Privacy in het bestuursrecht

VAR VERENIGING VOOR BESTUURSRECHT

Preadviezen Jonge VAR 2015

mr. M.M.C. van Graafeiland &

mr. N.N. Bontje, mr. A. de Jong,

mr. M. Belhaj & mr. S. Gün

13

BJu Boom Juridische uitgevers

Jonge VAR-reeks
13

Privacy in het bestuursrecht

Preadviezen uitgebracht door

Mr. M.M.C. van Graafeiland en mr. N.N. Bontje
Mr. A. de Jong
Mr. M. Belhaj en mr. S. Gün

Voor de bijeenkomst
van de Jonge VAR
op 12-12-2014

Boom Juridische uitgevers
Den Haag
2015

Aanbevolen citeerwijze: Jonge VAR-reeks 13

ISBN 978-94-6290-044-8
ISBN 978-94-6274-269-7
NUR 823

www.bju.nl

Inhoud

Voorwoord

Op 12 december 2014 vond de jaarlijkse bijeenkomst van de Jonge VAR plaats in het kantoor van de landsadvocaat, Pels Rijcken & Droogleever Fortuijn. Het onderwerp van dit jaar was als altijd zeer actueel: privacy in het bestuursrecht. In dit boek zijn de preadviezen en een verslag van de bijeenkomst opgenomen.

Preadviseurs waren Marte van Graafeiland en Nina Bontje (Pels Rijcken & Droogleever Fortuijn), Arjan de Jong (ministerie van Binnenlandse Zaken en Koninkrijksrelaties) en Mohammed Belhaj en Sultan Gün (gemeente Amsterdam). De onderwerpen die in de preadviezen aan de orde komen, variëren van fundamentele vragen over Big Data, de gegevensverstrekking binnen verschillende nationale samenwerkingsverbanden en gegevensverstrekking door bestuursorganen aan buitenlandse counterparts. Met hun preadviezen leveren de auteurs een bijzondere bijdrage aan de discussie over privacy(regelgeving).

Met genoegen kijkt de VAR terug op de bijeenkomst van de Jonge VAR. Het verslag van de levendige discussie is opgetekend door Jo-Anne Nijland (Pels Rijcken & Droogleever Fortuijn). Het VAR-bestuur dankt de preadviseurs en de verslaglegger hartelijk voor hun inspanningen.

Ben Schueler,
Voorzitter van de VAR

Grensoverschrijdende gegevensuitwisseling en privacy

*Mr. M.M.C. van Graafeiland en mr. N.N. Bontje**

* Marte van Graafeiland en Nina Bontje zijn advocaat te Den Haag. Zij bedanken mr. C.M. Bitter en mr. drs. R.W. Veldhuis voor hun opmerkingen bij eerdere versies.

1 Grensoverschrijdende administratieve samenwerking in vogelvlucht

1.1 Inleiding

Grensoverschrijdende problemen vereisen een grensoverschrijdende aanpak. Een voorbeeld van een grensoverschrijdend probleem is een malafide webwinkel die vanuit Nederland consumenten in het buitenland oplicht, of een uit het BIG-register geschrapte arts die in het buitenland aan de slag wil. Ook kan worden gedacht aan een Nederlandse online aanbieder van kansspelen die zonder vergunning in andere landen kansspelen aanbiedt, aan een buschauffeur die zich over de grens niet aan de regels voor rusttijden houdt, of aan belastingheffing over eigendommen in het buitenland. In dergelijke gevallen is samenwerking tussen autoriteiten uit verschillende landen van groot belang voor een effectieve aanpak.

1.2 De verschillende varianten van grensoverschrijdende administratieve samenwerking

Er zijn grofweg drie vormen van grensoverschrijdende samenwerking, die van elkaar kunnen worden onderscheiden op basis van de mate waarin wordt samengewerkt.[1] De eerste en minst intensieve vorm is de uitwisseling van gegevens.[2] Die uitwisseling kan incidenteel plaatsvinden (spontaan of op verzoek van een buitenlandse autoriteit) of structureel (bijvoorbeeld door gegevens op te slaan in een gezamenlijke database). De tweede vorm van grensoverschrijdende samenwerking is toezicht op verzoek. Een autoriteit uit het ene land (de verzoekende autoriteit) vraagt dan een autoriteit uit het andere land (de aangezochte autoriteit) om haar toezichtbevoegdheden uit te oefenen ten behoeve van de verzoekende autoriteit. Bij deze vorm van samenwerking wordt onderscheid gemaakt tussen indirect toezicht op verzoek en direct toezicht op verzoek. Indirecte toezichtverzoeken betreffen meestal informatieverzoeken van een buitenlandse autoriteit, waarbij de aangezochte autoriteit eerst één of meerdere toezichthandelingen moet

1 In navolging van Boswijk e.a. in P. Boswijk e.a., *Transnationale samenwerking tussen toezichthouders in Europa*, Den Haag: WODC 2008, p. 29-30.

2 Strikt genomen vormt de uitwisseling van *best practices* de minst intensieve vorm van samenwerking. Die vorm laten wij buiten beschouwing, omdat in dat kader geen tot personen herleidbare gegevens worden uitgewisseld en ons preadvies juist op die uitwisseling betrekking heeft.

verrichten (bijvoorbeeld het vorderen van inlichtingen) om de desbetreffende informatie te kunnen verstrekken. Van directe toezichtverzoeken is sprake als een autoriteit door een buitenlandse autoriteit wordt verzocht om specifieke toezichthandelingen te verrichten, zoals het brengen van een bedrijfsbezoek aan een mogelijke overtreder die is gevestigd in het land van de aangezochte autoriteit. De derde en meest vergaande vorm van samenwerking tussen autoriteiten uit verschillende landen is grensoverschrijdend toezicht. Daarbij is een buitenlandse autoriteit op een of andere wijze betrokken bij een toezichtprocedure op het grondgebied van een ander land. Er moet een onderscheid worden gemaakt tussen onzelfstandig en zelfstandig grensoverschrijdend toezicht. Bij onzelfstandig grensoverschrijdend toezicht opereert de buitenlandse autoriteit onder leiding van de autoriteit van het land waar de toezichthandelingen worden verricht. Bij zelfstandig grensoverschrijdend toezicht opereert de buitenlandse autoriteit zelfstandig en voor eigen verantwoordelijkheid, maar met toestemming van het land in kwestie, in een ander land.[3]

In dit preadvies richten wij ons met name op de eerstgenoemde vorm van grensoverschrijdende samenwerking: de gegevensuitwisseling tussen autoriteiten uit verschillende landen. Daarbij speelt ook de tweede vorm van grensoverschrijdende samenwerking – het toezicht op verzoek – soms een rol, namelijk als de autoriteit toezichthandelingen verricht om te kunnen voldoen aan een informatieverzoek van een buitenlandse autoriteit. Wij hebben voor deze insteek gekozen, omdat zich vooral in dat kader privacyvraagstukken kunnen voordoen. Denk aan de situatie dat het voornemen bestaat gevoelige persoonsgegevens,[4] zoals strafrechtelijke gegevens, aan een buitenlandse autoriteit te verstrekken, of aan de situatie dat de gegevens die worden verstrekt voor andere doeleinden zijn verzameld dan waarvoor ze nu worden verstrekt.[5]

De vraag die in dit preadvies centraal staat, is met welke privacyaspecten Nederlandse autoriteiten nu en in de (nabije) toekomst voornamelijk rekening zullen moeten houden als zij persoonsgegevens aan autoriteiten in het buitenland willen verstrekken. De focus ligt daarbij op gegevensverstrekking door Nederlandse autoriteiten aan autoriteiten in andere landen, de zogenoemde horizontale samenwerking.[6] Wij beperken ons daarbij tot de zogeheten administratieve

3 Zie over grensoverschrijdend toezicht L. Michiels, 'Europese samenwerking bij bestuurlijk sanctioneren. Over (de noodzaak van) wederzijdse erkenning en tenuitvoerlegging van bestuursrechtelijke sancties en maatregelen in Europa', in: R.A.J. van Gestel & J. van Schooten (red.), *Europa & de toekomst van de nationale wetgever*, Nijmegen: Wolf Legal Publishers 2008, p. 178-179.

4 Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon (artikel 1 onder a van de Wet bescherming persoonsgegevens (Wbp)). Bijzondere persoonsgegevens zijn persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag (artikel 16 Wbp).

5 Zie hierover in de context van gegevensuitwisseling tussen Nederlandse toezichthouders A.J.C. de Moor-van Vugt e.a., *Gegevensuitwisseling door Toezichthouders*, Amsterdam: WODC 2012.

6 Verticale samenwerking, bijvoorbeeld tussen nationale autoriteiten en de Europese Commissie, valt buiten de reikwijdte van dit preadvies.

bijstand; op de privacyaspecten van internationale rechtshulp in strafzaken gaan wij niet in.

1.3 Aanpak

In hoofdstuk 2 beschrijven wij allereerst wat voor regelingen de grondslag vormen voor grensoverschrijdende gegevensuitwisseling door Nederlandse autoriteiten. Meer specifiek bekijken wij in hoeverre in die regelingen aandacht is besteed aan privacy. Wij stippen ook kort aan in hoeverre Nederlandse autoriteiten in de praktijk rekening houden met privacyregels als zij gegevens aan een buitenlandse autoriteit willen verstrekken. In hoofdstuk 3 wordt toegelicht met welke privacyregels met name rekening zal moeten worden gehouden als een Nederlandse autoriteit voornemens is persoonsgegevens aan een buitenlandse autoriteit te verstrekken. In hoofdstuk 4 toetsen wij of en, zo ja, in hoeverre die regels onder de voorgestelde Algemene Verordening Gegevensbescherming (AVG)[7] anders zullen zijn. In hoofdstuk 5 zetten wij tot slot onze belangrijkste bevindingen uiteen.

7 Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens betreffende het vrije verkeer van die gegevens (Algemene Verordening Gegevensbescherming), 25 januari 2012, COM(2012) 11. Waar in dit preadvies naar de AVG wordt verwezen, doelen wij op de ontwerp-AVG zoals is voorgesteld op 25 januari 2012, tenzij anders is vermeld.

2 Regelingen voor en praktijk van grensoverschrijdende gegevensuitwisseling

2.1 Inleiding

Wil verstrekking van (persoons)gegevens door een Nederlandse autoriteit aan een buitenlandse autoriteit mogelijk zijn, dan is daarvoor een grondslag nodig.[8] Die grondslag is c.q. wordt veelal gecreëerd in Europese verordeningen en in nationale wetgeving die al dan niet de implementatie vormt van een Europese richtlijn. Vaak wordt daarbij een onderscheid gemaakt tussen uitwisseling met lidstaten en met zogenoemde derde landen. Wij hebben een aantal van deze regelingen op privacyrechtelijke aspecten onderzocht.[9] Dat betreffen zowel Europese verordeningen als nationale wetgeving. De bevindingen lichten wij hierna toe. Ook stippen wij kort aan in hoeverre Nederlandse autoriteiten in de praktijk rekening houden met privacyregels als zij gegevens aan een buitenlandse autoriteit willen verstrekken.

2.2 Privacyrechtelijke bevindingen ten aanzien van regelingen voor grensoverschrijdende gegevensuitwisseling

Wat aan de (door ons onderzochte) Europese verordeningen opvalt, is de inconsistentie in de keuze om wel,[10] niet[11] of alleen ten aanzien van de bepaling over

8 De omstandigheid dat een grondslag nodig is voor internationale gegevensverstrekking volgt naar ons oordeel uit de algemene (artikel 2:5 Algemene wet bestuursrecht) en/of – indien van toepassing – uit de specifieke geheimhoudingsplicht van de betreffende Nederlandse autoriteit.

9 Een groot aantal Nederlandse autoriteiten kan of moet op de voet van één of meer van de door ons onderzochte regelingen gegevens aan buitenlandse autoriteiten verstrekken, waaronder de Autoriteit Consument en Markt (ACM), de Autoriteit Financiële Markten (AFM), de Belastingdienst, het College bescherming persoonsgegevens (CBP), De Nederlandsche Bank, de Inspectie Leefomgeving en Transport, de Nationale en Internationale Wegvervoer Organisatie, de Nederlandse Voedsel en Waren Autoriteit en de Sociale verzekeringsbank. Voor de regelingen die wij hebben onderzocht, verwijzen wij naar het overzicht dat wij aan het einde van ons preadvies hebben opgenomen. In het vervolg van dit preadvies zullen wij de daarin genoemde verordeningen aanduiden met het nummer dat de desbetreffende verordening in dat overzicht heeft gekregen.

10 Verordening 1 (artikel 4 lid 7 en artikel 14), verordening 3 (artikel 28 lid 4), verordening 4 (artikel 77), verordening 5 (artikel 84 lid 5 onder a), verordening 6 (artikelen 19 en 34) en verordening 8 (artikel 24).

11 Verordeningen 2, 7 en 10.

verstrekking van gegevens aan derde landen[12] te bepalen dat de privacyregelgeving in acht moet worden genomen. De achtergrond van deze inconsistentie is ons niet duidelijk. Ook verordeningen die géén bepalingen over het in acht nemen van de privacyregelgeving bevatten, zullen verwerking van persoonsgegevens tot gevolg kunnen hebben. Artikel 22 van verordening 7[13] – een van de verordeningen waarin niets over de verwerking van persoonsgegevens is bepaald – kent bijvoorbeeld de verplichting om alle beschikbare informatie aan andere lidstaten te verstrekken over inbreuken door niet-ingezetenen op de bepalingen over bemanning, rijtijden, onderbrekingen en rusttijden en de sancties die in dat verband jegens die niet-ingezetenen zijn toegepast. Een ander voorbeeld is artikel 24 van verordening 10,[14] op basis waarvan onder meer alle gegevens moeten worden verstrekt die nodig zijn om te kunnen verifiëren of de bepalingen inzake de bescherming van dieren tijdens het vervoer worden nageleefd.

Mogelijk leidt de hiervoor bedoelde inconsistentie in een concreet geval tot verwarring over het antwoord op de vraag of de privacyregelgeving moet worden betrokken bij de beoordeling om tot verstrekking van gegevens aan een buitenlandse autoriteit over te gaan. Wij achten die verwarring met name voorstelbaar in de situatie dat binnen één verordening ten aanzien van een deel van de verstrekkingsgrondslagen wel en ten aanzien van een ander deel niet wordt bepaald dat de privacyregelgeving in acht moet worden genomen.[15] Onze suggestie aan de Europese wetgever zou dan ook zijn om – in ieder geval binnen een en dezelfde verordening – op een eenduidige manier te bepalen of de privacyregelgeving in acht moet worden genomen.

Wellicht ten overvloede stellen wij nog vast dat de omstandigheid dat in een verordening níet is opgenomen dat de bepalingen over de bescherming van persoonsgegevens van toepassing zijn, niet maakt dat die bepalingen niet steeds in acht hoeven te worden genomen. Hetzelfde geldt voor de omstandigheid dat slechts ten aanzien van een deel van de verstrekkingsgrondslagen in de verordening is opgenomen dat de privacyregelgeving in acht moet worden genomen: indien en voor zover Nederlandse autoriteiten voornemens zijn om op basis van een Europese verordening persoonsgegevens aan een buitenlandse autoriteit te verstrekken, zullen zij moeten beoordelen of de Wbp niet aan die verstrekking in de weg staat.[16] Diezelfde beoordeling zal moeten plaatsvinden als het voornemen bestaat om op grond van nationale regelgeving persoonsgegevens aan buiten-

12 Verordening 9 (artikelen 34 en 36 tot en met 38 versus artikel 39).

13 Verordening (EG) 56/2006 van het Europees Parlement en de Raad van 15 maart 2006 tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer, tot wijziging van Verordeningen (EEG) nr. 3821/85 en (EG) nr. 2135/98 van de Raad en tot intrekking van Verordening (EEG) nr. 3820/85 van de Raad (PbEU 2006, L 102/1).

14 Verordening 1/2005 van de Raad van 22 december 2004 inzake de bescherming van dieren tijdens het vervoer en daarmee samenhangende activiteiten en tot wijziging van de Richtlijnen 64/432/EEG en 93/119/EG en van Verordening (EG) nr. 1255/97 (PbEU 2005, L 3/1).

15 Zie bijvoorbeeld verordening 9.

16 De Wbp vormt de implementatie van 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 (hierna: de Privacyrichtlijn). Autoriteiten uit andere lidstaten zullen een beoordeling moeten maken aan de hand van hun eigen – op de Privacyrichtlijn gebaseerde – regelgeving.

landse autoriteiten te verstrekken. Kijken we naar Nederlandse wettelijke bepalingen over het verstrekken van gegevens aan buitenlandse autoriteiten, dan valt op dat in dat verband niet één keer naar de Wbp wordt verwezen.[17] Een dergelijke bepaling zou ook niet nodig hoeven te zijn.

2.3 Privacyrechtelijke bevindingen ten aanzien van de praktijk van grensoverschrijdende gegevensuitwisseling

In het kader van dit preadvies hebben wij met verschillende toezichthoudende autoriteiten gesproken om een beeld te krijgen van de praktijk van grensoverschrijdende gegevensuitwisseling. Er blijkt bij bepaalde toezichthoudende autoriteiten regelmatig sprake te zijn van een zekere terughoudendheid bij de verstrekking van (persoons)gegevens. Die terughoudendheid heeft verschillende oorzaken. Allereerst kunnen de verschillende afdoeningssystemen van landen leiden tot terughoudendheid om gegevens te verstrekken. Op een bepaald toezichtsubject kan bijvoorbeeld in Nederland bestuursrechtelijk toezicht worden gehouden, terwijl dat toezicht in het buitenland strafrechtelijk is ingekleed. Het verstrekken van gegevens aan buitenlandse autoriteiten, wetende dat die gegevens daar kunnen worden gebruikt in een strafrechtelijke procedure, kan voor Nederlandse autoriteiten een reden zijn om de gevraagde gegevens niet te verstrekken.[18] Ook kan onduidelijkheid over wat er met de gegevens zal gebeuren of een negatieve uitkomst van een wederkerigheidstoets een reden zijn om geen informatie te verstrekken.[19] Meer praktische redenen die soms aan informatieverstrekking in de weg staan, zijn bijvoorbeeld communicatie- en taalproblemen en capaciteitsproblemen.[20]

Aarzelingen van privacyrechtelijke aard om informatie te verstrekken werden soms wel en soms niet genoemd. Als gezegd, zullen Nederlandse autoriteiten bij iedere verstrekking van persoonsgegevens aan een buitenlandse autoriteit echter wel de privacyregels in acht moeten nemen, onafhankelijk van het antwoord op de vraag of in de regeling waarin de verstrekkingsgrondslag is opgenomen wel of niet wordt opgemerkt dat de bepalingen over de bescherming van persoonsgegevens van toepassing zijn.

---

17 Zie bijvoorbeeld (artikel 37 van) de Dienstenwet, (artikel 7 van) de Instellingswet Autoriteit Consument en Markt (hierna: Instellingswet ACM), (artikel 61 lid 6 van) de Wbp, (artikelen 1:51 tot en met 1:51b en 1:65 van) de Wet op het financieel toezicht (Wft), (artikelen 5, 7 en 31 van) de Wet op de internationale bijstandsverlening bij de heffing van belastingen, en (artikel 18.20 van) de Telecommunicatiewet.

18 Die problematiek wordt door Luchtman besproken in zijn proefschrift. Daarin doet hij ook aanbevelingen ter oplossing van die problematiek. Zie M.J.J.P. Luchtman, *Grensoverschrijdende sfeercumulatie. Over de handhavingssamenwerking tussen financiële toezichthouders, fiscale autoriteiten en justitiële autoriteiten in EU-verband*, Nijmegen: Wolf Legal Publishers 2007.

19 Een wederkerigheidstoets houdt in dat de autoriteit slechts die informatie verstrekt die zij ook zou krijgen indien zij een vergelijkbaar verzoek aan de verzoekende autoriteit zou doen.

20 Wij noemen het IOSCO Multilaterale Memorandum of Understanding, waar effectentoezichthouders uit honderd landen (waaronder de AFM) bij zijn aangesloten, als voorbeeld van een constructie waarmee genoemde redenen voor terughoudendheid om gegevens te verstrekken goed lijken te worden geadresseerd.

3 De privacyrechtelijke regels voor grensoverschrijdende gegevensuitwisseling nu

3.1 Inleiding

Als een Nederlandse autoriteit persoonsgegevens aan een buitenlandse autoriteit wil verstrekken, waarmee moet dan rekening worden gehouden in de afweging of dat vanuit privacyrechtelijk perspectief is toegestaan? Wij noemen eerst de belangrijkste regels die uit de Wbp volgen. In het volgende hoofdstuk toetsen wij of en, zo ja, in hoeverre deze regels ook zullen gelden onder de AVG.

3.2 Grondslag voor de verstrekking: artikel 8 Wbp

Artikel 8 Wbp bepaalt dat persoonsgegevens alleen mogen worden verwerkt – daaronder begrepen het verstrekken van persoonsgegevens – als daarvoor een grondslag bestaat.[21] Indien en voor zover een Nederlandse autoriteit persoonsgegevens aan een buitenlandse autoriteit wil verstrekken, zal er naast een grondslag voor de internationale gegevensverstrekking als zodanig dus ook een grondslag moeten bestaan om persoonsgegevens te verstrekken.

Artikel 8 Wbp geeft een limitatieve opsomming van de grondslagen die als rechtvaardiging voor het verwerken van persoonsgegevens kunnen dienen. Bij de verstrekking van persoonsgegevens aan buitenlandse autoriteiten zullen met name de grondslagen onder c, e en f van belang zijn:

> 'Persoonsgegevens mogen slechts worden verwerkt indien:
> (…)
> c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
> (…)
> e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of
> f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de

21 Dit kan bijvoorbeeld ook worden afgeleid uit artikel 10 Grondwet en artikel 8 EVRM.

betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.'

In de memorie van toelichting bij artikel 8 Wbp is over onderdeel c opgemerkt dat de term 'wettelijke verplichting' betrekking heeft 'op iedere verplichting tot gegevensverwerking die krachtens een algemeen verbindend voorschrift wordt opgelegd' en een dergelijke verplichting 'alleen bij of krachtens een wet in formele zin in het leven kan worden geroepen (...)'.[22] Naar ons oordeel mag desondanks worden aangenomen dat ook een verplichting in het Europese recht kwalificeert als wettelijke verplichting in de zin van artikel 8 onder c Wbp. Ter ondersteuning van deze opvatting wijzen wij op het advies van de Article 29-Working Group[23] over artikel 7 Privacyrichtlijn, dat in artikel 8 Wbp is geïmplementeerd:

> 'It is also important to emphasise that Article 7(c) refers to the laws of the European Union or of a Member State. Obligations under the laws of third countries (...) are not covered by this ground.'[24]

Daarnaast wijzen wij op het equivalent van artikel 8 van de Wbp onder de Algemene Verordening Gegevensbescherming. Uit artikel 6 lid 3 AVG volgt, kort gezegd, dat de wettelijke verplichting moet zijn voorzien in EU-wetgeving of in de wetgeving van de lidstaat waaraan de voor de verwerking verantwoordelijke onderworpen is.

