het anonimiseren van persoonsgegevens in deze situatie een uitkomst biedt. Onderzoek en enkele schrijnende praktijkvoorbeelden tonen aan dat anonimiseren praktisch

[90] Groep Gegevensbescherming Artikel 29, Opinion 08/2012 providing further input on the data protection reform discussions, Adopted on 05 October 2012, WP 199. Beschikbaar via: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf.

[91] Momenteel ligt het voorstel voor eerste lezing bij het Europees Parlement. Zie voor het verloop van het wetgevingstraject: www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=COM%282012%290011.

haast onmogelijk is, aangezien reeds eenvoudige combinaties tussen enkele triviale gegevens – die meer en meer op internet beschikbaar zijn – tot identificatie kunnen leiden.

Hoewel de voorgestelde Verordening voor de bescherming van persoonsgegevens geen wijzigingen met zich meebrengt wat betreft het begrip persoonsgegeven, lijkt overweging 24 van deze Verordening de deur toch op een kiertje te zetten om – wat betreft onlinediensten – iets meer met de praktijk mee te gaan doordat bepaalde gegevens niet altijd als persoonsgegevens gezien worden waar dat voorheen wel het geval was. De Artikel 29-Werkgroep heeft echter in zijn opinie betreffende de nieuwe Verordening al aangegeven deze overweging gewijzigd te willen zien, dus de vraag is of deze tegemoetkoming aan de praktijk niet in de kiem gesmoord gaat worden.

De oplossing van Schwarz en Solove om persoonsgegevens in verschillende categorieën te verdelen spreekt ons aan. Echter, een uitleg van het recht op gegevensbescherming in het licht van het recht op privacy biedt wat ons betreft wellicht een betere route om het uitdijende recht op gegevensbescherming te begrenzen. Hoewel deze weg met het Verdrag van Lissabon niet eenvoudig te bewandelen is, lijkt de post Lissabon-rechtspraak van het Hof van Justitie ruimte te bieden om privacy wel degelijk een rol te geven bij de interpretatie van het recht op gegevensbescherming.

De voorliggende verkenning van de gevolgen van een uitdijende reikwijdte van het concept persoonsgegevens is ingegeven door nader onderzoek dat momenteel wordt uitgevoerd naar de juridische aspecten van datamining in open bronnen. Een veelvoorkomend fenomeen, waarvan de legaliteit, mede vanuit het perspectief van privacy en gegevensbescherming – maar bijvoorbeeld ook vanuit het perspectief van auteursrecht – discutabel is. Door de zeer ruime uitleg van het begrip persoonsgegevens kwalificeert vrijwel elk stukje informatie op internet als persoonsgegeven, hetgeen, zoals hierboven geschetst, vrijwel niet kan worden opgelost door anonimiseren. Hierdoor is het juridische kader betreffende de verwerking van persoonsgegevens onverkort van toepassing op het gehele proces van datamining in open bronnen. Of, en zo ja in hoeverre, deze wetgeving praktisch gezien ook daadwerkelijk wordt nageleefd is interessant voor nader onderzoek. Onze hypothese in deze is dat hiervan niet of nauwelijks sprake zal zijn onder het mom van de voor de hand liggende redenering: *Alles wat in open bronnen staat is toch vrij te gebruiken…*