De conclusie dat ook een verplichting in het Europese recht kwalificeert als wettelijke verplichting in de zin van artikel 8 onder c Wbp is van belang, omdat de mogelijkheid om gegevens aan andere *lidstaten* te verstrekken in bijna alle (van de door ons onderzochte) Europese verordeningen wordt geformuleerd als een verplichting.[25] Dat geldt zowel als het gaat om gegevensverstrekking op verzoek, als wanneer zogenoemde spontane verstrekking aan de orde is. Voorbeelden van (veel) gebruikte formuleringen zijn: 'Een aangezochte instantie verstrekt', 'Op verzoek van de verzoekende autoriteit verstrekt de aangezochte autoriteit', 'Na ontvangst van een (...) verzoek zorgt de aangezochte bevoegde autoriteit ervoor dat', 'Wanneer een bevoegde autoriteit kennis neemt van (...) geeft zij de betreffende informatie onverwijld op eigen initiatief door', 'Wanneer een bevoegde autoriteit kennis krijgt van (...) stelt zij (...) in kennis' en 'De bevoegde autoriteiten (...) verstrekken elkaar'. In dit laatste voorbeeld wordt geen onderscheid gemaakt tussen bijstand op verzoek en bijstand op eigen initiatief. Dat is (in de door ons onderzochte verordeningen) eerder uitzondering dan regel. Die uitzondering doet zich ook voor in het volgende voorbeeld, waarbij de Europese

---

22 *Kamerstukken II* 1997/98, 25892, 3, p. 83.

23 De Article 29-Working Group is opgericht op grond van artikel 29 Privacyrichtlijn en heeft onder meer tot taak een uniforme toepassing van de principes uit de Privacyrichtlijn te bewerkstelligen. In de Working Group zijn de nationale privacytoezichthouders van de lidstaten vertegenwoordigd.

24 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 844/14/EN. WP217, p. 19.

25 Artikel 12 van verordening 2 en artikel 16 van verordening 3 vormen een uitzondering. Overigens bevat verordening 3 nog een aantal bepalingen waar verplichte verstrekking wél aan de orde is.

wetgever uitdrukkelijk(er) het verplichte karakter van de verstrekking aanduidt: 'De organen en de personen die onder deze verordening vallen, zijn (...) verplicht elkaar inlichtingen te verstrekken (...).'[26]

De bepalingen uit verordeningen over betrekkingen met *derde landen* zijn steeds op dezelfde manier opgebouwd. Enerzijds wordt een verplichting gecreëerd om informatie die van derde landen is ontvangen onder omstandigheden aan andere lidstaten te verstrekken. Dit sluit aan bij de conclusie die wij zojuist al trokken: er is bijna altijd sprake van een als verplichting geformuleerde grondslag voor de verstrekking van gegevens aan een andere lidstaat. Anderzijds wordt er een bevoegdheid gecreëerd om onder omstandigheden informatie die in het kader van de desbetreffende verordening is ontvangen, *aan* een derde land te verstrekken.[27]

Wij zien dit beeld terug in de nationale wetgeving. Ook daar is in het gros van de gevallen sprake van een verplichting tot verstrekking aan andere *lidstaten*.[28] De grondslag voor verstrekking van informatie aan *derde landen* wordt daarentegen bijna altijd als een bevoegdheid geformuleerd.[29]

Uit het voorgaande volgt dat voor de verstrekking van informatie door een Nederlandse autoriteit aan andere lidstaten vaak een grondslag gevonden zal kunnen worden gevonden in artikel 8 onder c Wbp, namelijk als het Europese recht of de nationale wet een verplichting in het leven roept om bepaalde gegevens aan andere lidstaten te verstrekken.

Is sprake van een verstrekkingsbevoegdheid, dan is een nadere afweging onder artikel 8 Wbp vereist. In die gevallen zal van belang zijn of de verstrekking door de Nederlandse autoriteit aan de buitenlandse autoriteit noodzakelijk is voor de vervulling van de publiekrechtelijke taak van de Nederlandse autoriteit. Als dat zo is, dan zal een grondslag gevonden kunnen worden in artikel 8 onder e Wbp.[30]

---

26 Artikel 76 lid 4 van verordening 4.

27 Zie artikel 14 van verordening 1, artikel 32 van verordening 3, de artikelen 19 tot en met 22 van verordening 6 en artikel 39 van verordening 9.

28 Zie artikel 37 Dienstenwet, artikel 61 lid 6 Wbp, de artikelen 1:51 tot en met 1:51b Wft, de artikelen 5 en 7 lid 1 Wet op de internationale bijstandsverlening bij de heffing van belastingen (in artikel 5 wordt gesproken over (het bredere) 'staat'), en artikel 18.20 Telecommunicatiewet. Een uitzondering wordt gevormd door artikel 7 Instellingswet ACM. Dat artikel bevat een bevoegdheid, maar spreekt over 'een buitenlandse instelling'. Er wordt dus geen onderscheid gemaakt tussen lidstaten en derde landen. Ook artikel 7 lid 2 en artikel 31 Wet op de internationale bijstandsverlening bij de heffing van belastingen bevatten een bevoegdheid, maar ook in deze artikelen wordt het onderscheid lidstaat/derde land niet gemaakt. Het gaat daar over 'staat'.

29 Zie artikel 7 Instellingswet ACM, artikel 1:65 Wft, en artikel 7 lid 2 en artikel 31 lid 2 Wet op de internationale bijstandsverlening bij de heffing van belastingen. Een uitzondering wordt gevormd door artikel 5 Wet op de internationale bijstandsverlening bij de heffing van belastingen, dat een verstrekkingsverplichting bevat jegens een 'verzoekende staat'.

30 Zie in dit verband bijvoorbeeld artikel 39 lid 2 van verordening 9: 'Indien het derde land wettelijk kan garanderen dat het de bijstand die nodig is om bewijsmateriaal te verzamelen inzake klaarblijkelijke of vermeende inbreuken op de relevante wetgeving inzake diervoeders en levensmiddelen, kan bieden, kan de informatie die in de context van deze verordening is verzameld, aan dat derde land worden medegedeeld, op voorwaarde dat de bevoegde autoriteiten die de

De gedachte zou ook kunnen zijn dat het de gemeenschappelijke (publiekrechtelijke) taak van de verschillende autoriteiten binnen de Europese Unie – waaronder de Nederlandse autoriteit – is om inbreuken op het EU-recht te voorkomen.[31] Een soortgelijke vlieger gaat wellicht evenzeer op bij de verstrekking aan een counterpart in een derde land, mits de verstrekking (dus) plaatsvindt ten behoeve van de uitoefening van een soortgelijke taak als waarmee de Nederlandse autoriteit is belast.[32] Kan geen grondslag worden gevonden in artikel 8 onder e Wbp, dan zal beoordeeld moeten worden of er, kort gezegd, sprake is van een gerechtvaardigd belang dat zwaarder weegt dan het belang van de betrokkene (artikel 8 onder f Wbp). Wij denken in algemene zin dat veelal wel een grondslag in een van de beide onderdelen (e of f) gevonden zal kunnen worden. Zou dat anders zijn, dan zou dat de wonderlijke consequentie hebben dat de (Europese of nationale) wetgever enerzijds een nadrukkelijke bevoegdheid heeft gecreëerd om gegevens – waaronder ook persoonsgegevens worden begrepen – te verstrekken, terwijl aan de andere kant van deze bevoegdheid veelal geen gebruik zou kunnen worden gemaakt als de te verstrekken informatie persoonsgegevens bevat.

De verstrekking van de persoonsgegevens zal wel steeds noodzakelijk moeten zijn ter verwezenlijking van het doel waarmee zij worden verstrekt: het voldoen aan de wettelijke verplichting (onderdeel c), de goede vervulling van de publiekrechtelijke taak (onderdeel e) of de verwezenlijking van het gerechtvaardigde belang (onderdeel f). Is verstrekking van persoonsgegevens daarvoor niet nodig, dan zullen die gegevens ook niet mogen worden verstrekt. Wel zou dat in dat geval in geanonimiseerde vorm kunnen, wat betekent dat uit de wel verstrekte gegevens niet kan worden afgeleid om welke natuurlijke persoon of personen het gaat.[33] Daarbij moet overigens wel gewaarborgd zijn dat de buitenlandse autoriteit de gegevens ook niet kan herleiden door ze te combineren met gegevens die deze zelf al heeft.

3.3 (On)verenigbaar gebruik: artikel 9 Wbp

Onder omstandigheden zal ook met artikel 9 Wbp rekening moeten worden gehouden. Het eerste lid van dit artikel bepaalt dat persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. In het tweede lid is een niet-limitatieve opsomming gegeven

---

informatie hebben verstrekt, daarvoor toestemming geven, in overeenstemming met de wetgeving inzake het verstrekken van persoonsgegevens aan derde landen.'

31 Zie ook artikel 7 onder e Privacyrichtlijn, dat in artikel 8 onder e Wbp is geïmplementeerd: 'De Lid-Staten bepalen dat de verwerking van persoonsgegevens slechts mag geschieden indien: (...) e. de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de voor de verwerking verantwoordelijke of de derde aan wie de gegevens worden verstrekt, drager is opgedragen.'

32 Vergelijk in dit verband artikel 1:65 jo. artikel 1:90 Wft, waaruit kan worden afgeleid dat een (van de) voorwaarde(n) voor verstrekking van gegevens aan derde landen is dat het beoogde gebruik door het derde land past in het kader van het toezicht op financiële markten of op personen die op die markten werkzaam zijn.

33 *Kamerstukken II* 1997/98, 25892, 3, p. 47-50.

van de omstandigheden waarmee bij de beoordeling of van (on)verenigbaar gebruik sprake is, rekening moet worden gehouden. Het gaat om:

'a. de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen;
b. de aard van de betreffende gegevens;
c. de gevolgen van de beoogde verwerking voor de betrokkene;
d. de wijze waarop de gegevens zijn verkregen en
e. de mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.'

Als het voornemen bestaat om persoonsgegevens aan een buitenlandse autoriteit te verstrekken, dan zal, gelet op artikel 9 Wbp, eerst moeten worden nagegaan of het daarbij gaat om gegevens die de verstrekkende Nederlandse autoriteit in eerste instantie ten behoeve van zichzelf heeft vergaard, of dat de persoonsgegevens – bijvoorbeeld in het kader van het in hoofdstuk 1 omschreven toezicht op verzoek – speciaal ten behoeve van de buitenlandse autoriteit zijn verzameld. In het laatste geval zal de voorgenomen verstrekking niet aan artikel 9 Wbp hoeven te worden getoetst, omdat van een zogenoemde verdere verwerking dan geen sprake is. Het doel waarmee de gegevens zijn vergaard, is gelijk aan het doel dat de beoogde verstrekking dient: het kunnen beantwoorden aan een informatieverzoek van de buitenlandse autoriteit.

Bestaat het voornemen gegevens te verstrekken die de Nederlandse autoriteit in eerste instantie ten behoeve van zichzelf heeft vergaard – die situatie zal zich bijvoorbeeld vaak bij beoogde spontane verstrekkingen voordoen –, dan zal onder omstandigheden moeten worden beoordeeld of sprake is van (on)verenigbaar gebruik. Die beoordeling hoeft naar ons oordeel niet plaats te vinden als sprake is van een wettelijke *verplichting* om gegevens te verstrekken. In dat geval is door de wetgever al een afweging gemaakt. De verstrekking aan een buitenlandse autoriteit strekt er in dat geval toe om aan een wettelijke verplichting te voldoen.

Bij een verstrekkings*bevoegdheid* zal naar ons oordeel in beginsel wel aan artikel 9 Wbp moeten worden getoetst. Als er in het kader van die verstrekkingsbevoegdheid echter een mogelijkheid bestaat om de gegevens te vorderen ten behoeve van de buitenlandse autoriteit,[34] dan zal er naar ons oordeel veelal van uit kunnen worden gegaan dat van onverenigbaar gebruik geen sprake is. Waren de gegevens – die nu toevallig al onder de desbetreffende autoriteit berusten – vergaard naar aanleiding van een informatieverzoek van een buitenlandse autoriteit, dan zou de beoogde verstrekking immers überhaupt niet aan artikel 9 Wbp getoetst hoeven te worden. Het zou vreemd zijn als de toevalligheid dat een autoriteit al over die gegevens beschikt, zou maken dat artikel 9 Wbp aan de verstrekking in de weg zou kunnen staan.

Als sprake is van een verstrekkingsbevoegdheid waar géén vergaarmogelijkheid aan is gekoppeld, zal onverenigbaar gebruik wel aan de orde kunnen zijn. In dat geval kan artikel 43 Wbp uitkomst bieden. Artikel 9 Wbp kan op grond van dit

34 Zie in dit verband bijvoorbeeld artikel 1:65 jo. artikel 1:68 Wft en artikel 7 lid 2 jo. artikel 8 lid 1 en 2 Wet op de internationale bijstandsverlening bij de heffing van belastingen.

artikel buiten toepassing worden gelaten voor zover dit noodzakelijk is in het belang van:

'a. de veiligheid van de staat;
b. de voorkoming, opsporing en vervolging van strafbare feiten;
c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of
e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen'.

Goed denkbaar is dat met name de uitzonderingen achter c en d onder omstandigheden een grondslag zullen kunnen bieden om artikel 9 Wbp buiten toepassing te laten. Moet wel een afweging op grond van artikel 9 Wbp worden gemaakt, dan kan daarbij een rol spelen of de buitenlandse autoriteit is belast met de toepassing van dezelfde regels of van regels op dezelfde gebieden als waarmee de Nederlandse autoriteit is belast, en of ook alleen in dat verband gegevens worden verstrekt.[35] Als dit zo is, zal snel(ler) sprake zijn van een sterke verwantschap tussen het doel waarvoor de gegevens zijn verkregen en het doel van de beoogde verstrekking (artikel 9 lid 2 onder a Wbp). Ten aanzien van het criterium achter c (gevolgen voor de betrokkene) merken wij in dit verband nog op dat de verstrekking er veelal toe dient de naleving en handhaving van het recht te bevorderen en dat daaraan vaak gewicht toegekend zal kunnen worden. Ten aanzien van het criterium achter e (passende waarborgen) kan bijvoorbeeld van belang zijn of (op grond van de verstrekkingsregeling) moet worden gewaarborgd dat de informatie niet voor een ander doel wordt gebruikt dan waarvoor deze is verstrekt en dat geheimhouding ten aanzien van de ontvangen informatie wordt betracht. Uiteindelijk zal het afhankelijk zijn van de omstandigheden van het geval hoe de toetsing moet uitvallen. Wij gaan daar dan ook niet verder op in.

3.4 Bijzondere persoonsgegevens

Van belang is verder dat voor de verwerking van zogenoemde bijzondere persoonsgegevens, zoals strafrechtelijke persoonsgegevens, een strikter regime geldt: verwerking daarvan is op grond van artikel 16 Wbp verboden, tenzij sprake is van een van de in de artikelen 17 tot en met 23 Wbp genoemde uitzonderingsgronden die dit verbod kunnen doorbreken. De artikelen 17 tot en met 22 Wbp

35 Hier zou, gelet op de niet op de privacyregelgeving toegespitste woorden 'de toezichthoudende autoriteiten van de andere lidstaten van de Europese Unie' in artikel 61 lid 6 Wbp, ten aanzien van verstrekking door het CBP twijfel over kunnen bestaan. Die twijfel wordt echter weggenomen door lezing van artikel 28 Privacyrichtlijn. Dat artikel heeft als titel 'toezichthoudende autoriteit'. Elke lidstaat moet ingevolge artikel 28 lid 1 bepalen dat 'een of meer autoriteiten worden belast met het toezicht op de toepassing op zijn grondgebied van de ter uitvoering van *deze richtlijn* (...) vastgestelde bepalingen' (onze cursivering). Artikel 61 lid 6 Wbp vormt blijkens de memorie van toelichting de implementatie van artikel 28 lid 6 Privacyrichtlijn (*Kamerstukken II* 1997/98, 25892, 3, p. 183).

bevatten uitzonderingsgronden die zijn toegesneden op een bepaalde categorie van bijzondere persoonsgegevens. Artikel 23 Wbp bevat een aantal uitzonderingsgronden die voor alle categorieën van bijzondere persoonsgegevens gelden.

Voor zover wij kunnen overzien, zullen de specifieke uitzonderingsgronden in de artikelen 17 tot en met 21 Wbp bij het voornemen om bijzondere persoonsgegevens aan een buitenlandse autoriteit te verstrekken, veelal geen rol van betekenis kunnen spelen. Ten aanzien van artikel 22 Wbp – dat de gronden bevat voor doorbreking van het verbod om strafrechtelijke persoonsgegevens te verwerken[36] – zou dat anders kunnen liggen. Wij wijzen in dit verband op artikel 22 lid 6 Wbp:

> 'Het verbod is niet van toepassing op verwerkingen van strafrechtelijke gegevens door en ten behoeve van publiekrechtelijke samenwerkingsverbanden van verantwoordelijken of groepen van verantwoordelijken indien de verwerking noodzakelijk is voor de uitvoering van de taak van deze verantwoordelijken of groepen van verantwoordelijken en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.'

Bij een publiekrechtelijk samenwerkingsverband moet blijkens de memorie van toelichting worden gedacht aan een samenwerkingsverband dat wordt beheerst door regels van publiekrecht en dat bestaat uit hetzij bestuursorganen, hetzij privaatrechtelijke vormgegeven organen die bij of krachtens de wet zijn belast met een publiekrechtelijke taak.[37] Als een Nederlandse autoriteit samenwerkt met buitenlandse autoriteiten die dezelfde regels uitvoeren c.q. die regels toepassen op dezelfde gebieden als waarmee de Nederlandse autoriteit is belast, dan kunnen wij ons voorstellen dat ook deze samenwerking kan kwalificeren als een samenwerkingsverband in de zin van artikel 22 lid 6 Wbp. De verwerking van strafrechtelijke gegevens moet dan wel noodzakelijk zijn voor de uitvoering van de taak van het samenwerkingsverband, en bij de uitvoering moet zijn voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Dat wil zeggen dat er altijd voldaan zal moeten zijn aan de eisen van proportionaliteit en subsidiariteit en dat er binnen het samenwerkingsverband regels worden opgesteld over beveiliging van gegevens en systemen, over verwijdering van gegevens en over de overige eisen die de

---

36 'Het begrip "strafrechtelijke gegevens" heeft betrekking zowel op veroordelingen als op min of meer gegronde verdenkingen. Veroordelingen betreffen gegevens waarbij de rechter, al dan niet onherroepelijk, strafrechtelijk gedrag heeft vastgesteld. Bij verdenkingen gaat het om concrete aanwijzingen jegens een bepaalde persoon. Het begrip strafrechtelijk gegevens omvat mede gegevens omtrent de toepassing van het formele strafrecht, bijvoorbeeld het gegeven dat iemand is gearresteerd of dat tegen hem proces-verbaal is opgemaakt wegens een bepaald vergrijp.' Zie *Kamerstukken II* 1997/98, 25892, 3, p. 118. Zie ook HR 29 mei 2009, ECLI:NL:HR:2009:BH4720, r.o. 4.4.

37 Zie *Kamerstukken II* 2008/09, 31841, 3, p. 9. Een goed voorbeeld hiervan is een zogenoemd Regionaal Informatie- en Expertise Centrum (RIEC). Een RIEC heeft tot doel om georganiseerde criminaliteit te bestrijden. Samenwerkingspartners zijn bijvoorbeeld gemeenten, het Openbaar Ministerie, de politie en de Belastingdienst. In het preadvies van mr. M. Belhaj en mr. S. Gün wordt aandacht besteed aan de uitwisseling van persoonsgegevens binnen een RIEC.

Wbp stelt.[38] Voorts moet worden bedongen dat gegevens niet voor andere doeleinden, zoals strafvorderlijke doeleinden, mogen worden gebruikt.[39]

De Wbp bevat als gezegd ook een bepaling met een aantal uitzonderingsgronden die voor alle categorieën van bijzondere persoonsgegevens gelden, te weten artikel 23 Wbp. Het eerste lid van dit artikel bepaalt:

> 'Onverminderd de artikelen 17 tot en met 22 is het verbod om persoonsgegevens als bedoeld in artikel 16, te verwerken niet van toepassing voor zover:
> a. dit geschiedt met uitdrukkelijke toestemming van de betrokkene;
> b. de gegevens door de betrokkene duidelijk openbaar zijn gemaakt;
> c. dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte;
> d. dit noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of van een derde en het vragen van diens uitdrukkelijke toestemming onmogelijk blijkt;
> e. dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting of
> f. dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het College ontheffing heeft verleend. Het College kan bij de verlening van ontheffing beperkingen en voorschriften opleggen;
> g. de gegevens worden verwerkt door het College of een ombudsman als bedoeld in artikel 9:17 van de Algemene wet bestuursrecht en dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, voor de uitvoering van de hun wettelijk opgedragen taken en bij die uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.'

Er zal in het concrete geval getoetst moeten worden of een van de hiervoor genoemde uitzonderingsgronden van toepassing is. De gronden achter a tot en met d zullen naar ons oordeel (veelal) geen uitkomst kunnen bieden. Voor de grond achter g geldt hetzelfde, tenzij het gaat om een verstrekking van bijzondere gegevens aan een buitenlandse autoriteit door het CBP die plaatsvindt ter uitvoering van de eigen wettelijke taken. De onderdelen e (volkenrechtelijke verplichting) en f (bij wet bepaald) verdienen bijzondere aandacht.

Onderdeel e zal een grondslag kunnen bieden als sprake is van een verstrekkingsverplichting die in een *Europese verordening* is opgenomen. Een verplichting die voortvloeit uit een Europese verordening kwalificeert namelijk als een volkenrechtelijke verplichting als bedoeld in artikel 23 lid 1 onder e Wbp. Wij wijzen in dit verband op een passage in de parlementaire geschiedenis van de wijziging van de Wet personenvervoer 2000 ter uitvoering van, onder meer, verordening 8:[40] 'De grondslag voor de verwerking van de onder stroom 1 bedoelde gegevens is

38 Zie *Kamerstukken II* 2008/09, 31841, 3, p. 10.

39 Zou dat niet worden bedongen, dan zou dat bijvoorbeeld tot gevolg kunnen hebben dat buiten het (verdrags)kader dat voor internationale rechtshulp in strafzaken geldt, strafrechtelijke persoonsgegevens worden uitgewisseld.

40 Verordening 1071/2009 van het Europees Parlement en de Raad van 21 oktober 2009 tot vaststelling van gemeenschappelijke regels betreffende de voorwaarden waaraan moet zijn voldaan om het beroep van wegvervoerondernemer uit te oefenen en tot intrekking van Richtlijn 96/26/EG van de Raad (*PbEU* 2009, L 300/51).

artikel 23, eerste lid, onder e, Wbp: de noodzaak om gevoelige (strafrechtelijke) gegevens te verwerken ter voldoening aan een volkenrechtelijke verplichting. Het verwerken van een strafrechtelijk gegeven is daarom geoorloofd indien daarmee wordt gehandeld ingevolge de verplichting op grond van een Europese verordening (hier: toetsing van de Europese eis van betrouwbaarheid) en deze verplichting noodzaakt tot het verwerken van bepaalde gevoelige gegevens. Daarbij moet ook steeds sprake zijn van een "algemeen zwaarwegend belang".'[41]

Onderdeel e biedt geen grondslag voor de verstrekking van bijzondere persoonsgegevens als die verstrekking plaatsvindt op grond van een verstrekkingsverplichting die in *een nationale wet* is opgenomen; dan is geen sprake van een volkenrechtelijke verplichting. Hetzelfde geldt voor een verstrekking die wordt gebaseerd op een (Europese of nationale) verstrekkingsbevoegdheid. De vraag die dan rijst is of het verbod om bijzondere persoonsgegevens te verwerken – en dus te verstrekken – kan worden doorbroken met een beroep op artikel 23 lid 1 onder f Wbp. De verwerking zal daarvoor noodzakelijk moeten zijn met het oog op een zwaarwegend algemeen belang, er moeten passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en 'dit' moet bij wet zijn bepaald. Uit de memorie van toelichting blijkt dat het verwerken van de bijzondere persoonsgegevens als zodanig formeel wettelijk moet zijn geregeld.[42] In de door ons onderzochte regelingen wordt veelal bepaald dat gegevens aan een buitenlandse autoriteit moeten of mogen worden verstrekt. De vraag is of dat voldoende specifiek is. Wij menen dat onder omstandigheden ook ruimte bestaat voor verstrekking van bijzondere persoonsgegevens, omdat er nu juist een specifieke verplichting/bevoegdheid in het leven wordt geroepen om (persoons)gegevens te verstrekken. Daar kunnen – afhankelijk van het antwoord op de vraag of uitwisseling van bijzondere persoonsgegevens in het specifieke kader onvermijdelijk en (dus) geïmpliceerd is – naar ons oordeel ook bijzondere persoonsgegevens onder vallen. Volstrekt helder is dit niet, terwijl die helderheid juist bij de verwerking van bijzondere persoonsgegevens verwacht zou mogen worden. Het zou daarom aanbeveling verdienen dat de (Europese en nationale) wetgever er – bijvoorbeeld in de toelichting bij de desbetreffende verstrekkingsbepaling – expliciet aandacht aan besteedt of de desbetreffende bepaling ook een verplichting of bevoegdheid in het leven roept om bijzondere persoonsgegevens te verstrekken.

Wij concluderen dat het verbod op verstrekking van bijzondere persoonsgegevens in ieder geval zal kunnen worden doorbroken als het voornemen om die gegevens

41 *Kamerstukken II* 2011/12, 33184, 9, p. 3. Zie ook p. 2: 'Daarnaast is het verbod van artikel 16 Wbp niet van toepassing indien de verwerking van strafrechtelijke gegevens noodzakelijk is ter uitvoering van een volkenrechtelijke verplichting (artikel 23, eerste lid, onder e, Wbp), zoals Europese verordeningen.'

42 Zie *Kamerstukken II* 1997/98, 25892, 3, p. 124: 'De zinsnede "bij wet bepaald" brengt met zich dat de verwerking van een gevoelig gegeven alleen mogelijk is indien bij formele wet daarin is voorzien. Dit betekent dat een zodanige verwerking in de WBP of in een formele wet uitdrukkelijk moet zijn geregeld.' En: 'Indien de wetgever van oordeel is dat een bepaalde verwerking noodzakelijk is met het oog op een algemeen zwaarwegend algemeen belang en voor een zodanige verwerking een uitdrukkelijke wettelijke basis creëert, behoeft bij de toepassing van de regeling niet steeds opnieuw in concreto aan de betreffende norm te worden getoetst.'

te verstrekken is gebaseerd op een verstrekkingsverplichting in een Europese verordening. In dat geval biedt artikel 23 lid 1 onder e Wbp de grondslag voor de doorbreking. Of het verbod ook kan worden doorbroken als sprake is van een nationale verstrekkingsverplichting – die nota bene vaak een uitvloeisel vormt van een Europese richtlijn – of van een Europese of nationale verstrekkingsbevoegdheid, is minder zeker. Is het verbod eenmaal doorbroken, dan moet de verstrekking vervolgens nog wel aan de overige eisen van de Wbp worden getoetst. Er moet bijvoorbeeld worden beoordeeld of voor de verstrekking een grondslag kan worden gevonden in artikel 8 Wbp en – onder omstandigheden – of geen sprake is van onverenigbaar gebruik (artikel 9 Wbp).

3.5 Verstrekking aan derde landen

Bestaat het voornemen om gegevens aan een derde land te verstrekken, dan moet ook acht worden geslagen op de artikelen 76 tot en met 78 Wbp. Er zal eerst beoordeeld moeten worden of het derde land een passend beschermingsniveau waarborgt. Is dat niet zo, dan verbiedt artikel 76 lid 1 Wbp dat aan dat land persoonsgegevens worden verstrekt.[43] Het beoordelingskader is opgenomen in artikel 76 lid 3 Wbp:

> 'Het passend karakter van het beschermingsniveau wordt beoordeeld gelet op de omstandigheden die op de doorgifte van gegevens of op een categorie gegevensdoorgiften van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde of de doeleinden en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectoriële rechtsregels die in het betrokken derde land gelden, alsmede de regels van het beroepsleven en de veiligheidsmaatregelen die in die landen worden nageleefd.'

Het gaat hierbij niet om een beoordeling van de wetgeving in een derde land in het algemeen, maar om de vraag of voor (de verwerking van) de desbetreffende gegevens een passend beschermingsniveau kan worden geboden.[44] De beoordeling moet door de verantwoordelijke (lees: de Nederlandse autoriteit die voornemens is om persoonsgegevens aan een autoriteit in een derde land te verstrekken) worden gemaakt. Een van de voornaamste elementen waarmee rekening moet worden gehouden is het bestaan van een EU-rechtelijk besluit over het beschermingsniveau in het desbetreffende derde land.[45] Als er een positief besluit van de Europese Commissie bestaat met betrekking tot het beschermingsniveau in het desbetreffende derde land, dan heeft de verantwoordelijke in beginsel[46] zekerheid over het rechtmatige karakter van de doorgifte, mits wordt voldaan aan eventuele

43 Persoonsgegevens kunnen wel naar een land buiten de Europese Unie worden doorgegeven indien dat land partij is bij de op 2 mei 1992 te Porto totstandgekomen Overeenkomst betreffende de Europese Economische Ruimte (*Trb.* 1992, 132), tenzij uit een besluit van de Commissie van de Europese Gemeenschappen of de Raad van de Europese Unie voortvloeit dat deze doorgifte is beperkt of verboden (artikel 76 lid 2 Wbp).

44 *Kamerstukken II* 1997/98, 25892, 3, p. 193.

45 Zie artikel 78 lid 3 Wbp.

46 Zie artikel 78 lid 4 en 5 Wbp.

voorwaarden die de Commissie in haar besluit heeft gesteld.[47] Als er geen beslissing is genomen op EU-niveau, dan moet de Nederlandse autoriteit de specifieke omstandigheden van het geval zelf beoordelen aan de hand van de in artikel 76 lid 2 Wbp omschreven criteria.[48]

Als blijkt dat geen sprake is van een passend beschermingsniveau, dan wil dat niet zeggen dat de doorgifte van gegevens absoluut verboden is. Er zullen in dat geval toch persoonsgegevens doorgegeven kunnen worden als (artikel 77 lid 1 Wbp):

'a. de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven;
b. de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de doorgifte noodzakelijk is voor de sluiting of uitvoering van een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst;
d. de doorgifte noodzakelijk is vanwege een zwaarwegend algemeen belang, of voor de vaststelling, de uitvoering of de verdediging in rechte van enig recht;
e. de doorgifte noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene, of
f. de doorgifte geschiedt vanuit een register dat bij wettelijk voorschrift is ingesteld en dat door een ieder dan wel door iedere persoon die zich op een gerechtvaardigd belang kan beroepen, kan worden geraadpleegd, voor zover in het betrokken geval is voldaan aan de wettelijke voorwaarden voor raadpleging;
g. gebruik wordt gemaakt van een modelcontract als bedoeld in artikel 26, vierde lid, van richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie 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 L 281).'

---

47 Zie p. 14 van de de *Nota derde landen. De doorgifte van persoonsgegevens naar derde landen in het kader van de WBP*, Den Haag: College bescherming persoonsgegevens 2003 (hierna: *Nota derde landen* van het CBP), en *Handelingen I* 1999/2000, 34, p. 1625. De Europese Commissie heeft op het moment van schrijven een beslissing genomen over het beschermingsniveau in Andorra, Argentinië, Australië, Canada, Færöer Eilanden, Guernsey, Isle of Man, Israël, Jersey, Nieuw-Zeeland, Verenigde Staten (Passenger Name Record: informatie van vliegtuigpassagiers doorgegeven aan de United States Bureau of Customs and Border Protection Uruguay en Safe Harbour; er wordt alleen een passend beschermingsniveau geboden door de bedrijven en andere organisaties die zich hebben verplicht tot het toepassen van de zogenoemde Safe Harbour-regels; in de Verenigde Staten bestaat geen algemene wetgeving voor de bescherming van persoonsgegevens; actuele informatie over de Safe Harbour-regeling en de actuele lijst van ondernemingen die het systeem toepassen is te vinden op: www.export.gov/safeharbor/) en Zwitserland. Zie voor de beslissingen van de Commissie: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-2. Het toepassingsgebied van een beslissing kan variëren. Zo kan deze voor een heel land gelden (bijvoorbeeld Zwitserland), voor een groep verantwoordelijken die een specifiek stelsel volgen (bijvoorbeeld Safe Harbour-regeling) of voor een bepaald deel van de wetgeving (bijvoorbeeld Canada).

48 Daarbij kan bijvoorbeeld gebruik worden gemaakt van de hiervoor bedoelde *Nota derde landen* van het CBP en van de Working Document Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive van 24 juli 1998. DG XV D/5025/98. WP 12 van de Article 29-Working Group.

In het gros van de gevallen zullen alleen de uitzonderingen achter d (zwaarwegend algemeen belang) en g (modelcontract) mogelijk uitkomst kunnen bieden.

In de *Nota derde landen* van het CBP is over de uitzondering achter d opgemerkt: 'In dat geval vindt de doorgifte (...) plaats (...) omdat daar een algemeen belang mee is gediend. Deze uitzondering kan van toepassing zijn op beperkte doorgiftes tussen overheidsinstellingen, hoewel ervoor moet worden gewaakt dat deze bepaling niet al te ruim wordt opgevat. Een algemeen belang is op zich geen afdoende rechtvaardiging voor de doorgifte, er moet een zwaarwegend algemeen belang mee gediend zijn. Overweging 58 van de Richtlijn geeft aan dat doorgiftes tussen administraties van belastingdiensten of douane of tussen sociale-zekerheidsinstanties doorgaans onder deze uitzondering zullen vallen. Doorgiftes tussen toezichthoudende autoriteiten in de financiële sector kunnen wellicht ook onder deze uitzondering vallen.'[49] Naar ons oordeel mag worden aangenomen dat dit ook zal gelden voor andere gebieden waarbinnen de Europese dan wel nationale wetgever verstrekking van gegevens aan derde landen mogelijk heeft gemaakt. Zou dat anders zijn, dan zou dat (wederom[50]) de wonderlijke consequentie hebben dat aan de ene kant nadrukkelijk een (Europees of nationaalrechtelijke) bevoegdheid[51] is gecreëerd om gegevens – waaronder ook persoonsgegevens worden begrepen – aan derde landen te verstrekken, terwijl aan de andere kant van deze bevoegdheid veelal geen gebruik kan worden gemaakt, voor zover de te verstrekken informatie persoonsgegevens bevat. Bovendien spreekt het CBP over de doorgifte 'tussen overheidsinstellingen'. Als sprake is van doorgifte tussen overheidsinstellingen, zal naar ons oordeel in principe sprake zijn van een algemeen belang bij die doorgifte. Er zal in een concreet geval echter steeds moeten worden beoordeeld of dat algemeen belang ook zwaarwegend is.

Deze hiervoor bedoelde passage van het CBP is (kennelijk) gebaseerd op een advies van de Article 29-Working Group over artikel 26 lid 1 Privacyrichtlijn, het artikel dat in artikel 77 lid 1 Wbp is geïmplementeerd. In dat advies wordt over onderdeel d verder nog opgemerkt dat deze uitzonderingsgrond niet van toepassing kan zijn als alleen het derde land een zwaarwegend algemeen belang heeft bij de verstrekking. De verstrekking moet ook een zwaarwegend algemeen belang van 'the authorities of an EU Member State themselves' dienen.[52] Uit het advies blijkt verder dat de uitzonderingsgrond strikt moet worden geïnterpreteerd (p. 7). De achtergrond daarvan is dat er bij een verstrekking op de voet van artikel 77 lid 1 onder d Wbp strikt genomen geen sprake hoeft te zijn van een passend beschermingsniveau.[53] Vanzelfsprekend moeten wel de overige eisen die de Wbp stelt in acht worden genomen (p. 8). Bovendien stelt de Article 29-Working

49 *Nota derde landen* van het CBP, p. 21.

50 Vergelijk de voorlaatste alinea van paragraaf 3.2.

51 En in een enkel geval zelfs de verplichting, zie bijvoorbeeld artikel 5 Wet op de internationale bijstandsverlening bij de heffing van belastingen.

52 Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 van 25 november 2005. 2093/05/EN. WP 114, p. 15.

53 Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 van 25 november 2005. 2093/05/EN. WP 114, p. 6: 'In fact, these exceptions allow the transfer to take place to third countries that do not ensure an adequate level of protection.'

Group voorop dat de verantwoordelijke, indien mogelijk, zou moeten kiezen voor een van de alternatieve grondslagen voor doorgifte van persoonsgegevens naar derde landen. 'Best practice' is dat eerst wordt beoordeeld of het derde land een passend beschermingsniveau heeft (artikel 76 Wbp). Als dat niet het geval is, dan zou de verantwoordelijke (lees: de Nederlandse autoriteit) moeten bezien of toepassing van artikel 26 lid 2 Privacyrichtlijn mogelijk is. Dat artikel is geïmplementeerd in artikel 77 lid 2 Wbp, dat bepaalt:

> 'In afwijking van het eerste lid, kan Onze Minister, gehoord het College, een vergunning geven voor een doorgifte of een categorie doorgiften van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt. Aan de vergunning worden de nadere voorschriften verbonden die nodig zijn om de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen, alsmede de uitoefening van de daarmee verband houdende rechten te waarborgen.'

De Article-29-Working Group merkt op dat 'Only if this is truly not practical and/or feasible, then the data controller should consider using the derogations of Article 26(1)' en voegt daaraan toe dat zij 'would recommend that the derogations of Article 26(1) of the Directive should preferably be applied to cases in which it would be genuinely inappropriate, maybe even impossible for the transfer to take place on the basis of Article 26(2)'. De Working Group zou het 'regrettable' vinden als een 'public authority would plan to make significant transfers of data to a third country without providing an appropriate framework for the transfer, when it has the practical means of providing such protection (e.g. a contract, (...), a convention)'. Van belang is verder dat hoewel 'the cases listed in Article 26(1) may constitute a derogation to the principle that the third country should guarantee an adequate protection, they do not provide additional exemptions from the rule that fundamental rights should be respected'. De nationale privacytoezichthouders 'should ensure that these derogations are applied in situations that do not entail a breach of the data subjects' fundamental rights and which correspond to the need to maintain a strict interpretation of these derogations' en kunnen in dit verband, 'if there is sufficient reason to do so, intervene at any time and recommend that an international transfer of data should be carried out on the basis of adequate safeguards in the meaning of Article 26(2) rather than by applying the exceptions listed in Article 26(1)' (p. 9-10).

Uit de voorgaande citaten kan worden afgeleid dat het sterk aanbeveling verdient dat een Nederlandse autoriteit die persoonsgegevens naar een derde land wil doorgeven daarvoor een vergunning bij de minister van Veiligheid en Justitie aanvraagt op de voet van artikel 77 lid 2 Wbp,[54] dan wel een overeenkomst

54 Een verantwoordelijke hoeft niet voor elke afzonderlijke doorgifte een vergunning aan te vragen. Er kan een vergunning voor een categorie van doorgiftes worden aangevraagd, met andere woorden, een duidelijk omschreven verzameling van doorgiftes met gemeenschappelijke elementen waarbij dezelfde omstandigheden een rol spelen. Een vergunning kan alleen worden verleend op basis van specifieke en duidelijk omschreven omstandigheden en waarborgen die worden ingesteld om specifieke risico's af te schermen en waarbij het toepassingsgebied van de vergunning te allen tijde kan worden bepaald. Zie p. 23-24 van de *Nota derde landen* van het CBP. De minister van Veiligheid en Justitie heeft bijvoorbeeld een vergunning verleend aan de AFM om

conform het modelcontract als bedoeld in artikel 77 lid 1 onder g Wbp met het derde land sluit. De Europese Commissie heeft tot nu toe drie modelcontracten goedgekeurd, waarvan er twee zouden kunnen worden gebruikt door een Nederlandse autoriteit die persoonsgegevens aan een derde land wil verstrekken: de modelcontracten voor doorgifte tussen twee verantwoordelijken waarvan de een gevestigd is in een EU-land en de ander buiten de EU.[55] Wordt ervoor gekozen het modelcontract niet in ongewijzigde vorm over te nemen, dan is alsnog een vergunning nodig.[56]

Naar ons oordeel zal de Nederlandse autoriteit de persoonsgegevens alleen op de voet van artikel 77 lid 1 onder d Wbp aan een derde land mogen verstrekken als de route van een vergunning c.q. een overeenkomst conform een modelcontract niet haalbaar is. Er moet dan wel sprake zijn van een restrictief te interpreteren zwaarwegend algemeen belang, en de verstrekking van de persoonsgegevens moet noodzakelijk zijn ter verwezenlijking van dat belang.

3.6 Rechten van de betrokkene

De Nederlandse autoriteit zal bij een beoogde verstrekking verder (actief) rekening moeten houden met de informatieverplichting uit de artikelen 33 en 34 Wbp. Uit die artikelen vloeit voort dat op de Nederlandse autoriteit in beginsel de verplichting rust de betrokkene over een voorgenomen gegevensverstrekking en het doel daarvan te informeren, tenzij de gegevens met het oog op de verstrekking aan de buitenlandse autoriteit – bijvoorbeeld in het kader van toezicht op verzoek – van de betrokkene zelf zijn verkregen en de betrokkene van dit doel al op de hoogte is.[57]

Het informeren kan op grond van artikel 43 Wbp (tijdelijk) achterwege worden gelaten voor zover dat noodzakelijk is in het belang van:

'a. de veiligheid van de staat;
b. de voorkoming, opsporing en vervolging van strafbare feiten;

---

persoonsgegevens met de toezichthouder op accountantsorganisaties in Japan, de Financial Services Agency/Certified Public Accountants and Auditing Oversight Board (JFSA/CPAAOB), uit te wisselen ten behoeve van, kort gezegd, grensoverschrijdend toezicht op accountantsorganisaties. De wederzijdse afspraken zijn vastgelegd in een zogeheten Exchange of Letters. Zie www.afm.nl/nl/nieuws/2014/juni/eol-afm-japan.aspx. Een ander voorbeeld is de vergunning die is verleend voor de samenwerking met de toezichthouder op accountantsorganisaties in de Verenigde Staten, de Public Company Accounting Oversight Board (PCAOB). Zie www.afm.nl/nl/nieuws/2011/dec/samenwerking-afm-pcaob-toezicht-acc.aspx.

55 Zie voor de modelcontracten: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

56 *Kamerstukken II* 2008/09, 31841, 3, p. 16.

57 Vergelijk bijvoorbeeld artikel 17 van verordening 8, waarin is bepaald dat de lidstaten er met betrekking tot de toepassing van de Privacyrichtlijn met name voor zorgen dat iedere persoon wordt ingelicht als het voornemen bestaat gegevens die op hem betrekking hebben aan derden door te geven. Het is de vraag waarom deze bepaling zo expliciet is opgenomen. Dat zou niet nodig hoeven te zijn.

c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of
e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen.'

Van geval tot geval zal moeten worden bezien of een van deze belangen aan het informeren van de betrokkene in de weg staat. Goed denkbaar is dat met name de uitzonderingen achter c en d onder omstandigheden een grondslag zullen kunnen bieden om het informeren op het moment van verstrekking achterwege te laten.[58]

3.7 Deelconclusie

In het gros van de gevallen zal een Nederlandse autoriteit een grondslag voor de verstrekking aan een buitenlandse autoriteit kunnen vinden in artikel 8 onder c, (wettelijke verplichting), e (publiekrechtelijke taak) of f (gerechtvaardigd belang) Wbp. Als sprake is van een wettelijke verplichting om gegevens te verstrekken, zal naar ons oordeel niet aan de eis van verenigbaar gebruik van artikel 9 Wbp hoeven te worden getoetst. Als sprake is van een verstrekkingsbevoegdheid waar een vergaarmogelijkheid aan is gekoppeld, zal van onverenigbaar gebruik geen sprake zijn. Extra oplettendheid is vereist als het voornemen bestaat om bijzondere persoonsgegevens, zoals strafrechtelijke gegevens, aan een buitenlandse autoriteit te verstrekken. Er zal dan eerst beoordeeld moeten worden of sprake is van een van de doorbrekingsgronden uit de artikelen 17 tot en met 23 Wbp. Het verdient aanbeveling dat de (Europese en nationale) wetgever er – bijvoorbeeld in de toelichting bij de desbetreffende verstrekkingsbepaling – expliciet aandacht aan besteedt of de betreffende bepaling ook een verplichting/bevoegdheid in het leven roept om bijzondere persoonsgegevens te verstrekken. Ook bij de doorgifte van persoonsgegevens aan derde landen moet extra oplettendheid worden betracht. Er moet in de eerste plaats beoordeeld worden of het derde land een passend beschermingsniveau kent. Is dat niet het geval, dan zal zo mogelijk ofwel een vergunning van de minister van Veiligheid en Justitie moeten worden verkregen, ofwel een overeenkomst conform een modelcontract met het desbetreffende derde land moeten worden gesloten. Als dat niet mogelijk is, zal nog kunnen worden beoordeeld of een beroep kan worden gedaan op de (strikt te interpreteren) omstandigheid dat de doorgifte noodzakelijk is vanwege een zwaarwegend algemeen belang. Tot slot is relevant dat een betrokkene in beginsel over de voorgenomen verstrekking moet worden geïnformeerd, tenzij één of meer van de belangen als bedoeld in artikel 43 Wbp daaraan in de weg staan.

58 Vergelijk in dit verband bijvoorbeeld artikel 28 lid 4 van verordening 3, waarin is bepaald dat (onder meer) de informatieverplichting kan worden beperkt voor zover dat noodzakelijk is om de in artikel 13 lid 1 onder e Privacyrichtlijn – dat in artikel 43 onder c Wbp is geïmplementeerd – bedoelde belangen te vrijwaren. De beperking dient wel in verhouding te staan tot het belang in kwestie.

4 De privacyrechtelijke regels voor grensoverschrijdende gegevensuitwisseling in de toekomst

4.1 Inleiding

Aan het begin van dit preadvies hebben wij reeds genoemd dat de Privacyrichtlijn, die met de Wbp in de Nederlandse rechtsorde is geïmplementeerd, zal worden vervangen door een verordening: de Algemene Verordening Gegevensbescherming. Doel van de AVG is de regels betreffende de bescherming van persoonsgegevens verder te harmoniseren.[59] Omdat de AVG de privacyrechtelijke regels in de nabije toekomst zal veranderen, behandelen wij in dit hoofdstuk de mogelijke gevolgen van die verandering voor gegevensverstrekking door Nederlandse autoriteiten aan buitenlandse autoriteiten.

4.2 Grondslag voor verstrekking: artikel 6 AVG

Veel van de uitgangspunten en beginselen van het huidige privacyrechtelijke kader blijven gehandhaafd in de AVG. Zo ook het aan artikel 8 Wbp ten grondslag liggende beginsel dat persoonsgegevens alleen mogen worden verwerkt als daarvoor een grondslag bestaat en de gegevensverwerking noodzakelijk is ter verwezenlijking van het doel waarvoor de gegevens worden verwerkt. In artikel 6 lid 1 onder a tot en met f AVG zijn grosso modo dezelfde grondslagen te vinden als in artikel 8 Wbp. Een aantal nuanceverschillen kan echter relevant zijn voor verstrekking aan buitenlandse autoriteiten.

Omdat artikel 6 lid 1 onder c AVG nog steeds een wettelijke verplichting als grondslag voor gegevensverwerking aanmerkt, zullen Nederlandse autoriteiten die gegevens aan buitenlandse autoriteiten willen verstrekken op grond van een verstrekkings*verplichting* veelal in die bepaling een grondslag kunnen vinden. In paragraaf 3.2 is reeds genoemd dat uit artikel 6 lid 3 AVG expliciet volgt dat een wettelijke verplichting tot gegevensverwerking moet zijn voorzien in EU-

59 Toelichting op de AVG, 25 januari 2012, COM(2012) 11, p. 1-2. Zie ook de mededeling van de Europese Commissie die ten grondslag ligt aan de herziening van de Europese privacyregels: 'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie', COM(2010) 609.

wetgeving of in nationale wetgeving van de lidstaat waaraan de voor verwerking verantwoordelijke onderworpen is. Artikel 6 lid 3 AVG luidt:

> 'In de grondslag voor de in, eerste lid, onder c) en e), bedoelde verwerking moet worden voorzien in:
> a. EU-wetgeving, of
> b. de wetgeving van de lidstaat waaraan de voor de verwerking verantwoordelijke onderworpen is.
>
> Het recht van de lidstaat moet beantwoorden aan een doelstelling van algemeen belang of noodzakelijk zijn om de rechten en vrijheden van anderen te beschermen, de wezenlijke inhoud van het recht op de bescherming van persoonsgegevens eerbiedigen en evenredig zijn aan het nagestreefde rechtmatige doel.'

In het derde lid van artikel 6 AVG wordt aldus een aantal eisen opgesomd waaraan een verwerkingsverplichting die volgt uit het Europese of nationale recht moet voldoen. Dat betreft een doelstellingsvereiste, een gegevensbeschermingsvereiste en een proportionaliteitsvereiste. Wij verwachten niet dat artikel 6 lid 3 AVG het toepassingsbereik zal verkleinen van de grondslag in artikel 6 lid 1 onder c AVG ten opzichte van de huidige grondslag in artikel 8 onder c Wbp. De bepalingen met verstrekkingsverplichtingen zullen doorgaans voldoen aan het doelstellingsvereiste, omdat de bepalingen gericht op samenwerking tussen autoriteiten door de Europese of Nederlandse wetgever in het leven zijn geroepen ten behoeve van het algemeen belang, bijvoorbeeld ten behoeve van het belang van toezicht in een bepaalde sector. Aan het gegevensbeschermingsvereiste zal in beginsel worden voldaan indien de verstrekkende autoriteit de gegevensbeschermingsregels van de AVG (en eventuele bijzondere gegevensbeschermingsregels die van toepassing zijn) in acht neemt. Net als in het huidige regime van de Wbp betekent het hebben van een grondslag in artikel 8 Wbp niet dat de verstrekker van gegevens niet meer aan de overige vereisten van de Wbp hoeft te voldoen. Daarnaast zal verstrekking op grond van een wettelijke verplichting, net als onder de huidige gegevensbeschermingsregels, noodzakelijk moeten zijn voor de voldoening aan die wettelijke verplichting.

Ten aanzien van bepalingen waarin een verstrekkings*bevoegdheid* is opgenomen, merken wij op dat ook artikel 8 onder e Wbp een equivalent heeft in de AVG. Artikel 6 lid 1 onder e AVG luidt:

> 'De verwerking van persoonsgegevens is alleen rechtmatig wanneer en voor zover ten minste van een van de volgende gevallen sprake is:
> (…)
> e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of een taak die deel uitmaakt van de uitoefening van het openbaar gezag dat aan de voor de verwerking verantwoordelijke is opgedragen;'.

Hoewel artikel 6 lid 1 onder e AVG niet spreekt van 'publiekrechtelijke taak', is aannemelijk dat met de aldaar geformuleerde omschrijving hetzelfde wordt bedoeld als de 'publiekrechtelijke taak' in de zin van artikel 8 onder e Wbp. Wij wijzen op artikel 7 onder e Privacyrichtlijn, waarin ook niet wordt gesproken van

een 'publiekrechtelijke taak', maar van 'een taak van algemeen belang of een taak die deel uitmaakt van de uitoefening van het openbaar gezag'.

Indien de grondslag voor gegevensverstrekking in de toekomst door een Nederlandse autoriteit wordt gevonden in artikel 6 lid 1 onder e AVG, moet de publiekrechtelijke taak om de gegevens te verstrekken – net als de wettelijke verplichting ex artikel 6 lid 1 onder c AVG – een grondslag hebben in EU-wetgeving of in nationale wetgeving, gelet op artikel 6 lid 3 AVG (zie hiervoor). Ook aan de overige vereisten die in artikel 6 lid 3 AVG staan, moet in het geval van een grondslag die wordt gevonden in artikel 6 lid 1 onder e AVG worden voldaan. Aan het doelstellingsvereiste zal veelal worden voldaan, omdat bij een verstrekkingsbevoegdheid sprake is van een aan de autoriteit toebedeelde taak van algemeen belang of een taak die deel uitmaakt van de uitoefening van openbaar gezag in het kader waarvan deze autoriteit bevoegd is gegevens te verstrekken aan een buitenlandse counterpart. Voorts moeten de overige gegevensbeschermingsregels in acht worden genomen als de grondslag voor de verwerking wordt gevonden in artikel 6 lid 1 onder e AVG en moet de gegevensverstrekking noodzakelijk zijn voor de goede vervulling van de taak van algemeen belang of voor de taak die deel uitmaakt van de uitoefening van openbaar gezag.

In artikel 6 lid 1 onder f AVG is een vergelijkbare bepaling opgenomen als in artikel 8 onder f Wbp. In de f-grond van de AVG is overigens wel aan de bepaling toegevoegd dat geen sprake kan zijn van een gerechtvaardigd belang voor zover het gaat om de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken. Daarover is in de preambule het volgende opgenomen (nr. 37):

> 'Aangezien het aan de wetgever is om de rechtsgrondslag te creëren voor gegevensverwerking door overheidsinstanties, dient deze rechtsgrond niet van toepassing te zijn op de verwerking door overheidsinstanties in het kader van de uitvoering van hun taken.'

Die overweging leidt onzes inziens niet tot beperkingen voor autoriteiten om gegevens te verstrekken aan een buitenlandse autoriteit. Voor zover immers geoordeeld zou moeten worden dat een verstrekking aan een buitenlandse autoriteit niet plaatsvindt ter voldoening aan een wettelijke verplichting of ter uitvoering van een publiekrechtelijk taak van de verstrekkende overheidsinstantie, kan artikel 6 lid 1 onder f AVG in theorie nog steeds een grondslag vormen.

4.3 (On)verenigbaar gebruik: artikel 5 onder b AVG

Artikel 5 onder b AVG bevat, net als artikel 9 Wbp, het uitgangspunt dat persoonsgegevens niet mogen worden verwerkt voor andere doeleinden indien die doeleinden onverenigbaar zijn met de doeleinden waarvoor de gegevens in eerste instantie zijn verwerkt. Ook onder de AVG is de redenering houdbaar dat bij een wettelijke verplichting om gegevens te verstrekken geen beoordeling

plaats hoeft te vinden of sprake is van onverenigbaar gebruik. Zou dat anders zijn, dan zou een autoriteit buiten een door de wetgever opgedragen verplichting om alsnog moeten gaan toetsen of wel uitvoering kan worden gegeven aan de verplichting. Als er een verstrekkingsbevoegdheid bestaat en er in het kader van die bevoegdheid een mogelijkheid bestaat om gegevens te vergaren ten behoeve van de buitenlandse autoriteit, zal artikel 5 onder b AVG niet aan de verstrekking in de weg staan.

De criteria aan de hand waarvan moet worden beoordeeld of sprake is van onverenigbaar gebruik zijn, anders dan in artikel 9 Wbp, niet uitgewerkt. Dat is echter ook niet het geval in artikel 6 lid 1 onder b Privacyrichtlijn, dat in artikel 9 Wbp is geïmplementeerd. Uit het advies van de Article 29-Working Group over het doelbindingsvereiste kan worden afgeleid dat de criteria die zijn genoemd in artikel 9 Wbp grosso modo overeenkomen met wat gelet op dat advies in het kader van artikel 6 lid 1 onder b Privacyrichtlijn moet worden getoetst.[60] Gezien de gelijke formulering van artikel 6 lid 1 onder b Privacyrichtlijn en artikel 5 onder b AVG, zal de toets niet of nauwelijks veranderen wanneer de AVG wordt ingevoerd.

Wij wijzen nog op de mogelijkheden om het verbod op onverenigbaar gebruik te doorbreken. In paragraaf 3.3 wezen wij op artikel 43 Wbp, op basis waarvan artikel 9 Wbp onder omstandigheden buiten toepassing kan worden gelaten. In de AVG wordt artikel 21 opgenomen, dat vergelijkbaar is met artikel 43 Wbp.[61] Daarnaast bevat artikel 6 lid 4 AVG een specifieke bepaling om het verbod op onverenigbaar gebruik te doorbreken.

In artikel 6 lid 4 AVG is bepaald dat een verdere verwerking voor onverenigbare doeleinden wel mogelijk is indien die verdere verwerking minstens een grondslag heeft in artikel 6 lid 1 onder a tot en met e AVG. Dat betekent dat een autoriteit een verdere verwerking die onverenigbaar zou zijn met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, voor zover van belang, kan rechtvaardigen met een beroep op een wettelijke verplichting (artikel 6 lid 1 onder c AVG) of op een publiekrechtelijke taak (artikel 6 lid 1 onder e AVG).[62] Een grondslag alleen is echter, gelet op het woord 'minstens' in artikel 6 lid 4 AVG, onvoldoende. Uit de toelichting op dit artikel volgt dat er naast een grondslag voorts voor moet worden gezorgd dat de in de AVG vervatte beginselen worden toegepast – waaronder het criterium dat een gegevensverwerking noodzakelijk moet zijn – en dat de betrokkene wordt geïnformeerd over de verwerking die onverenigbaar

60 Opinion 03/2013 on purpose limitation van 2 april 2013. 00569/13/EN. WP203, p. 23-27.

61 Zie hierover paragraaf 4.6.

62 Hoewel in artikel 6 lid 4 AVG is opgenomen dat de bepaling met name van toepassing is op iedere wijziging van de clausules en algemene voorwaarden van overeenkomsten, nemen wij aan dat deze bepaling ook van toepassing kan zijn op andere vormen van verdere verwerkingen die onverenigbaar zijn met het oorspronkelijke doel waarvoor de persoonsgegevens zijn verkregen. Daarvoor vinden wij zowel steun in het feit dat de bepaling spreekt van 'met name' (en daarmee andere gevallen van verdere verwerking niet uitsluit), als in het feit dat ook de grondslag in artikel 6 lid 1 onder e AVG een dergelijke verdere verwerking kan rechtvaardigen. Bij verwerkingen op grond van de e-grond gaat het veelal om overheidsorganen die persoonsgegevens (verder) verwerken en niet zozeer (hoewel niet uitgesloten) om verdere verwerkingen door wijzigingen van overeenkomsten.

is met het doel waarvoor de persoonsgegevens zijn verzameld.[63] De informatieplicht is in de AVG neergelegd in artikel 14 (vergelijk artikelen 33 en 34 Wbp).[64]

Is de grondslag voor de verdere verwerking van persoonsgegevens door een Nederlandse autoriteit artikel 6 lid 1 onder f AVG, dan kan geen beroep worden gedaan op artikel 6 lid 4 AVG voor een verdere verwerking die onverenigbaar is met het doel waarvoor de persoonsgegevens zijn verzameld. In dat geval is verdere verwerking slechts mogelijk voor zover artikel 5 onder b AVG kan worden beperkt door artikel 21 AVG. De autoriteit hoeft dan niet 'slechts' het niet-informeren te kunnen rechtvaardigen met een beroep op artikel 21 AVG, maar moet het onverenigbare gebruik in zijn geheel kunnen rechtvaardigen met een beroep op artikel 21 AVG.[65]

4.4 Bijzondere persoonsgegevens

Het verbod om bijzondere persoonsgegevens te verwerken is opgenomen in artikel 9 lid 1 AVG. De specifieke doorbrekingsgronden zijn in artikel 9 lid 2 AVG opgesomd. Een specifieke doorbrekingsgrond voor volkenrechtelijke verplichtingen (artikel 23 lid 1 onder e Wbp) ontbreekt in de AVG. Wel komt de algemene doorbrekingsgrond (artikel 23 lid 1 onder f Wbp) terug in de AVG. In artikel 9 lid 2 onder g AVG is bepaald dat het verbod op verwerking van bijzondere persoonsgegevens niet van toepassing is, indien de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang, op grond van EU-wetgeving of de nationale wetgeving waarbij passende maatregelen worden vastgesteld ter bescherming van de gerechtvaardigde belangen van de betrokkene.

In de AVG is geen met artikel 22 lid 6 Wbp vergelijkbare bepaling opgenomen over de doorbreking van het verbod om strafrechtelijke persoonsgegevens te verwerken ten behoeve van een publiekrechtelijk samenwerkingsverband. Wel is er een algemene doorbrekingsgrond opgenomen met betrekking tot het verwerken van gegevens betreffende strafrechtelijke veroordelingen of daarmee verband houdende veiligheidsmaatregelen, te weten in artikel 9 lid 2 onder j AVG. Het Europees Parlement heeft voorgesteld dat het verbod om bijzondere persoonsgegevens te verwerken ook op gegevens betreffende bestuursrechtelijke sancties betrekking zou moeten hebben en dat dat verbod ook onder de in artikel 9 lid 2 onder j AVG genoemde omstandigheden zou moeten kunnen worden doorbroken.[66] Artikel 9 lid 2 onder j AVG) luidt:

> 'Lid 1 is niet van toepassing wanneer:
> (…)
> j) de verwerking van gegevens betreffende strafrechtelijke veroordelingen of daarmee verband houdende veiligheidsmaatregelen wordt uitgevoerd onder toezicht van de

63 Preambule, randnummer 39.
64 Onder omstandigheden kan de informatieplicht worden beperkt. Zie daarover paragraaf 4.6.
65 Zie hierover paragraaf 4.6.
66 Rapport van 22 november 2013 betreffende COM(2012) 11. Raadpleegbaar via www.europarl.europa.eu.

overheid of wanneer de verwerking noodzakelijk is om een wettelijke verplichting van de voor de verwerking verantwoordelijke na te komen of voor de vervulling van een taak om gewichtige redenen van algemeen belang, en voor zover zulks is toegestaan bij EU-wetgeving of de nationale wetgeving en deze wetgeving passende garanties biedt. Een volledig register van strafrechtelijke veroordelingen mag alleen worden bijgehouden onder toezicht van de overheid.'

Van doorbreking van het verbod om strafrechtelijke persoonsgegevens te verwerken met een beroep op artikel 9 lid 2 onder j AVG kan dus slechts sprake zijn als de verwerking wordt uitgevoerd onder toezicht van de overheid, als de verwerking noodzakelijk is om een wettelijke verplichting van de voor de verwerking verantwoordelijke na te komen of als dat nodig is voor de vervulling van een taak om gewichtige redenen van algemeen belang. Op grond van een samenwerkingsbepaling inhoudende een verstrekkings*verplichting* zullen aldus strafrechtelijke persoonsgegevens kunnen worden verstrekt aan een buitenlandse autoriteit voor zover dat noodzakelijk is om de wettelijke samenwerkingsverplichting na te komen. Op grond van een bepaling inhoudende een verstrekkings*bevoegdheid* zal de verstrekking van strafrechtelijke persoonsgegevens mogelijk zijn indien de verstrekking noodzakelijk is voor de vervulling van een taak om gewichtige redenen van algemeen belang. In beide gevallen is *daarnaast* nog vereist dat de verwerking van strafrechtelijke persoonsgegevens is toegestaan in een Europese of nationale wet en moeten er passende garanties worden geboden.

4.5 Verstrekking aan derde landen

Hoofdstuk vijf van de AVG ziet op de doorgifte van persoonsgegevens aan derde landen en internationale organisaties. Algemeen beginsel met betrekking tot gegevensverstrekking aan derde landen blijft dat dit slechts mogelijk is indien het land waaraan wordt verstrekt een passend beschermingsniveau waarborgt (artikel 41 lid 1 AVG). Een opmerkelijk verschil is dat de mogelijkheid om daaromtrent zelf een oordeel te vormen bij gebrek aan een besluit van de Commissie ontbreekt in de AVG. In artikel 41 lid 1 AVG staat expliciet dat doorgifte kan plaatsvinden als de Commissie heeft besloten dat een land een passend beschermingsniveau waarborgt.

Dat betekent niet dat het onmogelijk is persoonsgegevens te verstrekken aan een derde land ten aanzien waarvan de Commissie geen (positief) besluit heeft genomen. Indien de Commissie niet over een land heeft besloten dat het een passend beschermingsniveau waarborgt, bestaat de mogelijkheid om passende garanties te bieden door middel van een juridisch bindend instrument (artikel 42 lid 1 AVG). Dat kunnen, gelet op artikel 42 lid 2 AVG, (onder meer) door de Commissie (artikel 42 lid 2 onder b AVG) of door het CBP (artikel 42 lid 2 onder c AVG) goedgekeurde modelbepalingen zijn. Het gaat in dat geval om modelbepalingen die vooraf zijn goedgekeurd en door de verantwoordelijken kunnen worden toegepast zonder dat verdere toestemming van de privacytoezichthouder is vereist (artikel 42 lid 3 AVG). Een andere mogelijkheid is het sluiten van een contract tussen de verstrekker en de ontvanger, zonder dat de modelbepalingen worden toegepast (artikel 42 lid 2 onder d AVG). Voor het verstrekken van

persoonsgegevens aan derde landen op grond van een dergelijk contract is wel toestemming van het CBP nodig (artikel 42 lid 4 AVG). Tot slot staat in het vijfde lid van artikel 42 AVG dat ook vooraf toestemming kan worden verkregen van het CBP voor andere geschikte en evenredige maatregelen. Wij merken op dat de mogelijkheid om met toestemming van het CBP door middel van een met de ontvanger gesloten contract niet zijnde modelbepalingen (artikel 42 lid 2 onder d AVG) dan wel door middel van andere geschikte en evenredige maatregelen (artikel 42 lid 5 AVG) gegevens te verstrekken aan een derde land, nieuw is ten opzichte van de bepalingen in de Wbp. Op grond van artikel 77 lid 2 Wbp moet in die gevallen momenteel een vergunning worden aangevraagd bij de minister van Veiligheid en Justitie. De mogelijkheid van vergunningverlening door de minister van Veiligheid en Justitie vervalt.

Als er geen (positief) besluit van de Commissie over een passend beschermingsniveau van een derde land is en geen passende garanties overeenkomstig artikel 42 AVG zijn verkregen, kan doorgifte naar een derde land toch plaatsvinden als de doorgifte noodzakelijk is vanwege een zwaarwegend algemeen belang (artikel 44 lid 1 onder d AVG), zoals dat nu ook is geregeld in artikel 77 lid 1 onder d Wbp. In de preambule is over deze afwijkingen expliciet opgemerkt dat zij van toepassing kunnen zijn op doorgifte door verschillende soorten autoriteiten:

> 'Deze afwijkingen dienen met name te gelden voor gegevensdoorgiften die nodig zijn op grond van gewichtige redenen van algemeen belang, zoals internationale gegevensuitwisselingen tussen mededingingsautoriteiten, belasting- of douanediensten, financiële toezichthoudende autoriteiten, diensten met bevoegdheid op het gebied van de sociale zekerheid of de autoriteiten belast met de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten.'[67]

4.6 Rechten van de betrokkene

Met betrekking tot de informatieplicht merken wij op dat in het artikel in de AVG omtrent de informatieverstrekking aan de betrokkene (artikel 14 AVG) expliciet is opgenomen dat bij een voorgenomen verstrekking aan een derde land of internationale organisatie moet worden verwezen naar het besluit van de Commissie waarbij het beschermingsniveau passend wordt verklaard (artikel 14 lid 1 onder g AVG). Wij gaan ervan uit dat bij het ontbreken van een dergelijk besluit moet worden genoemd op welke andere wijze passende garanties voor de bescherming van de persoonsgegevens van de betrokkene worden geboden.

Voorts wijzen wij op de beperkingsmogelijkheid van artikel 21 AVG. Dat artikel luidt:

> '1. De reikwijdte van de in artikel 5, onder a) tot en met e), en de artikelen 11 tot en met 20 en artikel 32 neergelegde verplichtingen en rechten mogen bij EU-

67 Toelichting bij COM(2012) 11, p. 35, randnummer 87. Gezien de specifieke verwijzing naar internationale gegevensuitwisselingen in de preambule bij randnummer 87, is het de vraag of een autoriteit voor gegevensuitwisseling met derde landen ook nog een grondslag zou kunnen vinden in artikel 44 lid 1 onder h AVG (gerechtvaardigd belang, als geen sprake is van een frequente of massale verwerking; zie randnummer 88).

wetgeving of nationale wetgeving door middel van een wettelijke maatregel worden beperkt, wanneer een dergelijke beperking in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van:

a. de openbare veiligheid;
b. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten;
c. andere algemene belangen van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden en de bescherming van de marktstabiliteit en -integriteit;
d. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
e. een taak op het gebied van toezicht, inspectie of regelgeving die verbonden is, ook al is dit incidenteel, met de uitoefening van het openbaar gezag in de onder a), b), c) en d), bedoelde gevallen;
f. de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

2. De in lid 1 wettelijke maatregelen bevatten met name specifieke bepalingen met betrekking tot ten minste de doelstellingen die met de verwerking moeten worden nagestreefd en de vaststelling van de voor de verwerking verantwoordelijke.'

Artikel 21 AVG is het equivalent van de huidige artikelen 13 Privacyrichtlijn en 43 Wbp. Artikel 13 bepaalt, voor zover van belang:

'1. De Lid-Staten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in artikel 6, lid 1, artikel 10, artikel 11, lid 1, artikel 12 en artikel 21 bedoelde rechten en plichten indien dit noodzakelijk is ter vrijwaring van (...)'

Artikel 43 Wbp is de wettelijke maatregel als bedoeld in artikel 13 Privacyrichtlijn. Het is de vraag of een en ander met de wettelijke maatregelen zoals genoemd in artikel 21 AVG er in de praktijk anders uit komt te zien. Er zijn geen aanwijzingen dat een wijziging ten opzichte van de huidige situatie is beoogd. Wij zouden het onwenselijk vinden als wordt vereist dat in iedere wettelijke regeling uit hoofde waarvan de verstrekking van persoonsgegevens aan de orde kan zijn, een beperkingsclausule moet worden opgenomen. De verantwoordelijke – in dit geval de Nederlandse autoriteit – zou de beoordeling in een concreet geval steeds zelf moeten kunnen maken. Net als nu en net zoals de verantwoordelijke in staat wordt geacht diverse andere beoordelingen onder de Wbp en AVG volledig zelfstandig te maken. Het feit dat een heleboel wettelijke regelingen zouden moeten worden aangepast, lijkt overigens ook niet praktisch.

Verder valt op dat artikel 21 AVG spreekt van beperkingen, terwijl het in artikel 43 Wbp (en artikel 13 Privacyrichtlijn) over uitzonderingen en beperkingen gaat. Dat kan erop wijzen dat artikel 21 AVG ten opzichte van artikel 43 Wbp strikter van aard is. Anderzijds zijn de belangen genoemd in artikel 21 AVG op grond waarvan een beperking gerechtvaardigd kan worden geacht, ruimer dan de belangen genoemd in artikel 43 Wbp. In artikel 43 onder d Wbp is bepaald dat bepaalde uitzonderingen of beperkingen noodzakelijk kunnen zijn in het belang van het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve

van de belangen bedoeld onder b en c. In artikel 43 onder b en c Wbp wordt slechts verwezen naar het voorkomen, opsporen en vervolgen van strafbare feiten (b) en de gewichtige, economische en financiële belangen van de staat en andere openbare lichamen (c). In artikel 21 lid 1 onder e AVG is bepaald dat bepaalde beperkingen noodzakelijk kunnen zijn in het belang van toezicht, inspectie of regelgeving die al dan niet incidenteel is verbonden met de uitoefening van het openbaar gezag in de onder a, b, c en d bedoelde gevallen. In artikel 21 lid 1 onder a, b, c, en d AVG wordt verwezen naar de openbare veiligheid (a), het voorkomen, opsporen en vervolgen van strafbare feiten (b), andere algemene belangen van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een andere lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden en de bescherming van de marktstabiliteit en -integriteit (c) en de voorkoming, het onderzoek en de opsporing en de vervolging van schendingen van de beroepscodes van gereglementeerde beroepen (d).

4.7 Deelconclusie

Hoewel de uitgangspunten en beginselen van de Wbp niet drastisch veranderen wanneer de AVG van kracht zal worden, is er wel een aantal veranderingen aan te wijzen. Zo biedt artikel 6 lid 4 AVG een (extra) specifieke mogelijkheid om gegevens aan een buitenlandse autoriteit te verstrekken voor een ander doel dan waarvoor die gegevens in eerste instantie zijn verkregen. Wij wijzen er verder op dat de beperkingsgronden onder artikel 21 AVG ruimer zijn dan onder artikel 43 Wbp. Mogelijk is er nog een ander verschil tussen artikel 21 AVG enerzijds en (artikel 13 Privacyrichtlijn en) artikel 43 Wbp anderzijds. Artikel 43 Wbp is de wettelijke maatregel als bedoeld in artikel 13 Privacyrichtlijn. Het is de vraag of een en ander met de wettelijke maatregelen zoals genoemd in artikel 21 AVG er in de praktijk anders uit komt te zien. Wij hebben hiervoor geen aanwijzingen gevonden. Tot slot is van belang dat het CBP bij verstrekking van persoonsgegevens aan derde landen onder de AVG een belangrijkere rol krijgt.

5 Conclusies

Als een Nederlandse autoriteit op grond van een Europeesrechtelijke of nationaalrechtelijke regeling gegevens aan een buitenlandse autoriteit beoogt te verstrekken, zal steeds moeten worden bezien of van die gegevens ook persoonsgegevens onderdeel uitmaken. Als dat het geval is, zullen ten aanzien van die gegevens de bepalingen over de bescherming van persoonsgegevens in acht moeten worden genomen, onafhankelijk van het antwoord op de vraag of dat in de desbetreffende regeling waarin de verstrekkingsgrondslag is opgenomen, is bepaald. Wij hebben gesignaleerd dat de Europese wetgever in dit verband niet consequent is in de formuleringen. Dat zou mogelijk tot verwarring over de toepasselijkheid van de privacyregelgeving kunnen leiden.

Regelgeving waarin een verstrekkingsgrondslag is opgenomen, zal er in het gros van de gevallen toe leiden dat er voor de Nederlandse autoriteit een grondslag in artikel 8 onder c (wettelijke verplichting), e (publiekrechtelijke taak) of f (gerechtvaardigd belang) Wbp zal kunnen worden gevonden om persoonsgegevens aan een buitenlandse counterpart te verstrekken. Als sprake is van een wettelijke verplichting om gegevens te verstrekken zal naar ons oordeel niet aan de eis van verenigbaar gebruik van artikel 9 Wbp hoeven te worden getoetst. Als sprake is van een verstrekkingsbevoegdheid waar een vergaarmogelijkheid aan is gekoppeld, zal van onverenigbaar gebruik geen sprake zijn. Extra oplettendheid is vereist als het voornemen bestaat bijzondere persoonsgegevens, zoals strafrechtelijke gegevens, aan een buitenlandse autoriteit te verstrekken. Er zal dan eerst beoordeeld moeten worden of sprake is van een van de doorbrekingsgronden uit de artikelen 17 tot en met 23 Wbp. Het verdient aanbeveling dat de (Europese en nationale) wetgever er – bijvoorbeeld in de toelichting bij de desbetreffende verstrekkingsbepaling – expliciet aandacht aan besteedt of de betreffende bepaling ook een verplichting of bevoegdheid in het leven roept om bijzondere persoonsgegevens te verstrekken. Ook bij de doorgifte van persoonsgegevens aan derde landen moet extra oplettendheid worden betracht. Er moet in de eerste plaats beoordeeld worden of het derde land een passend beschermingsniveau kent. Is dat niet het geval, dan zal zo mogelijk ofwel een vergunning van de minister van Veiligheid en Justitie moeten worden verkregen, ofwel een overeenkomst conform een modelcontract met het desbetreffende derde land moeten worden gesloten. Als dat niet mogelijk is, zal eventueel een beroep kunnen worden gedaan op de (strikt te interpreteren) omstandigheid dat de doorgifte noodzakelijk is vanwege een zwaarwegend algemeen belang. Tot slot is relevant dat een betrokkene in beginsel over de voorgenomen verstrekking moet worden geïnformeerd, tenzij één of meer van de belangen als bedoeld in artikel 43 Wbp daaraan in de weg staan.

Als de Algemene Verordening Gegevensbescherming in werking treedt, zal de kern van het regime van de Wbp niet drastisch veranderen. Wel biedt de AVG, gelet op artikel 6 lid 4 AVG, een (extra) specifieke mogelijkheid om gegevens aan een buitenlandse autoriteit te verstrekken voor een ander doel dan waarvoor die gegevens in eerste instantie zijn verkregen. Wij wijzen er verder op dat de beperkingsgronden onder artikel 21 AVG ruimer zijn dan onder artikel 43 Wbp. Mogelijk is er nog een ander verschil tussen artikel 21 AVG enerzijds en (artikel 13 Privacyrichtlijn en) artikel 43 Wbp anderzijds. Artikel 43 Wbp is de wettelijke maatregel als bedoeld in artikel 13 Privacyrichtlijn. Het is de vraag of een en ander met de wettelijke maatregelen zoals genoemd in artikel 21 AVG er in de praktijk anders uit komt te zien. Wij hebben hiervoor geen aanwijzingen gevonden. Voor verstrekking aan derde landen gaat toestemming van het CBP een belangrijke(re) rol spelen. De mogelijkheid om een vergunning te verkrijgen van de minister van Veiligheid en Justitie vervalt.

6 Aanbevelingen/stellingen

1. De Europese wetgever moet – in ieder geval binnen een en dezelfde verordening – op een eenduidige manier bepalen of de privacyregelgeving in acht moet worden genomen als persoonsgegevens zullen worden verwerkt (paragraaf 2.2).
2. Verstrekkingsbepalingen moeten worden toegespitst op de verwerking van bijzondere persoonsgegevens als de wetgever die verwerking mogelijk wil maken, omdat anders niet zeker is dat het verwerkingsverbod kan worden doorbroken (paragraaf 3.4 en 4.4).

7 Onderzochte regelingen

7.1 Onderzochte Europese verordeningen met bepalingen over het verstrekken van gegevens aan buitenlandse autoriteiten

1. Verordening 2006/2004 van het Europees Parlement en de Raad van 27 oktober 2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming (PbEU 2004, L 149/2)
2. Verordening (EG) 1/2003 van de Raad van 16 december 2001 betreffende de uitvoering van de mededingingsregels van de artikelen 81 en 82 van het Verdrag (PbEU 2003, L 1/1)
3. Verordening 389/2012 van de Raad van 2 mei 2012 betreffende administratieve samenwerking op het gebied van de accijnzen en houdende intrekking van Verordening (EG) nr. 2073/2004 (PbEU 2012, L 121/1)
4. Verordening 883/2004 van het Europees Parlement en de Raad van 29 april 2004 betreffende de coördinatie van de socialezekerheidsstelsels (PbEU 2004, L 166/1)
5. Verordening 1408/71 van de Raad van 14 juni 1971 betreffende de toepassing van de socialezekerheidsregelingen op werknemers en zelfstandigen, alsmede op hun gezinsleden, die zich binnen de Gemeenschap verplaatsen (PbEU 1971, L 149/2)
6. Verordening 515/97 van de Raad van 13 maart 1997 betreffende de wederzijdse bijstand tussen de administratieve autoriteiten van de lidstaten en de samenwerking tussen deze autoriteiten en de Commissie met het oog op de juiste toepassing van de douane- en landbouwvoorschriften (PbEU 1997, L 82/1)
7. Verordening (EG) 56/2006 van het Europees Parlement en de Raad van 15 maart 2006 tot harmonisatie van bepaalde voorschriften van sociale aard voor het wegvervoer, tot wijziging van Verordeningen (EEG) nr. 3821/85 en (EG) nr. 2135/98 van de Raad en tot intrekking van Verordening (EEG) nr. 3820/85 van de Raad (PbEU 2006, L 102/1)
8. Verordening 1071/2009 van het Europees Parlement en de Raad van 21 oktober 2009 tot vaststelling van gemeenschappelijke regels betreffende de voorwaarden waaraan moet zijn voldaan om het beroep van wegvervoerondernemer uit te oefenen en tot intrekking van Richtlijn 96/26/EG van de Raad (PbEU 2009, L 300/51)
9. Verordening 882/2004 van het Europees Parlement en de Raad van 29 april 2004 inzake officiële controles op de naleving van de wetgeving inzake diervoeders en levensmiddelen en de voorschriften inzake diergezondheid en dierenwelzijn (PbEU 2004, L 165/1)

10. Verordening 1/2005 van de Raad van 22 december 2004 inzake de bescherming van dieren tijdens het vervoer en daarmee samenhangende activiteiten en tot wijziging van de Richtlijnen 64/432/EEG en 93/119/EG en van Verordening (EG) nr. 1255/97 (PbEU 2005, L 3/1)

7.2 Onderzochte nationale wetgeving met bepalingen over het verstrekken van gegevens aan buitenlandse autoriteiten

11. Dienstenwet
12. Instellingswet Autoriteit Consument en Markt
13. Wet bescherming persoonsgegevens
14. Wet op het financieel toezicht
15. Wet op de internationale bijstandsverlening bij de heffing van belastingen
16. Telecommunicatiewet

Big Data – Fundamentele rechten in een fundamenteel veranderende wereld

*Mr. A. de Jong**

* Mr. Arjan de Jong is werkzaam bij de directie Burgerschap en informatiebeleid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Dit preadvies is op persoonlijke titel geschreven.

1 Inleiding

1.1 Een veranderende wereld

De ontwikkeling van onze informatiemaatschappij gaat in een hoog tempo en lijkt te versnellen. Dit is duidelijk te zien aan snel opeenvolgende innovaties op het vlak van ICT, maar ook bij andere steeds meer met ICT convergerende disciplines, zoals bio-, nano- en cognitieve technologie.[1] Alhoewel de aanduidingen van deze ontwikkelingen, zoals *cloud computing* en het *internet of things*, uit commercieel oogpunt door het bedrijfsleven met *buzz words* en hypes worden omgeven, zijn het ontwikkelingen die wezenlijke gevolgen voor onze maatschappij met zich meebrengen. Een laatste ontwikkeling die op steeds meer maatschappelijke belangstelling heeft mogen rekenen en die in de bredere trend van ontwikkelingen past, is Big Data.[2]

Big Data is, in het kort, een verzamelnaam voor het met hoge snelheid verzamelen en analyseren van grote hoeveelheden diverse gegevens.[3] Op de resultaten hiervan kan door mensen of geautomatiseerd actie ondernomen worden. Big Data wordt mogelijk gemaakt door het feit dat steeds meer gegevens verzameld en gedeeld (kunnen) worden, de kosten van opslag en het verwerken van deze gegevens drastisch dalen en de methoden van analyse verbeteren. Denk hierbij niet alleen aan het verzamelen van persoonsgegevens op het world wide web, bijvoorbeeld met behulp van cookies, maar ook aan het verzamelen van persoonsgegevens in de fysieke wereld, zoals het bijhouden van hartslag en bloeddruk door nieuwe 'slimme' fitnessbandjes. Het gaat echter niet alleen om persoonsgegevens, maar ook om bijvoorbeeld meteorologische informatie, informatie over de staat van rivier- of zeedijken of andere infrastructuur, en bedrijfsprocessen die gemonitord worden met behulp van sensoren. De hoeveelheid digitale informatie die elk jaar wordt gemaakt, neemt enorm toe. In 2013 werd 90% van alle informatie ter wereld in de laatste twee jaar gecreëerd en zeker is dat deze groei zich doorzet.[4]

1 Rathenau Instituut, *Intieme technologie: de slag om ons lichaam en gedrag*, Den Haag: Rathenau Instituut 2014.

2 Volgens de 2014 Gartner Hype Cycle Special Report is Big Data in 2014 op zijn top qua hype, waarna ontnuchtering plaatsvindt. B. Burton & D.A. Willis, *Gartner's Hype Cycle Special Report for 2014*, www.gartner.com.

3 Een nadere definiëring wordt in hoofdstuk 2 gegeven.

4 Åse Dragland, 'Big Data – for better or worse', www.sintef.no/home/Press-Room/Research-News/Big-Data–for-better-or-worse/ (geraadpleegd op 3 september 2014).

Economische machtsblokken als de Verenigde Staten[5] en de Europese Unie[6] zien grote maatschappelijke en economische kansen voor de inzet van Big Data. Tegelijkertijd brengt het, zoals elke technologische ontwikkeling, ook mogelijke risico's met zich mee. Deze spelen in het bijzonder ten aanzien van de bescherming van fundamentele rechten.[7] Dit roept fundamentele vragen op ten aanzien van de adequaatheid van huidige regelgeving en de invulling daarvan. De herziening van de Privacyrichtlijn (Richtlijn 95/46/EG) in de vorm van de voorgestelde Algemene Verordening Gegevensbescherming (AVG) moet dan ook mede in dat licht bekeken worden.[8]

1.2 Onderzoek

In dit preadvies wordt onderzocht wat de gevolgen van het inzetten van Big Data zijn voor fundamentele rechten, in het bijzonder voor de bescherming van de persoonlijke levenssfeer,[9], de bescherming van persoonsgegevens,[10] het non-discriminatiebeginsel,[11] de vrijheid van gedachte[12] en de vrijheid van meningsuiting.[13] Centraal in dit preadvies staat hierbij dat de technologische ontwikkelingen niet uitsluitend in de sleutel van privacyvraagstukken geformuleerd dienen te worden, maar juist in de sleutel van een samenspel van fundamentele rechten en de onderliggende ethische overwegingen. Voor de bescherming van deze fundamentele rechten wordt het gegevensbeschermingsrecht als belangrijk instrument gezien.

Om een antwoord op deze te vraag te kunnen formuleren zal in hoofdstuk 2 het begrip Big Data nader onderzocht en gedefinieerd worden. Aansluitend wordt Big Data in relatie gebracht tot enkele andere technologische ontwikkelingen die van belang zijn om de gevolgen van Big Data voor fundamentele rechten te duiden. Vervolgens zal in hoofdstuk 3 een overzicht gegeven worden van de (internationaal) juridische grondslag voor de genoemde fundamentele rechten in relatie tot technologische ontwikkelingen in de maatschappij. In de vier opvolgende hoofdstukken zal vervolgens een viertal thema's behandeld worden om de gevolgen van Big Data voor de persoonlijke levenssfeer, de bescherming van persoonsgegevens,

5 Executive Committee of the White House, *Big Data: Seizing Opportunities, preserving values*, 1 mei 2014.

6 Mededeling van de Europese Commissie, *Naar een bloeiende data-economie*, 2 juli 2014.

7 Big Data kan echter ook gevolgen hebben op het vlak van mededinging en consumentenbescherming. Zie onder andere European Data Protection Supervisor, *Preliminary opinion on privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, mei 2014.

8 Voorstel voor een verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene Verordening Gegevensbescherming), COM(2012)/11 final, 25 januari 2012.

9 Artikel 8 EVRM, artikel 7 Handvest van de grondrechten van de Europese Unie (hierna: Handvest EU), artikel 16 Verdrag betreffende de werking van de Europese Unie.

10 Artikel 8 Handvest EU.

11 Artikel 14 EVRM, artikel 1 Algemene wet gelijke behandeling, artikel 21 Handvest EU.

12 Artikel 9 EVRM, artikel 10 Handvest EU, artikel 18 Universele verklaring van de rechten van de mens.

13 Artikel 10 EVRM en artikel 11 Handvest EU.

het non-discriminatie beginsel, de vrijheid van gedachte en de vrijheid van meningsuiting te duiden. Allereerst zal worden geanalyseerd wat Big Data betekent voor de positie van het individu te midden van Big Data aan de hand van het in het gegevensbeschermingsrecht centrale begrip persoonsgegeven. In hoofdstuk 5 wordt ingegaan op transparantie van en voor het individu. In hoofdstuk 6 worden de gevolgen van Big Data in de context van geautomatiseerde besluitvorming onderzocht. Ten slotte zal het gebruik van Big Data door de overheid besproken worden en wordt afgesloten met een conclusie.

2 Big Data

2.1 Definitie van Big Data

In de inleiding is Big Data kort beschreven. Voor een goed begrip hiervan is echter een nadere analyse vereist. Informatie wordt namelijk al decennia met behulp van ICT verwerkt, hierbij gebruikmakend van statistiek, in bijvoorbeeld de financiële en retailsector. Verwante begrippen zijn *data mining* en *business intelligence*. Dit roept vragen op naar de betekenis van Big Data.

Wanneer naar een definitie van Big Data wordt gevraagd, lopen de antwoorden uiteen, vaak afhankelijk van het perspectief van de geïnterviewde.[14] Big Data wordt door de Europese Commissie gedefinieerd als '(...) grote hoeveelheden data van diverse aard die met hoge snelheid uit een groot aantal bronnen van diverse aard worden gehaald. Voor het verwerken van de zeer uiteenlopende realtime datasets die momenteel ter beschikking staan, zijn nieuwe instrumenten en methoden nodig, zoals sterke processors, software en algoritmen.'[15] Gartner omschrijft het als 'Big data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.' De centrale eigenschappen zijn derhalve snelheid, volume en verscheidenheid van de data en de verwerking hiervan, en het kosteneffectief verkrijgen van nieuwe inzichten en het maken van keuzes op basis van deze data.[16] Wat onder 'groot' of 'big' moet worden verstaan, is gezien de snelle ontwikkelingen op het vlak van verwerkings- en opslagcapaciteit relatief. Dit zal veranderen met de tijd en is sectorafhankelijk.[17] Om de gevolgen van Big Data te kunnen duiden valt binnen dit preadvies het gehele proces van verzamelen, opslaan, verwerken/analyseren en het maken van keuzes op basis van de data binnen de definitie van Big Data. Met name de laatste onderscheide stap is van belang, omdat op deze wijze met Big Data direct invloed op individuen en onze maatschappij kan worden uitgeoefend.

De enorme groei aan hoeveelheid data wordt voornamelijk door twee ontwikkelingen mogelijk gemaakt. Allereerst dalen de kosten van het opslaan van gegevens

14 Een onderzoek van de University Berkely leverde 42 definities op. http://datascience.berkeley.edu/what-is-big-data/ (geraadpleegd op 10 september 2014).

15 Mededeling van de Europese Commissie, *Naar een bloeiende data-economie*, 2 juli 2014.

16 In het Engels wordt verwezen naar de '3 V's' van velocity, volume en variety. Zie Executive Office of the President, *Big data: Seizing opportunities, preserving values*, mei 2014, p. 4.

17 Zie de definitie van McKinsey '(...) This definition is intentionally subjective and incorporates a moving definition of how big a dataset needs to be in order to be considered big data (...) Also note that the definition can vary by sector (...)'. McKinsey Global Institute, *Big data: The next frontier for innovation, competition, and productivity*, juni 2011, p. 1.

die (steeds meer) standaard door organisaties verzameld en verwerkt worden. Zo kunnen deze tegen lagere kosten worden opgeslagen.[18] Ten tweede kan de toename worden toegeschreven aan de grote stappen die gemaakt zijn op het gebied van sensortechnologie. Denk aan een smartphone die tegenwoordig standaard met zo'n dertien sensoren en vele verbindingsmogelijkheden uitgerust is.[19] De productie- en inzetkosten van sensoren lopen snel terug en het formaat wordt steeds kleiner, waardoor gebruik van sensoren binnenkort niet meer is voorbehouden aan de hightechindustrie.[20] Ze worden al steeds breder ingezet bij domotica (het automatiseren van woningen).[21] De inzet van sensoren zal de komende jaren doordringen in alle sectoren van de economie, zowel voor consumenten als voor bedrijven en overheden.

De data kunnen continu (in *real time*) en met grote snelheid worden verzameld door de toegenomen mogelijkheden om (draadloze) netwerk- en internetverbindingen te gebruiken. Dit wordt ook wel omschreven als het *internet of things*, dat uitgebreide machine-naar-machinecommunicatie mogelijk maakt. Ook hierdoor kunnen sensoren tegen lage kosten breed ingezet worden.[22]

Bij Big Data verschilt de aard van de gegevens in grote mate; het gaat om heterogene data. Het kunnen foto's, audiobestanden, video, tekst, binaire data, geolocatiegegevens of simpelweg andersoortige gegevens uit sensoren zijn, en dat alles gestructureerd of ongestructureerd, persoonsgegevens en niet-persoonsgegevens.

Nieuwe analysetechnieken maken het mogelijk om deze grote hoeveelheden data die snel verzameld worden en die sterk gevarieerd zijn te analyseren en hier informatie en nieuwe kennis uit te halen. Waar echter in het verleden gewerkt werd met een hypothese en (representatieve) steekproef, is bij Big Data het 'gebruik alles en zoek de verbanden'-principe leidend. Hierbij gaat het derhalve om het zoeken van verbanden in enorme hoeveelheden data die op zichzelf weinig informatie prijsgeven, maar met behulp van geavanceerde algoritmen nieuwe inzichten bieden.[23] Hierbij staan correlaties centraal, niet het vaststellen van causaliteit.[24] Op basis van deze correlaties kunnen modellen worden gemaakt waarmee toekomstige ontwikkelingen voorspeld kunnen worden.

---

18 www.zdnet.com/storage-in-2014-an-overview-7000024712/ (geraadpleegd op 15 september 2014).

19 Denk aan microfoon, camera, gps, nabijheidssensor, lichtmeter, gyroscoop, magnetometer (kompas), versnellingsmeter, thermometer, touchscreen, NFC, wifi, Bluetooth, vingerafdrukscanner.

20 www.cio.com/article/2606003/consumer-technology/stanfords-ant-sized-radios-could-connect-the-world.html (geraadpleegd op 13 september 2014).

21 Verwacht wordt dat in 2022 elke woning gemiddeld 500 'slimme' apparaten bevat. www.gartner.com/newsroom/id/2839717 (geraadpleegd op 13 september).

22 www.cio.com/article/2604262/firechats-developer-wants-to-give-iot-a-meshnetwork-boost.html (geraadpleegd op 13 september 2014).

23 Een algoritme is een verzameling van stappen die gevolgd worden om een probleem op te lossen. Zie www.merriam-webster.com/dictionary/algorithm.

24 Correlatie geeft aan dat er een statistisch significant verband is tussen X en Y. Als bijvoorbeeld X zich voordoet, doet Y zich ook voor. Correlatie is probabilistisch van aard. Causaliteit betekent een duidelijke oorzaak en gevolg. X veroorzaakt Y. Deze natuurwetenschappelijke causaliteit is niet altijd hetzelfde als juridische causaliteit. De criteria voor de vaststelling van de laatste

Data spreken niet voor zichzelf. Data moeten worden verzameld en worden verwerkt met algoritmen, en vervolgens dient de uitkomst van de analyse geïnterpreteerd te worden. In alle drie de stadia kunnen mogelijk vertekeningen optreden.[25] Zo zal zelfs als er sprake is van een grote hoeveelheid verzamelde data, slechts een gedeelte van de werkelijkheid verzameld worden. Ten tweede zal van deze gegevens een representatie van deze werkelijkheid worden gemaakt. Er wordt, in andere woorden, een model of abstractie van de werkelijkheid gemaakt. Vervolgens komen met behulp van algoritmen tijdens de analysefase verschillende (soorten) verbanden bovendrijven. Ten slotte dienen de uitkomsten hiervan weer geïnterpreteerd te worden door mens of machine.

Het gebruik van Big Data als instrument voor het genereren van nieuwe inzichten is derhalve geen sinecure en vereist een grote hoeveelheid kennis van statistiek en kennisrepresentatie.

2.2 Big Data als onderdeel van grotere technologische verandering

In paragraaf 2.1 is beschreven wat Big Data omhelst en welke technologische ontwikkelingen Big Data mogelijk maken. Andersom is Big Data ook een *enabler* die andere technologische ontwikkeling mogelijk maakt en voortstuwt. Om de ontwikkeling van Big Data en de gevolgen ervan voor fundamentele rechten te doorgronden zal Big Data dan ook in de context van deze toekomstige ontwikkelingen geplaatst moeten worden.

In het rapport *Intieme technologie* van het Rathenau Instituut wordt deze ontwikkeling als volgt verwoord: 'We beleven thans het historische omslagpunt waarop de afstand tussen technologie en onszelf in hoog tempo kleiner wordt.'[26] Dit wordt veroorzaakt door een convergentie van nano-, biomedische-, informatie- en cognitieve technologie (NBIC). Hiermee vervagen steeds meer de grenzen tussen de digitale (ICT) en de biologische en fysieke wereld. Er treedt een versmelting tussen NBIC-technologie en de mens op, steeds meer technologie komt in ons, tussen ons, over ons en wordt als ons.[27] De eerste ontwikkelingen hiervan zijn al zichtbaar bij de snelle ontwikkeling van *wearables*, slimme apparatuur die ons niet alleen informatie over de staat van de wereld geeft, maar vooral over onze interne staat, zoals hartslag, glucoseniveaus, stressniveau en zelfs hersenactiviteit.[28] Er wordt wel gesproken over de *quantified self*.[29] Daarnaast maakt deze NBIC-convergentie mogelijk dat onze leefwereld steeds adaptiever gemaakt kan worden,

---

verschilt per rechtsgebied, zoals strafrecht, civielrecht, bestuursrecht. Zo is in het civielrecht toerekening een belangrijk element. Zie ook A.J. Akkermans, 'Causaliteit bij letselschade en medische expertise', *Tijdschrift voor vergoeding personenschade* 2003-4, p. 93-104.

25 http://blogs.hbr.org/2013/04/the-hidden-biases-in-big-data/ (geraadpleegd op 1 november 2014).

26 Rathenau Instituut 2014, p. 8.

27 Rathenau Instituut 2014, p. 10.

28 Waar EEG-scanners voorheen voorbehouden waren aan ziekenhuizen, zijn ze tegenwoordig ook binnen bereik van consumenten. Zie http://interaxon.ca. Ethici vrezen dat hiermee de laatste privacybarriere op termijn geslecht gaat worden, namelijk de beslotenheid van onze gedachten. Zie D.J. Church, 'Neuroscience in the Courtroom: An International Concern', *William & Mary Law Review* 53-5, p. 1826-1853.

29 http://ecp.nl/item/4158 (geraadpleegd op 21 oktober 2014).

steeds meer aanpasbaar, al dan niet aangestuurd door kunstmatige intelligentie. Dit betreft niet alleen bekende voorbeelden als thermostaten[30] die zich aanpassen aan het leefpatroon van bewoners van een huis, maar eveneens zichzelf organiserende of zelfs bouwende (mini)robots.[31] Ten slotte wordt een steeds nauwere verbondenheid van ICT en levende wezens, inclusief mensen, mogelijk. Een van de verstrekkendste ontwikkelingen hiervan is hersen-machinecommunicatie, ook wel *mind-machine communication* genoemd, die mogelijk gemaakt wordt door cognitieve technologie en waarvan nu al praktische toepassingen mogelijk zijn.

Big Data is zowel een gevolg als een voorwaarde voor deze vergaande ontwikkelingen. De versmelting van mens en machine en de versmelting van de omgeving met technologie brengen toenemende mogelijkheden voor het verzamelen van informatie met zich mee. Ten tweede kunnen met deze informatie steeds verdergaande analyses uitgevoerd worden. Ten slotte kan er door de versmelting van technologie in onszelf en onze omgeving ook steeds meer controle over onze digitale en fysieke wereld en onszelf uitgeoefend worden. Deze onderdelen staan centraal in de hierop volgende hoofdstukken.

30 Denk aan het bedrijf NEST, dat slimme, zichzelf automatisch configurerende thermostaten en rookalarmen produceert.

31 http://wyss.harvard.edu/viewpressrelease/162 en www.seas.harvard.edu/news/2014/08/self-organizing-thousand-robot-swarm (geraadpleegd op 21 oktober 2014).

3 Samenspel van fundamentele rechten in een wereld met Big Data

Evenals Big Data niet alleen op zichzelf bekeken dient te worden, geldt dit ook voor de fundamentele rechten die door deze ontwikkelingen worden geraakt. Zoals in de introductie aangegeven, gaat het hierbij in het bijzonder om de nauw met elkaar verbonden bescherming van de persoonlijke levenssfeer, de bescherming van persoonsgegevens, non-discriminatie, de vrijheid van gedachte en de vrijheid van meningsuiting. Deze fundamentele rechten zullen in samenhang besproken worden, omdat ze elkaar ondersteunen en versterken. De fundamentele rechten hebben, in andere woorden, naast een eigenstandig ook een zeker complementair en zelfs instrumenteel karakter ten opzichte van elkaar. Zo is de bescherming van persoonsgegevens instrumenteel bij het beschermen van de persoonlijke levenssfeer, non-discriminatie en de vrijheid van gedachte.[32] Eveneens zijn de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer instrumenteel aan de vrijheid van meningsuiting.[33] Tegelijkertijd kan er juist ook spanning ontstaan tussen deze rechten.[34]

Uit de grote hoeveelheid jurisprudentie die zich rond deze fundamentele rechten heeft ontwikkeld, kunnen de bescherming van de persoonlijke autonomie,[35] keuzevrijheid,[36] fysieke en psychische integriteit van het individu[37] en een vrije stroom van denkbeelden als basis voor zelfontwikkeling[38] als kernpunten worden gezien. Naast het belang van de ontwikkeling van het individu en het waarborgen van zijn vrijheden worden deze rechten ook gezien als waarborgen voor het goed functioneren van een pluriforme democratische samenleving.

---

32 Dit gegeven komt expliciet naar voren in de considerans van Richtlijn 95/46/EG. Het Duitse Bundesverfassungsgericht maakte deze verbinding al in 1983. Zie BVerfG 15 december 1983, 65.

33 Vergelijk HvJ 8 april 2014, zaken C-293/12 en C-594/12, r.o. 28.

34 EHRM 24 juni 2004, 59320/00 (Von Hannover).

35 EHRM 12 juni 2014, 56030/07 (Fernández Martínez vs. Spain); EHRM 29 april 2002, 2346/02 (Pretty vs. the United Kingdom); EHRM 15 januari 2009, 1234/05 (Reklos and Davouris vs. Greece); EHRM 10 april 2007, 6339/05 (Evans vs. the United Kingdom). Zie ook N.R. Koffeman, '(The right to) personal autonomy in the case law of the European Court of Human Rights', http://bit.ly/1xevIe6.

36 EHRM 18 mei 1976, 6825/74 (X. vs. Iceland). Zie T. Gomez-Arostequi, 'Defining private life under the European Convention on Human Rights by referring to reasonable expectations', *California Western International Law Journal* 2005, 35 (2), p. 161.

37 EHRM 4 december 2008, NJ 2009/410 (S. and Marper vs. United Kingdom), r.o. 66.

38 EHRM 8 juli 1986, 9815/82 (Lingens vs. Austria), r.o. 41 en EHRM 18 juli 2000, 26680/25 (Sener vs. Turkey), r.o. 39.

De hiervoor genoemde fundamentele rechten zijn niet van absolute aard. In casu dient te worden gekeken naar de functie ervan in de samenleving en dient er een afweging te worden gemaakt tussen (individuele en publieke) conflicterende rechten en belangen.[39]

Ondanks dat fundamentele rechten voortvloeiend uit het Europees Verdrag voor de rechten van de mens (EVRM) in principe tussen de staat en de burger gelden, wordt in de Straatsburgse jurisprudentie ook in bepaalde gevallen een positieve verplichting aan de verdragsstaten opgelegd om de in het verdrag neergelegde rechten tevens in horizontale verhoudingen, tussen burgers onderling en daarmee ook tussen burgers en niet-statelijke actoren, te beschermen.[40] De mate van bescherming die geboden moet worden tegen bijvoorbeeld inbreuken op de persoonlijke levenssfeer kan met de tijd veranderen en is onder andere afhankelijk van toekomstige geavanceerde technologieën die inbreuken mogelijk maken.[41]

De verhouding tussen de fundamentele rechten kan op velerlei wijze gekenschetst worden. Wanneer de nadruk echter op de vier hiervoor genoemde kernpunten van persoonlijke autonomie, keuzevrijheid, integriteit en vrije stroom van denkbeelden gelegd wordt, kan het in figuur 1 verbeelde proces onderscheiden worden. Hierbij gaat het in het bijzonder om de onderlinge verhoudingen en niet of ze in een specifieke context succesvol ingeroepen zouden kunnen worden jegens de staat of een derde.

Een burger heeft in beginsel de vrijheid om een mening te koesteren en inlichtingen en denkbeelden te ontvangen of te uiten, tenzij de beperking in de wet voorzien is en noodzakelijk is in een democratische samenleving en in het belang is van de nauw omschreven gronden van artikel 10 lid 2 EVRM. De vrijheid om informatie te ontvangen is een belangrijk aspect van de zelfontwikkeling van het individu en een pluriforme democratische samenleving. Zonder vrije nieuwsgaring wordt de stroom van ideeën binnen de maatschappij en daarmee naar individuen bemoeilijkt.[42]

In de eigen persoonlijke levenssfeer kan het individu zonder interferentie van buitenaf zijn eigen persoonlijkheid, identiteit en opvattingen, mede gebaseerd op denkbeelden ontvangen van andere partijen, vormgeven.[43] Dit aspect kan

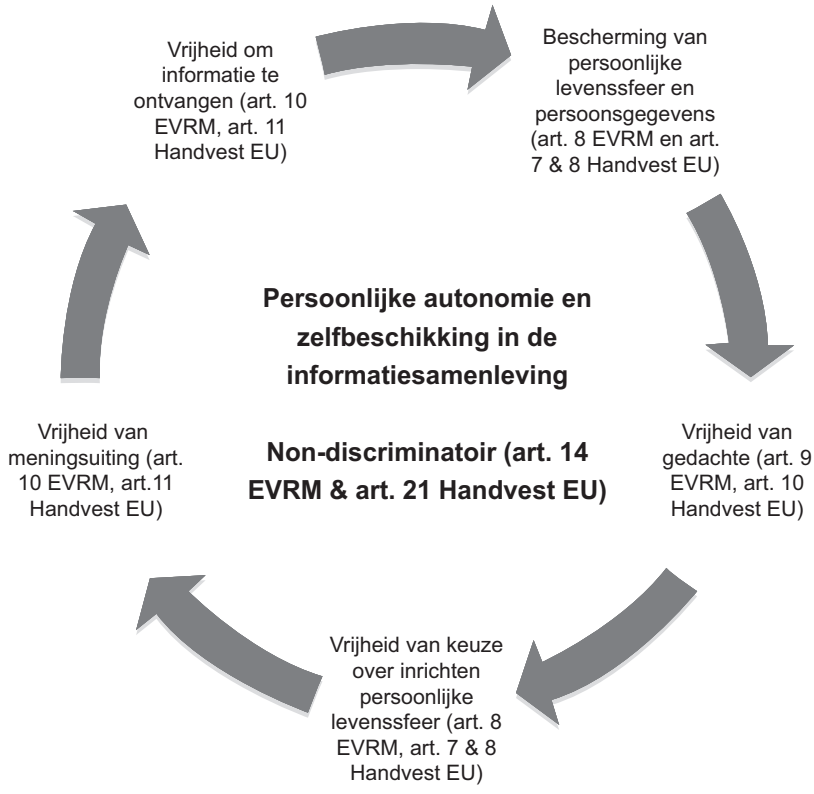
39 HvJ 9 november 2010, zaken C-92/09 en C93/09 (Volker and Markus Schecke vs. Land Hessen), r.o. 48.

40 EHRM 8 juli 2003, 36022/97 (Hatton et al. vs. United Kingdom) en EHRM 24 juni 2004, 59320/00 (Von Hanover), r.o. 57.

41 EHRM 4 december 2008, NJ 2009/410 (S. en Marper vs. Verenigd Koninkrijk), r.o. 71.

42 De vrije stroom van ideeën kan ook in economisch opzicht van groot belang worden geacht. Recente sociaalpsychologische studies, uitgevoerd met moderne technologie en Big Data-analyse waarmee de interactie tussen personen en groepen kan worden geanalyseerd, tonen een sterke relatie tussen een vrije stroom van ideeën en innovatie en hiermee economisch succes aan. Zie A. Pentland, *Social Physics: How Good Ideas Spread – The Lessons from a New Science*, New York: Penguin Press 2014.

43 In de literatuur wordt hierbij een onderscheid gemaakt tussen de *ipse*-identiteit, het reflectieve zelfbewustzijn een uniek individu te zijn, en de *idem*-identiteit, waarmee we ons positioneren in de wereld, bijvoorbeeld sociaal, cultureel, economisch en juridisch. Zie o.a. P.J.A. de Hert, *A right to identity in the face of the internet of things*, Straatsburg: Unesco 2008, p. 1.



Figuur 1

gekwalificeerd worden als negatieve vrijheid, vrij zijn van inmenging. Deze persoonlijke levenssfeer wordt beschermd door artikel 8 EVRM, dat als gekwalificeerd recht wederom alleen mag worden ingeperkt onder de condities van lid 2. In het verlengde van de bescherming van de persoonlijke levenssfeer ligt de bescherming van persoonsgegevens, om zo (volledige) transparantie van de persoonlijke levenssfeer te voorkomen.[44] De verwerking van persoonsgegevens is nodig voor het goed functioneren van de maatschappij, maar de verwerking ervan is gereguleerd. Een nadere invulling van het recht op bescherming van persoonsgegevens wordt gegeven door Conventie 108,[45] Richtlijn 95/46/EG en de hiervan afgeleide Wet bescherming persoonsgegevens (Wbp). Zowel de richtlijn als de conventie ondergaat momenteel een vernieuwingsslag. Ter vervanging van de richtlijn is de Algemene Verordening Gegevensbescherming in januari 2012 door de Europese Commissie gepresenteerd. Het Europese Parlement heeft in eerste lezing zijn positie bepaald, de onderhandelingen in de Raad duren nog

44 In feite reguleert dit de vrijgave en het verwerken van attributen van de *idem*-identiteit aan de buitenwereld, de persoonsgegevens.

45 Conventie 108 voor de bescherming van individuen in relatie tot de geautomatiseerde verwerking van persoonsgegevens, ook wel Verdrag van Straatsburg van 1981 genoemd, valt binnen het juridisch kader van de Raad van Europa. http://conventions.coe.int/Treaty/en/Treaties/html/108.htm.

voort. Over modernisering van Conventie 108 wordt momenteel onderhandeld in Straatsburg.

In het verlengde van vrije vorming van persoonlijkheid, identiteit en opvattingen ligt de vrijheid van gedachte, die zijn grondslag vindt in artikel 9 EVRM, waarin in het eerste lid wordt gesteld: 'een ieder heeft recht op vrijheid van gedachte, geweten en godsdienst (...)'. De meeste jurisprudentie omtrent artikel 9 EVRM ziet op de vrijheid van godsdienst, maar ook het hebben van principes of overtuigingen zoals veganisme,[46] pacifisme[47] en atheïsme[48] vallen onder dit recht. Het recht kan in twee delen worden onderscheiden, namelijk ten aanzien van het *forum internum* en het *forum externum*.[49] Het *forum internum* betreft de eigenlijke gedachte of overtuiging van een persoon, zonder dat deze gedachte zich door een handeling in de buitenwereld gemanifesteerd heeft.[50] Zo kan iemand een voorkeur voor een politicus hebben die pas geopenbaard wordt en bewezen kan worden door het uitbrengen van een stem.[51] De bescherming van het *forum internum* is hoofdzakelijk een negatieve vrijheid. Het *forum externum* betreft het handelen in overeenstemming met de overtuiging, gedachte of het geloof, een vorm van positieve vrijheid. Dit aspect heeft met name betrekking op het tweede deel van het eerste lid van het artikel: '(...) dit recht omvat tevens de vrijheid om van godsdienst of overtuiging te veranderen, alsmede de vrijheid hetzij alleen, hetzij met anderen, zowel in het openbaar als privé zijn godsdienst te belijden of overtuiging tot uitdrukking te brengen in erediensten, in onderricht, in praktische toepassing ervan en in het onderhouden van geboden en voorschriften.' Alleen het belijden van een godsdienst of het uiten van een overtuiging kan aan beperkingen worden onderworpen, het *forum internum* niet.[52] In jurisprudentie die zich tot op heden heeft ontwikkeld omtrent artikel 9 EVRM waren de eisen van de eiser met name gericht op het kunnen uitoefenen van activiteiten op het *forum externum* en niet ongeoorloofde inmenging in het *forum internum*. De jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) heeft zich dan ook gericht op rechtsvragen met betrekking tot het *forum externum*, wat de vraag oproept hoe het Hof een beroep op uitsluitend het *forum internum* zal behandelen, in het bijzonder in de context van horizontale verhoudingen.[53] De mogelijkheden om direct en indirect invloed uit te oefenen op cognitieve processen van personen nemen namelijk sterk toe, wat een bedreiging kan vormen voor de vrijheid van gedachte in het *forum internum*. Zo kunnen op basaal niveau al met fMRI-techniek gezichten die mensen zien of zich voorstellen, uitgelezen worden uit de hersenen.[54] Ook

46 EHRM 10 februari 1993, 18187/91 (W. vs. the United Kingdom).
47 EHRM 12 oktober 1978, 7050/75 (Arrowsmith vs. the United Kingdom).
48 EHRM 3 december 1986, 10491/83 (Angeleni vs. Sweden).
49 J. Murdoch, *Protecting the right to freedom of thought, conscience and religion under the European Convention on Human Rights*, Straatsburg 2012, p. 18.
50 EHRM 22 februari 1995, 22838/93 (Van den Dungen vs. the Netherlands.)
51 EHRM 8 juli 2008, 9103/04 (Georgian Labour Party vs. Georgia), als genoemd in Murdoch 2012, p. 19.
52 Artikel 9 lid 2 EVRM.
53 Deze vraag geldt uiteraard ook voor de uitleg van artikel 10 Handvest EU door het Hof van Justitie.
54 A.S. Cowen, 'Neural portraits of perception: Reconstructing face images from evoked brain activity', *NeuroImage* 2014-94, p. 12-22.

werden de hersenen van twee ratten via het internet met elkaar verbonden, waardoor ze over grote afstand konden samenwerken om een actie uit te voeren en zo een beloning te krijgen.[55]

De vrijheid van het maken van keuzes en uitingen gebaseerd op de gedachten en overtuigingen van het *forum internum* wordt, naast artikel 9 lid 1 EVRM, met name gebaseerd op de notie van persoonlijke autonomie beschermd onder artikel 8 EVRM.[56] Deze keuzevrijheid kan alleen worden ingeperkt op basis en onder de voorwaarden van artikel 8 lid 2 EVRM.

Het uiten van gedachten en meningen wordt, zoals eerder aangegeven, beschermd door artikel 10 EVRM, de vrijheid van meningsuiting. Deze gedachten en meningen kunnen vervolgens weer door anderen binnen de maatschappij ontvangen worden. Hiermee wordt de cirkel rond. Alhoewel niet uitputtend, zorgen de genoemde fundamentele rechten voor het waarborgen van de persoonlijke autonomie, in de zin van vorming van persoonlijkheid, identiteit en opvattingen.

Het recht op non-discriminatie ex artikel 14 EVRM zorgt er hierbij voor dat rechten krachtens het EVRM voor eenieder gelden en bijvoorbeeld niet op basis van geslacht, etniciteit of ras kunnen worden onthouden.[57] Artikel 21 Handvest EU gaat hierbij nog verder met een algeheel verbod op discriminatie, met name op grond van geslacht, ras, kleur, etnische of sociale afkomst, genetische kenmerken, taal, godsdienst of overtuigingen, politieke of andere denkbeelden, het behoren tot een nationale minderheid, vermogen, geboorte, een handicap, leeftijd of seksuele geaardheid.

55 www.nature.com/news/intercontinental-mind-meld-unites-two-rats-1.12522 (geraadpleegd op 20 november 2014).

56 EHRM 29 april 2002, 2346/02 (Pretty vs. The United Kingdom), r.o. 61 en 82.

57 De reikwijdte van het non-discriminatiebeginsel binnen het EVRM is met het twaalfde protocol van het EVRM uitgebreid. Waar artikel 14 beperkt was tot rechten krachtens het EVRM, is onder protocol 12 het gelijkheidsbeginsel van toepassing voor alle rechten. Nederland heeft dit protocol in 2004 geratificeerd, waarna het in 2005 in werking is getreden.

4 Het individu te midden van Big Data

In de enorme hoeveelheid digitale data die vandaag de dag gegenereerd wordt, zijn veel gegevens te vinden die betrekking hebben op natuurlijke personen. Deze gegevens worden verzameld voor velerlei administratieve processen, marketing en het verlenen van diensten aan individuen. Daarnaast worden ze ook gebruikt om beter inzicht te krijgen in het gedrag van individuen of groepen van mensen. Dit roept de vraag op welke positie het individu te midden van deze Big Data inneemt en hoe deze gekenschetst kan worden.

Het verwerken van gegevens van individuen ligt gevoelig, omdat het kan leiden tot een inbreuk op de informationele privacy van het individu.[58] Dit omvat zeggenschap over welke informatie wanneer, hoe en in hoeverre over hen gedeeld wordt. Daarnaast kan het ook om relationele privacy gaan, omdat uit gegevens de sociale context van een persoon te herleiden valt, namelijk met wie hij omgaat. Met de aan Big Data gelieerde ontwikkelingen zoals geschetst in hoofdstuk 2 kan het ook de ruimtelijke privacy beïnvloeden, aangezien individuen in bijvoorbeeld hun eigen huis steeds meer geobserveerd kunnen worden. Ten slotte kan met NBIC ook de lichamelijke privacy steeds meer geraakt worden, bijvoorbeeld door *wearables* of zelfs technologie in het lichaam.

4.1 Identiteit

Het gegevensbeschermingsrecht, uitgewerkt in onder andere de Wbp, tracht het verwerken van gegevens die individuen raken te reguleren, de zogeheten persoonsgegevens. Artikel 1 sub a Wbp definieert een persoonsgegeven als 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'. De definitie in artikel 2 sub a Richtlijn 95/46/EG voegt daar aan toe: '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'. Gegevens over personen zullen op velerlei wijzen in de Big Data terechtkomen. Wanneer er geen sprake is van persoonsgegevens, is het gegevensbeschermingsrecht niet van toepassing. Gezien de grote belangen die gemoeid zijn bij het verwerken van gegevens over individuen, is het niet verrassend dat er veelvuldig gediscussieerd wordt over de reikwijdte van dit begrip.

58 A. Westin, *Privacy and Freedom*, New York 1967.

Het dient derhalve te gaan om een geïdentificeerd of identificeerbaar natuurlijk persoon. Wanneer een verzameling gegevens de naam, woonplaats, geboortedatum, nationaliteit en taal omvat, is er meestal geen twijfel over mogelijk dat het gegevens van een identificeerbaar natuurlijk persoon betreft.[59] Dit ligt anders wanneer er sprake is van andersoortige gegevens die in het normale maatschappelijk verkeer niet direct een associatie met een aanwijsbaar individu opleveren, zoals een (cookie-)code, waarmee bijvoorbeeld (koop)gedrag van een persoon wordt bijgehouden en advertenties worden getoond. Betreft dit wel een identificeerbaar natuurlijk persoon?

De computerwetenschap maakt niet alleen de verwerking van deze gegevens mogelijk, maar biedt ook een analytisch instrumentarium om deze vraag uit te werken.[60] De natuurlijk persoon kan omschreven worden als 'entiteit', de mens van vlees en bloed. Deze entiteit kan vervolgens aangeduid worden met verschillende identiteiten, die bestaan uit een aantal attributen die gezamenlijk deze identiteit vormgeven. In het normale taalgebruik gaan aanduiding van de entiteit en aanduiding van de burgerlijke identiteit zoals naam, adres en woonplaats, vaak hand in hand. Identiteit heeft in deze zin een sociale functie, namelijk een permanente verwijzing naar een persoon.[61] Als we spreken over Willem-Alexander, wonende te Wassenaar, weet iedereen wie we bedoelen. Dezelfde persoon zouden we echter ook kunnen aanduiden als 'vader van drie kinderen, wonende te Wassenaar en liefhebber van voetbal'. Deze aanduiding zal in andere situaties toepasselijk kunnen zijn. Dit voorbeeld toont aan dat een identiteit contextueel is.[62] Beide identiteiten refereren naar dezelfde persoon (entiteit) en zijn hier een representatie van. De identiteit bestaat uit een aantal attributen of kenmerken. Of deze identiteit (verzameling attributen of één uniek attribuut zoals burgerservicenummer of een apparaatnummer) uniek is, hangt af van de vraag of er binnen de groep die de verantwoordelijke[63] kan overzien niet meer dan één persoon (entiteit) aan deze set van attributen (identiteit) voldoet.[64] De samenstelling van deze groep kan echter wijzigen. Identiteit is in die zin onzeker of kansgebaseerd en contextgebonden. Daarnaast kunnen verschillende identiteiten gemeenschappelijke attributen hebben en hiermee aan elkaar gelinkt worden.

59 HvJ 17 juli 2014, C-141/12 en C-372/12, r.o 38.

60 J. Talburt, 'Entity and identity resolution', http://mitiq.mit.edu/IQIS/2010/Addenda/T2A%20-%20JohnTalburt.pdf (geraadpleegd op 31 oktober 2014).

61 STI Workingpaper 2007/7, At a Crossroads: 'personhood' and Digital Identity in the Information Society (OECD), p. 27.

62 STI Workingpaper 2007/7, At a Crossroads: 'personhood' and Digital Identity in the Information Society (OECD), p. 26.

63 De verantwoordelijke wordt in artikel 1 sub d Wbp gedefinieerd als 'de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'.

64 Dit wordt ook wel k-Anonimity genoemd, waarbij k in dit geval 1 moet zijn. www.springerreference.com/docs/html/chapterdbid/64340.html.

4.2 Identiteit in Big Data

De identiteit van een persoon kan geautomatiseerd, bijvoorbeeld met behulp van Big Data-analyse, tot stand worden gebracht. Deze praktijk wordt ook wel als *profiling* omschreven. Theoretisch maar ook praktisch gezien zou er een profiel van een persoon kunnen worden opgesteld, bestaande uit kenmerken die gezamenlijk uniek zijn voor die persoon. In bepaalde gevallen kan met behulp van dit profiel een persoon fysiek worden teruggevonden, in andere gevallen niet. In andere woorden, een identiteit kan niet altijd terug herleid worden naar de achterliggende entiteit in de fysieke wereld.

Dit leidt tot een onderscheid in wat Leenes noemt, opzoek-identiteiten en herken-identiteiten.[65] Bij de eerste variant is iemand terug te herleiden naar zijn burgerlijke identiteit, dan wel direct door NAW–gegevens (naam, adres, woonplaats), dan wel indirect via bijvoorbeeld zijn telefoonnummer of kentekennummer waaraan een derde partij NAW-gegevens kan koppelen. Bij de tweede variant is een persoon onderscheidbaar van anderen, maar is er geen link te leggen naar de burgerlijke identiteit van de persoon. Naast deze twee vormen onderscheidt Leenes eveneens een categorische identiteit die aansluit bij de Big Data-praktijk, waarbij personen op basis van attributen die bij de verantwoordelijke bekend zijn in bepaalde klassen (collectieve identiteiten of groepsprofielen) worden ingedeeld. Het behoren tot een bepaalde klasse impliceert meestal dat de desbetreffende persoon ook over andere kenmerken beschikt, zelfs indien die niet door de verantwoordelijke zelf zijn vastgesteld. Het hebben van een bepaalde identiteit kan dan ook, soms onverwachte, gevolgen met zich meebrengen.[66]

Vaak zal binnen Big Data-analyse sprake zijn van een combinatie van een herken-identiteit en een categorische identiteit. Dat betekent dat de persoon binnen de dataset uniek te herkennen is en dat hem op basis van de klasse-indeling extra kernmerken worden toegedicht, zonder dat zijn burgerlijke identiteit te achterhalen is. Een identiteit is in die zin samengesteld. Enerzijds vormt de betrokkene[67] zelf deel van zijn identiteit, anderzijds wordt deze door anderen vormgegeven.[68]

Bij de behandeling van de AVG is door het Europees Parlement het onderscheid in verschillende vormen van identiteiten in zekere mate erkend. In artikel 4 sub 2a AVG wordt het begrip 'pseudonieme gegevens' gedefinieerd. Dit zijn 'persoonsgegevens die niet kunnen worden geattribueerd aan een specifieke betrokkene zonder het gebruik van aanvullende informatie, zo lang deze informatie gescheiden wordt bewaard en onderworpen is aan technische en organisatorische maatregelen om non-attributie te verzekeren'. In feite wordt er een informationele

65 R. Leenes, 'Do They Know Me? Deconstructing Identifiability', *University of Ottawa Law & Technology Journal* 2007-4, p. 146.

66 STI Workingpaper 2007/7, At a Crossroads: 'personhood' and Digital Identity in the Information Society (OECD), p. 26.

67 Artikel 1 sub f Wbp. De betrokkene is degene op wie een persoonsgegeven betrekking heeft.

68 STI Workingpaper 2007/7, At a Crossroads: 'personhood' and Digital Identity in the Information Society (OECD), p. 26.

machtenscheiding gemaakt.[69] De opzoek-identiteit wordt gescheiden van de herken-identiteit. Als het dit type gegevens betreft, wordt de verantwoordelijke in bepaalde gevallen meer ruimte gegeven om gegevens te verwerken. De Article 29–Working Group ziet dit niet als een anonimiseringstechniek, maar als een beveiligingsmaatregel.[70] De Working Group ziet effectieve anonimisering als een situatie waarin het voor alle partijen onmogelijk is om een specifiek persoon uit de dataset te lichten, gegevens binnen een set of meerdere sets van gegevens aan een persoon te linken of extra informatie over een persoon uit de dataset af te leiden.[71]

Het maken van onderscheid tussen de beschreven vormen van identiteit is van belang in het debat over Big Data, omdat enerzijds langs deze lijnen het begrip persoonsgegeven in de toekomst verder zal moeten worden ingevuld. Anderzijds dwingt het tot een precieze definiëring van begrippen als pseudonimisering en ook anonimisering. Als een persoon herkend kan worden aan een van zijn identiteiten en op basis daarvan anders beoordeeld of behandeld wordt,[72] is het moeilijk vol te houden dat het om anonieme gegevens, niet zijnde persoonsgegevens gaat.[73]

Met het gebruik van verschillende soorten identiteiten kan mede invulling worden gegeven aan de beginselen van proportionaliteit en subsidiariteit waaraan moet worden voldaan bij het verwerken van persoonsgegevens. In veel gevallen is het namelijk niet nodig om de burgerlijke identiteit van iemand te gebruiken, maar kan van een andere vorm van identiteit, bijvoorbeeld herken-identiteit, gebruik worden gemaakt die voor de betrokkene minder risico's met zich meebrengt.[74] Deze risicovermindering ziet echter, zoals gezegd, voornamelijk op het waarborgen van de beveiliging of vertrouwelijkheid van de gegevens en niet op de gevolgen die verwerking van de gegevens met zich meebrengen, bijvoorbeeld in het geval van geautomatiseerde besluitvorming. De link tussen individu en gegeven kan immers nog steeds gelegd worden.

69 G. Hornung & C. Schnabel, 'Data protection in Germany I: The population census decision and the right to informational self-determination', *Computer Law & Security Report* 2009, 25 (1), p. 85.

70 Article 29-Working Group 10 april 2014, Opinion 05/2014 on Anonymisation Techniques, p. 3. De Article 29-Working Group is het samenwerkingsverband van onafhankelijke toezichthouders dat conform artikel 29 van Privacyrichtlijn 95/46/EG ingesteld is.

71 Article 29-Working Group 10 april 2014, Opinion 05/2014 on Anonymisation Techniques, p. 9.

72 *Kamerstukken II* 1997/98, 25892, 3. p. 46-47.

73 Zie in lijn hiermee Article 29-Working Group 10 april 2014, Opinion 05/2014 on Anonymisation Techniques, p. 9 en 11.

74 Leenes 2007, p. 161.

5 Transparantie over of aan het individu

In het vorige hoofdstuk is beschreven op welke wijze een individu aangeduid kan worden te midden van Big Data. Doordat gegevens op steeds grotere schaal verwerkt kunnen worden en steeds meer gegevens over individuele personen verzameld kunnen worden, lijkt het individu steeds transparanter te worden. De vraag is of de betrokkene ook voldoende terug kan kijken, of dat hij geconfronteerd wordt met een situatie van een eenrichtingsspiegel waarbij transparantie slechts eenzijdig is.

Transparantie en informatieplichten richting de betrokkene, zoals beschreven in de artikelen 33 tot en met 35 Wbp, worden gezien als belangrijke instrumenten om diens positie en autonomie te versterken en een eerlijke verwerking van persoonsgegevens mogelijk te maken. Het wordt ook wel als basisbeginsel gezien, want een betrokkene kan immers pas zijn rechten laten gelden als hij überhaupt weet dat er gegevens over hem verwerkt worden. Verondersteld wordt dat dit weten de autonomie van het individu versterkt en hem in een betere controlepositie brengt. In deze tijd van Big Data en hieraan gelieerde technologische ontwikkelingen lijkt het instrument transparantie echter soms aan kracht in te boeten.

5.1 Taxonomie van gegevens

Binnen Big Data zijn gegevens afkomstig uit een veelvoud aan verschillende bronnen. Een taxonomie van deze bronnen van gegevens is een goed instrument om de verhouding tussen transparantie en gegevensverzameling scherp te krijgen.[75] Gegevens kunnen allereerst verstrekt worden door de persoon zelf waarop ze betrekking hebben. Deze informatie kan expliciet verstrekt worden, bijvoorbeeld NAW-gegevens, of impliciet door bijvoorbeeld een telefoonnummer te bellen. Ten tweede kunnen gegevens geobserveerd worden, bijvoorbeeld door het inzetten van sensoren of het krijgen van gegevens uit een derde bron. De betrokkene zal in veel gevallen niet op de hoogte zijn van het feit dat deze gegevens verzameld worden. Ten derde kunnen gededuceerde gegevens onderscheiden worden, die tot stand komen door gegevens te combineren en daar een logische gevolgtrekking uit te maken. Een voorbeeld hiervan is het uitzoeken uit welke leeftijdscategorie de meeste kopers van een product komen.

75 Deze taxonomie is ontleent aan OECD, Summary of the OECD Expert Roundtable Discussion 'Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking', DSTI/ICCP/REG(2014)4, p. 3.

Ten slotte is er nog de categorie van geïnduceerde gegevens die een probabilistisch karakter hebben. Een inmiddels bekend voorbeeld hiervan is de Amerikaanse supermarktketen Target, die op basis van de kooppatronen van een tiener afleidde dat zij waarschijnlijk zwanger was en haar op basis daarvan gerichte aanbiedingen deed, zelfs voordat haar eigen vader van het feit op de hoogte was.[76] Een ander voorbeeld is het afleiden van iemands seksuele geaardheid op basis van zijn of haar Facebook-activiteiten.[77] Dit zijn beide voorbeelden van indirecte bijzondere persoonsgegevens.[78]

Binnen de vorenstaande taxonomie nemen de betrokkenheid van de persoon bij en de voorzienbaarheid van het verwerken van deze gegevens steeds verder af. Juist in de laatste twee categorieën zit echter het zwaartepunt van Big Data. Met het toenemend aantal sensoren neemt de hoeveelheid geobserveerde data toe en vervolgens kunnen daar met Big Data-technieken met behulp van deductie, inductie en andere statistiek nieuwe gegevens worden verkregen en zo nieuwe identiteiten of profielen van personen worden gecreëerd. Dit zorgt in potentie voor een sterke informatie-asymmetrie tussen de verantwoordelijke en de betrokkene. Bovendien heeft de betrokkene mogelijk weinig invloed op de identiteit of het profiel dat zo van hem gecreëerd wordt.

Bij het verkrijgen van de gegevens bij de betrokkene zelf is de verantwoordelijke ex artikel 33 Wbp verplicht om, wanneer gegevens van de betrokkene worden verkregen, hem voor het moment van verkrijging van deze informatie te informeren over zijn identiteit, de doeleinden van de verwerking en nadere informatie die een zorgvuldige verwerking waarborgen, tenzij de betrokkene hiervan al op de hoogte is. Dit is volgens de memorie van toelichting bij de Wbp alleen van toepassing als de betrokkene zijn informatie zelf actief verstrekt.[79]

Bij de andere drie onderscheiden bronnen – observeren, deductie en inductie – dient te worden teruggevallen op artikel 34 Wbp. De verantwoordelijke dient dan de hiervoor genoemde informatie te verstrekken op het moment van vastleggen van de gegevens of, indien van toepassing, op het moment van eerste verstrekking aan een derde. Verstrekking van deze informatie is uit hoofde van artikel 34 lid 4 Wbp niet verplicht indien dit onevenredige inspanning kost of onmogelijk blijkt te zijn. In dat geval hoeft alleen de herkomst van de gegevens vastgelegd te worden. Artikel 14 van de voorgestelde AVG, dat dezelfde materie regelt, brengt geen wezenlijke verandering mee op dit vlak.

76 C. Duhigg, 'How companies learn your secrets', *The New York Times* 16 februari 2012, www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0.

77 Y. Bachrach e.a., 'Personality and Patterns of Facebook Usage', https://research.microsoft.com/pubs/163535/FacebookPersonality_michal_29_04_12.pdf.

78 Artikel 16 Wbp.

79 *Kamerstukken II* 1997/98, 25892, 3, p. 155-156.

5.2 Transparantie bij Big Data

Bij Big Data, waarbij sprake is van veelvoudig gebruik van data voor verschillende doeleinden,[80] met een veelvoud aan spelers, complexe waardenketens, grote snelheid en omvang van gegevensverwerking[81] en diversiteit van soorten gegevens, lijkt het bijzonder lastig een goede invulling te geven aan informatieverplichtingen uit de Wbp. De gegevens zijn immers vaak geobserveerd, gededuceerd of geïnduceerd en verbonden aan een herken-identiteit van de betrokkene.[82] Bij *internet of things*-toepassingen ontbreekt bovendien vaak de mogelijkheid voor uitgebreide communicatie naar de betrokkene. Veel van de apparatuur beschikt niet over een scherm om informatie over te dragen en verzamelt bovendien informatie over personen die de apparatuur niet hebben aangeschaft. In veel gevallen zal dit in de praktijk tot de conclusie kunnen leiden dat communicatie naar de betrokkene onevenredige inspanning vergt en daarom achterwege kan worden gelaten. Een actieve verstrekking van informatie conform artikel 34 Wbp bij het verzamelen van gegevens is daarom problematisch.

Een inzageverzoek in zijn persoonsgegevens door de betrokkene op basis van artikel 35 Wbp lijkt meer mogelijkheden te bieden. Op basis hiervan kan de betrokkene zich met redelijke tussenpozen richten tot de verantwoordelijke met de vraag of persoonsgegevens over hem worden verwerkt. Indien dit het geval is, dient ingevolge het tweede lid van het artikel een overzicht daarvan in begrijpelijke vorm te worden gegeven. Tevens doet de verantwoordelijke op verzoek mededeling over de logica die ten grondslag ligt aan de geautomatiseerde verwerking van de gegevens.[83]

Zoals omschreven in hoofdstuk 4 zal bij Big Data veel gebruik kunnen worden gemaakt van herken-identiteiten. De burgerlijke identiteit met NAW-gegevens van een persoon is niet bekend, maar hij heeft wel een unieke identiteit binnen de gegevensverzameling en kan hieraan herkend worden. Indien de gegevens die betrekking hebben op de herken-identiteit als persoonsgegevens worden gezien, zou de betrokkene op verzoek hier inzage in moeten krijgen. Hiervoor is het wel noodzakelijk dat de verantwoordelijke in staat is om de betrokkene voldoende betrouwbaar te herkennen aan zijn herken-identiteit. Identificatie zal dan waarschijnlijk ook moeten plaatsvinden binnen de context waarbinnen de identiteit is gevormd, zodat deze daar kan worden herkend. Een eenvoudig voorbeeld is het vormen van een herken-identiteit op basis van het surfgedrag van een gebruiker op internet. Zodra betrouwbaar genoeg is vastgesteld dat het om wederom dezelfde unieke internetsurfer gaat, zou op basis hiervan aan hem inzage in de over hem verzamelde gegevens geboden kunnen worden.

---

80 Dit levert spanning op met artikel 9 Wbp, waarin gesteld wordt dat persoonsgegevens niet verwerkt mogen worden voor een doel dat onverenigbaar is met waarvoor de gegevens zijn verkregen.

81 Dit levert spanning op met artikel 11 Wbp, waarin het beginsel van gegevensminimalisatie is beschreven.

82 Zie voor een beschrijving van de herken-identiteit hoofdstuk 4 van dit preadvies.

83 Artikel 35 lid 4 Wbp.

In artikel 10 van de voorgestelde AVG wordt gesteld dat wanneer de gegevens die door de verantwoordelijke verwerkt worden de verantwoordelijke niet in staat stellen om de natuurlijke persoon te identificeren, de verantwoordelijke niet verplicht is om extra informatie in te winnen om de betrokkene te identificeren om te voldoen aan regels uit de verordening. In feite wordt hiermee gesteld dat een verantwoordelijke van niet-persoonsgegevens geen persoonsgegevens hoeft te maken. Dit is tweeërlei bijzonder. Allereerst impliceert het hebben van de mogelijkheid om gegevens te herleiden naar een persoon dat het al om persoonsgegevens gaat. Ten tweede is het bijzonder dat dit zo absoluut gesteld is, omdat het in bepaalde gevallen de betrokkene de mogelijkheid ontneemt om via het gegevensbeschermingsrecht invloed op zijn gegevens uit te oefenen. In principe kan een herken-identiteit immers voldoende zijn om de betrokkene, in ieder geval op verzoek, van informatie te kunnen voorzien.

Bij het bieden van een betekenisvolle manier aan de betrokkene om kennis te nemen van persoonsgegevens en zo inzage te krijgen in de digitale identiteiten die rondom hem zijn gevormd, ligt derhalve een grote uitdaging. Deze uitdaging moet echter worden aangegaan en met een goede invulling hiervan zou Big Data juist voordelen voor het individu met zich mee kunnen brengen. Door inzage te geven in hoe een individu wordt gezien door de verantwoordelijke, inclusief betekenisvolle inzage in hoe dit tot stand kwam, kan de informatie-asymmetrie opgeheven worden en de positie van de betrokkene juist worden versterkt. Als de betrokkene immers weet hoe naar hem wordt gekeken, kan hij hierop reageren en eventueel ageren. Dit is bovendien van bijzonder belang voor het kunnen ontdekken van ongeoorloofde discriminatie. In de complexe ketens van Big Data vraagt dit echter wel veel van de infrastructuur van de verantwoordelijke. Het gaat immers om grote hoeveelheden heterogene data die op zichzelf niet veelzeggend hoeven te zijn, maar juist door analyse belangrijke inzichten voor zowel verantwoordelijke als betrokkene opleveren. Werkelijk betekenisvol inzicht geven in de gevormde identiteiten is daarmee een uitdaging. *Privacy by design*, het al in het ontwerpstadium van een systeem implementeren van de normen van het gegevensbeschermingsrecht, wordt vaak in de sleutel van doelbinding en gegevensminimalisatie gezet, maar is zo gezien ook een basisvoorwaarde om in de context van Big Data transparantie aan de betrokkene te bieden.[84]

84 Zie artikel 23 van de voorgestelde AVG.

6 Het autonome individu

Het controleren van het individu en het daarmee beperken van zijn autonomie is een terugkerend thema rondom Big Data. In verhalen en fictie gaan hierbij vaak de dreiging en kwade opzet uit van één partij. Vaak is de staat die partij.[85] Door de discussie hiertoe te beperken wordt tekortgedaan aan de complexe sociale, economische en technische systemen die onze samenleving en daarmee ook onszelf als individu beheersen.

6.1 Identiteitsvorming

Zoals omschreven in hoofdstukken 4 en 5 maken Big Data en gerelateerde ontwikkelingen het mogelijk om een veelvoud aan gegevens over een individu vast te leggen en uit te breiden met gededuceerde of geïnduceerde gegevens. Deze gegevens vormen een (categorische) identiteit die of een profiel dat aan een individu wordt verbonden.

Deze identiteit wordt derhalve door de verantwoordelijke (deels) samengesteld. De eerste vraag die hierbij speelt is of deze aangemeten identiteit wel klopt. De verantwoordelijke heeft de plicht om ervoor te zorgen dat de persoonsgegevens juist en nauwkeurig zijn, gelet op het doel van de verwerking.[86] Problematisch hierbij is dat een identiteit in wezen vaak een subjectief gegeven is.[87] Dit geldt evenzeer voor identiteiten die binnen Big Data bestaan. De verantwoordelijke kan namelijk besluiten dat persoon X tot categorie XYZ behoort en daarom anders behandeld wordt. Deze categorie XYZ kan echter vastgesteld zijn volgens lijnen die in het normale maatschappelijk verkeer geen duidelijke betekenis of classificatie zouden hebben. Het recht van de betrokkene om ex artikel 36 Wbp persoonsgegevens over hem 'te verbeteren, aan te vullen, te verwijderen, of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn', is daarmee voor dergelijke categorisatie maar van beperkte waarde. De controle van het individu over zijn identiteit(en) is derhalve maar gering.

De logica op basis waarvan nieuwe informatie over een individu en daarmee diens identiteit gecreëerd wordt, vormt een belangrijk startpunt om toch meer controle over de vorming van identiteiten of profielen te krijgen. Op basis van artikel 35 lid

85 Denk aan George Orwells 1984.
86 Artikel 11 lid 2 Wbp.
87 STI Workingpaper 2007/7, At a Crossroads: 'personhood' and Digital Identity in the Information Society (OECD), p. 26.

4 Wbp kan de betrokkene op verzoek inzage krijgen in de onderliggende logica van de geautomatiseerde verwerking. Uit de memorie van toelichting volgt dat dit artikel van toepassing is '(...) in geval bijzondere computerprogrammatuur een wijze van verwerking mogelijk maakt die de betrokkene niet reeds duidelijk is uit de mededeling ingevolge het tweede lid' en dat deze mededeling in algemene bewoording kan worden gedaan.[88] Deze inzage mag geen afbreuk doen aan een zakengeheim of het intellectueel eigendomsrecht, maar hierdoor mag ook niet totale inzage geweigerd worden. Deze bepaling, die zijn oorsprong vindt in artikel 12a Richtlijn 95/46/EG, is niet als zodanig opgenomen in het commissievoorstel voor de AVG. Het Europees Parlement heeft echter voorgesteld deze wederom op te nemen.[89] Inzage in de logica, als onderliggend mechanisme voor identiteitscreatie, is een belangrijke voorwaarde om betekenisvol andere rechten, zoals het correctierecht, uit te kunnen oefenen. Anders kan het tot een situatie leiden waarbij de betrokkene maar zeer weinig controle over de (geautomatiseerd) aan hem toegemeten identiteiten heeft, wat al *prima facie* als beperking van zijn autonomie kan worden gezien.

Deze identiteiten en de logica op basis waarvan de gegevens verwerkt worden, kunnen echter buiten de context waarin ze gebruikt worden weinig betekenisvol zijn. Dit wordt veroorzaakt doordat ook veel van deze logica wordt doorontwikkeld door *machine learning*, dat ervoor zorgt dat vaak ook de verantwoordelijke geen volledig zicht heeft op de reden waarom iemand een bepaalde identiteit of bepaalde attributen toegewezen heeft gekregen. Het is daarom van belang dat de verantwoordelijke altijd aanspreekbaar blijft voor de identiteit die wordt gecreëerd. Bij onvoldoende onderbouwing van de juistheid en relevantie hiervan zou de betrokkene mogelijk verwijdering van het profiel kunnen eisen.[90]

6.2 Persoonlijke autonomie en sturing

Op basis van de identiteiten van een betrokkene kunnen besluiten ten aanzien van hem worden genomen. Belangrijk hierbij is dat dit zowel ten aanzien van een opzoek-identiteit (burgerlijke identiteit) als van een herken-identiteit kan plaatsvinden. Iemand kan dus nog steeds geraakt worden door een besluit, zelfs wanneer de verantwoordelijke niet de naam, het adres, de geboorteplaats of andere meer gangbare kenmerken van de betrokkene weet.

Geautomatiseerde besluitvorming over het individu op basis van kenmerken van hem wordt ook wel aangeduid als *profiling*. Dit wordt door het Europees Parlement gedefinieerd als 'elke vorm van automatische verwerking van persoonsgegevens met als doel het evalueren van bepaalde persoonlijke aspecten van een natuurlijk persoon of het analyseren of voorspellen van deze natuurlijke persoon zijn prestatie op het werk, zijn economische situatie, locatie,

88 *Kamerstukken II* 1997/98, 25892, 3.
89 www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN.
90 Artikel 36 Wbp.

gezondheid, persoonlijke voorkeuren, betrouwbaarheid of gedrag'.[91] Dit is een zeer breed begrip en ziet in feite op het automatisch beslissen over personen op basis van door technologie geobserveerde, geïnduceerde of gededuceerde kenmerken op basis waarvan identiteiten (profielen) van mensen worden gecreëerd. Artikel 42 Wbp normeert deze situatie, waarbij aangetekend moet worden dat dit artikel alleen van toepassing is als er rechtsgevolgen aan het besluit zijn verbonden of wanneer het besluit de betrokkene in aanmerkelijke mate treft. In de AVG wordt in artikel 20 een soortgelijke regeling voorgesteld.

Geautomatiseerde besluitvorming op basis van inzichten verkregen uit Big Data-analyse kan gevolgen meebrengen voor de autonomie van het individu en diens fundamentele rechten. Deze gevolgen kunnen bijvoorbeeld het resultaat zijn van veranderingen in informatievoorziening en goederen en diensten. Die zullen namelijk tot in het extreme gepersonaliseerd kunnen worden op basis van data-analyse. Dit kan zorgen voor padafhankelijkheid of een zelfversterkend effect dat veroorzaakt wordt doordat op basis van het profiel een persoon anders behandeld wordt, op basis waarvan hij zich anders zal gedragen en waar vervolgens het profiel weer nader wordt verfijnd.

Een bekend voorbeeld hiervan is de door Eli Pariser gepopulariseerde *filter bubble*.[92] Zoekmachines passen hun zoekresultaten steeds meer aan op de gebruiker, gebaseerd op informatie over hem die binnen of buiten de zoekmachine is verzameld. Eenzelfde constructie wordt gebruikt door Facebook voor het bepalen welke items in het nieuwsoverzicht moeten worden getoond op basis van het EdgeRank algoritme.[93] Aangezien het wereldbeeld van mensen in sterke mate bepaald wordt door wat zij in hun omgeving waarnemen, kan aanpassing van de informatievoorziening aan mensen grote gevolgen hebben. Zo startte Facebook in 2014 een experiment waarin een groep van ongeveer 700.000 gebruikers uitsluitend positieve berichten van vrienden en familie getoond werd.[94] Dit zorgde ervoor dat deze groep ook steeds positievere informatie ging plaatsen. Dit toont duidelijk de invloed van deze mechanismen aan. De wijze van selectieve informatievoorziening kan natuurlijk via een veelvoud aan scheidslijnen plaatsvinden, waardoor steeds verdergaande personalisering of, negatief gesteld, manipulatie mogelijk wordt.

Sturing kan zich echter ook via andere wegen dan informatievoorziening voordoen. Lessig onderscheidt in zijn theorie van regulering een viertal modaliteiten

---

91 Artikel 4 sub 3a AVG (Europees Parlement, eerste lezing). www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN.

92 E. Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, Penguin Books 2012. De filter bubble wordt ook wel als *echo chamber* aangeduid. Zie International Working Group on Data Protection?in Telecommunications 5-6 mei 2014, Working Paper on Big Data and Privacy,?Privacy principles under pressure in the age of Big Data analytics, p. 11.

93 https://econsultancy.com/blog/7885-the-ultimate-guide-to-the-facebook-edgerank-algorithm en http://techcrunch.com/2010/04/22/facebook-edgerank/ (geraadpleegd op 2 november 2014).

94 www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html?_r=0 (geraadpleegd op 2 november 2014).

die invloed op de autonomie van het individu uitoefenen.[95] Dit betreft het recht, (sociale) normen, de markt en ten slotte architectuur. Het recht en rechtshandhaving beperken de autonomie van het individu of beschermen hem juist door de autonomie van derden te beperken. Sociale normen beperken eveneens de bewegingsvrijheid van het individu, evenals de markt waardoor vraag en aanbod en prijzen gestuurd worden. Ten slotte is er architectuur. Een goed voorbeeld in de fysieke wereld is de planologie van een stad die, naast verkeersregels (recht), in sterke mate het verkeer reguleert. Veel hiervan is statisch, zoals de ligging van de weg, maar ook dynamische elementen zoals verkeerslichten zijn mogelijk. Architectuur ligt echter tevens verborgen in de technologie waarmee onze wereld steeds meer doordrongen raakt. Ook hierdoor kan het individu gestuurd worden.

Wanneer dagelijkse objecten en structuren mensen kunnen herkennen en hierop kunnen reageren, wordt de vergaande personalisering in het fysieke domein werkelijkheid. Het functioneren van fysieke *smart objects* zal voor eenieder met hetzelfde profiel gelijk zijn, maar aangezien het profiel per persoon nooit helemaal gelijk zal zijn, zal de uitkomst tussen personen altijd verschillen. De omgeving en objecten zullen zich aanpassen aan de persoon met wie geïnteracteerd wordt.

Dit kan ook op een wijze dat een persoon wordt aangezet om bepaald gedrag te vertonen of bepaalde acties te ondernemen, ook wel *persuasion profiling* genoemd.[96] Deze *persuasion profiles* geven informatie over welke (soorten) informatie of interactie overtuigend is voor het individu dat door het profiel wordt beschreven. Uit onderzoek blijkt dat deze eigenschappen, bijvoorbeeld gevoeligheid voor autoriteit, schaarste (koopjes) of een streven naar consensus, zeer contextonafhankelijk zijn.[97] Met andere woorden, personen zijn in verschillende situaties gevoelig voor dezelfde soort overtuigingen.[98] Het is niet verwonderlijk dat marketeers op zoek zijn naar het gebruik van psychologische *triggers* om personen aan te zetten tot het aanschaffen van diensten en producten.[99] In de praktijk zijn dergelijke profielen echter ook al ingezet bij het overtuigen van kiezers, zoals tijdens de Amerikaanse presidentiële verkiezingen in 2008.[100]

Het gevaar bestaat dat het individu weinig tot geen controle heeft over de vorming van zijn identiteiten, de reactie daarop door zijn steeds slimmere omgeving en uiteindelijk het vormen van zijn eigen keuzes. Ook kan het leiden tot een *chilling effect* op de vrijheid van meningsuiting, omdat niet goed voorzienbaar is welke gevolgen de verzameling en verwerking van gegevens in de toekomst met zich

95 L. Lessig, *Code version 2.0*, New York: Basic Books 2006, p. 123.

96 M.C. Kaptein, *Personalized Persuasion in Ambient Intelligence* (diss. TU Eindhoven), Eindhoven: Technische Universiteit Eindhoven 2012, p. 101.

97 M.C. Kaptein & D. Eckles, 'Selecting Effective Means to Any End: Futures and Ethics of Persuasion Profiling', www.persuasion-profiling.com/wp-content/uploads/2010/04/EffectiveMeans.pdf, p. 2.

98 Dit brengt wederom een spanning met het beginsel van doelbinding van artikel 9 Wbp.

99 www.persuasionapi.com.

100 www.technologyreview.com/featuredstory/508836/how-obama-used-big-data-to-rally-voters-part-1/ (geraadpleegd op 2 november 2014).

meebrengt.[101] Het analyseren van alle activiteiten en gedrag maakt een persoon inzichtelijk en voorspelbaar. Daarnaast zou er ongeoorloofd onderscheid tussen personen kunnen worden gemaakt. Op de 36e Internationale Conferentie van Toezichthouders Gegevensbescherming zijn deze gevaren benoemd in de context van Big Data.[102] Om negatieve gevolgen zo veel mogelijk te beperken wordt onder andere opgeroepen doelbinding en gegevensminimalisatie te respecteren en waar passend toestemming te vragen. Daarnaast wordt nadruk gelegd op transparantie over gegevensverwerking, besluiten die genomen worden en profielen die samengesteld worden. In het bijzonder wordt opgeroepen om Big Data eerlijk, transparant en verantwoordelijk in te zetten en profielen en beslisregels continu te onderhouden, zodat de profielen eerlijk, ethisch en proportioneel zijn en er geen onterechte beslissingen worden genomen. Als er significante effecten voor het individu zijn, zou menselijke tussenkomst altijd mogelijk moeten zijn.[103]

6.3 Kansen ten aanzien van individuele autonomie

In de discussie is het duidelijk dat er steeds meer nadruk wordt gelegd op open begrippen als 'eerlijk', 'transparant', 'verantwoordelijk' en zelfs 'ethisch'. Gezien de snelle technologische ontwikkelingen wordt ook in de voorgestelde AVG zo veel mogelijk met techniek- en implementatieneutrale open normen gewerkt. Dit lijkt mede ingegeven door onzekerheid over de effectiviteit van instrumenten als toestemming en transparantie voor het beschermen van het individu. In die zin zou juist binnen de innovatie op het terrein van Big Data onderzoek gedaan moeten worden naar welke instrumenten in welke context effectief zijn in het beschermen van het individu en diens autonomie. Big Data kan namelijk ook juist de autonomie van het individu versterken. Zo kan het allereerst verborgen vormen van discriminatie die bewust of onbewust binnen de maatschappij plaatsvinden, inzichtelijk maken.[104] Daarnaast kunnen profielen, wanneer vrijgegeven aan de betrokkene, hem juist ook beter inzicht geven in zijn eigen besluitvormingsproces en hem zo weerbaarder maken voor subtiele overtuigingen of manipulatie.[105] Inzet in de praktijk hiervan zal echter afhankelijk zijn van de belangen van de verantwoordelijke, die er soms (commercieel) belang bij kan hebben juist niet het zelfinzicht van de betrokkene te versterken.

101 P. de Hert e.a., 'Legal safeguards for privacy and data protection in ambient intelligence', *Personal and Ubiquitous Computing* 2009-13, p. 436. Zie eveneens HvJ 8 april 2014, zaken C-293/12 en C-594/12, r.o. 28.

102 www.cbpweb.nl/downloads_med/Resolution%20Big%20Data.pdf (geraadpleegd op 2 november 2014).

103 Zie huidige artikel 42 lid 2 Wbp.

104 http://thehill.com/blogs/pundits-blog/technology/221583-big-data-is-a-powerful-weapon-in-the-fight-for-equality (geraadpleegd op 2 november 2014).

105 Kaptein 2012, p. 179.

7 Big Data en de overheid

Naast bedrijven zien ook overheden de potentiële voordelen en kansen van Big Data. Een groot deel van deze voordelen hebben betrekking op het in kaart brengen van zaken als milieuvervuiling en gezondheidsrisico's in steden, bijvoorbeeld door het op grote schaal meten van fijnstofconcentraties. Tevens kunnen gegevens over de hoeveelheid wegverkeer op het wegennet worden gebruikt om de inrichting van de infrastructuur te verbeteren.

Tegelijkertijd zijn er uiteraard ook aan Big Data gerelateerde toepassingen die voor controverse zorgen. Denk aan het gebruik van diverse gegevensbronnen voor het opsporen van fraudegevallen, bijvoorbeeld op basis van de wijziging op 1 januari 2014 van de Wet structuur uitvoeringsorganisatie Werk en inkomen en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekende zijnde gegevens. De discussie over het gebruik van dergelijke technieken wordt meestal gevoerd langs de lijn van bescherming van de persoonlijke levenssfeer tegen inmenging van de overheid. Alhoewel dit een wezenlijke en fundamentele discussie betreft, zal in dit preadvies de discussie langs een andere lijn gevoerd worden, namelijk onvoorziene gevolgen die het inzetten van deze technologie voor uitvoering en beleidsvorming met zich mee kan brengen.

7.1 Aandachtspunten in de context van de overheid

Big Data brengt op diverse wijzen kansen en risico's met zich mee, doordat het als instrument voor het maken van onderscheid kan worden gebruikt, op basis waarvan beleid vorm kan worden gegeven. In een paper over *data mining* analyseert Barocas risico's die onder andere relevant zijn in een overheidscontext.[106] Allereerst kan beleidsvorming op basis van Big Data tot ongewenste gevolgen leiden indien er sprake is van een statistische tekortkoming. Als voorbeeld wordt het inzetten van een app op moderne smartphones voor het opsporen van gaten in het wegdek benoemd.[107] Indien onderhoudswerkzaamheden vervolgens voornamelijk op basis van deze gegevens worden ingepland, bestaat er een risico dat bijvoorbeeld arme wijken worden achtergesteld omdat daar minder bewoners gebruikmaken van een moderne smartphone met de app. Indien beleidsmakers deze verborgen afwijkingen onvoldoende onderkennen, kan dit onbedoeld voor groeiende ongelijkheid zorgen.

106 S. Barocas, 'Data Mining and the Discourse on Discrimination', *Proceedings of Data Ethics Workshop*, 24 augustus 2014, p. 1-4.

107 Zie www.streetbump.org (geraadpleegd op 2 november 2014)

Tevens kunnen beslissingen genomen worden over individuen of groepen van individuen op basis van onvolledige gegevens. De door Big Data afgeleide gegevens zijn immers maar een beperkte representatie van de werkelijkheid. Daar tegenover bestaat het gevaar dat juist met Big Data heel precies individuen of groepen van individuen onderscheiden kunnen worden en voorspellingen over de toekomst kunnen worden gedaan. Doordat steeds preciezer inzichtelijk is hoeveel personen en groepen aan de maatschappij in sociale of economische zin bijdragen of kosten, kan dit de sociale cohesie, of *social fabric*, binnen de maatschappij verminderen en de druk op specifieke groepen verhogen.[108] Zo kunnen mensen bijvoorbeeld onder druk worden gezet om gezonder te leven. Als zij hier geen gevolg aan geven, kunnen zij gedwongen worden om bijvoorbeeld meer belasting of premie te betalen. Controle op hoe veilig en zuinig iemand rijdt, is een ander voorbeeld. Ten slotte kan een toegenomen controle op bepaalde groepen in de maatschappij *an* sich al met zich meebrengen dat vanzelf meer gevallen van normafwijkend gedrag worden geconstateerd, simpelweg omdat deze groepen vaker worden gecontroleerd.

De gemene deler van de vorenstaande noties is dat er de nodige mogelijke valkuilen zijn bij het inzetten van Big Data voor beleidsvorming. Het is daarom belangrijk om altijd de beperkingen van de technieken in ogenschouw te houden. Resultaten uit Big Data-analyse kunnen immers gepercipieerd worden als volstrekt objectief, terwijl ook daar op velerlei wijze vertekende beelden kunnen optreden.

7.2 Nieuwe vormen van regulering

Het gebruik van grote databronnen en data-analyse voor het reguleren van de maatschappij wordt ook wel aangeduid als *algorithmic regulation*.[109] Het idee is dat technieken die bijvoorbeeld ook door grote IT-bedrijven gebruikt worden om spam te filteren of zoekresultaten te filteren, tevens gebruikt kunnen worden voor regulering in meer traditionele zin. Een bedrijf als Google kan bijvoorbeeld niet handmatig continu nieuwe regels opstellen om spammails te detecteren.[110] Door continu de situatie te meten, automatisch regels (algoritmen) toe te passen en deze regels op basis van feedback van gebruikers en het systeem aan te passen aan de gewenste uitkomsten, kan snel ingespeeld worden op nieuwe situaties en kan stabiliteit van de gewenste uitkomsten verzekerd worden. In het voorbeeld is dat het juist aanduiden of verwijderen van spammails. Regulering wordt in die zin adaptief, ofwel dat de regels continu worden aangepast om tot de gewenste uitkomst te komen.

Een eerste voorbeeld in de context van de fysieke wereld en de overheid is het dynamisch aanpassen van de maximale snelheid op snelwegen (dynamax),

108 Barocas 2014, p. 3.

109 http://beyondtransparency.org/chapters/part-5/open-data-and-algorithmic-regulation/ (geraadpleegd op 2 november 2014).

110 www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation (geraadpleegd op 3 november 2014).

gebaseerd op de gemeten drukte op de weg en de hoeveelheid luchtvervuiling.[111] In 2009 zijn hier al uitgebreide proeven mee ondernomen, wat in 2011 tot een eindrapport met positieve resultaten heeft geleid.[112] Met behulp van een veelvoud aan metingen wordt duidelijk welke snelheid voorgeschreven dient te worden om de gewenste optimale reistijd, verkeersdrukte en hoeveelheid luchtvervuiling te krijgen.[113] Dynamische snelheden zijn een fenomeen waar we al aan gewend zijn, maar met de snelle ontwikkeling van het *internet of things*, waardoor onze volledige omgeving uitgerust kan worden met slimme technologie, nemen de mogelijkheden enorm toe om ook andere aspecten te monitoren en zelfs automatisch aan te passen. De eerste tekenen zijn al te zien, bijvoorbeeld bij het Living Lab in uitgaansgebied Stratumseind in Eindhoven, waar gebruik wordt gemaakt van een grote hoeveelheid sensoren, zoals voor geluid, temperatuur, bezoekersaantallen en dergelijke.[114] Op basis hiervan kunnen (automatisch) acties ondernomen worden om voor een goede sociale omgeving te zorgen. Uiteindelijk kan dit leiden tot steeds verdergaande *real time* adaptieve (invulling van) regelgeving, uitvoering en handhaving. In feite maakt dit meer maatwerk mogelijk, om zo het gewenste einddoel te behalen. Hier is een parallel te vinden met de inzet van open normen in het gegevensbeschermingsrecht. In plaats van materiële normen voor te schrijven hangt de invulling van deze open normen af van de omstandigheden van het geval en de ontwikkelingen in de jurisprudentie. Het verschil met *algoritmic regulation* is echter dat hierbij de omstandigheden van het geval geautomatiseerd worden gewogen en tot een vastgestelde uitkomst leiden.

Algorithmic regulation kan gevolgen met zich meebrengen voor de (rechts)positie van de individuele burgers, met name wanneer de uitkomsten van deze *algorithmic regulation* voor iedere burger anders kunnen zijn. Bij het invoeren van een dynamische maximumsnelheid is hier maar beperkt sprake van, omdat deze voor alle personen die op een bepaald moment op een specifieke weg rijden hetzelfde is. Echter, wanneer er maar rekening gehouden wordt met genoeg omstandigheden en de toepassing van de norm met zich meebrengt dat niet één burger gelijk is of zich op het hetzelfde moment in gelijke omstandigheden bevindt, zal dit voor iedere burger feitelijk tot een andere uitkomst leiden. Dit gegeven zal dan ook een belangrijk aandachtspunt zijn in debatten over gelijke behandeling.

De voorgaand geschetste ontwikkelingen zullen mogelijk tot efficiëntieverbeteringen kunnen leiden, maar deze zullen wel binnen de grenzen van een goede vervulling van de algemene beginselen van behoorlijk bestuur moeten blijven, zoals het al eerdergenoemde gelijkheidsbeginsel. Daarnaast kan het rechtszekerheidsbeginsel onder druk komen te staan. De kern van

111 www.wegenwiki.nl/Dynamische_maximumsnelheid (geraadpleegd op 3 november 2014).

112 www.rijksoverheid.nl/ministeries/ienm/documenten-en-publicaties/rapporten/2011/02/11/bijlage-2—rapport-dynamische-maximumsnelheden-evaluatie-praktijkproeven.html (geraadpleegd op 3 november 2014).

113 Op basis van artikel 186 Wegenverkeerswet 1994 kunnen experimenten uitgevoerd worden. Zie ook aanwijzing 10b van de Aanwijzingen voor regelgeving.

114 http://ditss.nl/nieuws/ditss-workshops-op-industria-congres-big-data-big-business-or-big-brother/ (geraadpleegd op 3 november 2014).

rechtszekerheid is voorzienbaarheid en kenbaarheid.[115] Dit kan onder druk komen te staan omdat de complexiteit van de regels vergroot wordt en de variabelen die gebruikt worden voor toepassing van de regel voor de burger weinig inzichtelijk kunnen zijn. Bij *algorithmic regulation* zal de uitkomst van de regels bovendien steeds meer afhankelijk kunnen zijn van factoren die buiten de burger liggen, maar die wel zijn positie beïnvloeden. In het geval van besluiten zal er in het bijzonder aandacht moeten zijn voor het motiveringsbeginsel. Uitkomsten van beleid en wetgeving kunnen immers uiteraard niet gebaseerd worden op de uitkomst van een *black box*. Voor het gebruik, de inhoud en de uitkomst van algoritmen dient in beginsel ook rekenschap te worden afgelegd, zogenoemde *algorithmic accountability*.[116] Dit kan gaan om informatie over op welke wijze gegevens gebruikt worden als invoer, hoe deze worden gestructureerd en geclassificeerd, welke afwijkingen er zijn en hoe doorlopend de juistheid van het algoritme wordt verzekerd, om zo een eerlijke en inhoudelijke juiste toepassing te verzekeren.[117]

115 R. Koning, 'De crisis- en herstelwet: nood, spoed of experiment', in: A.G. Bregman, H.E. Bröring & K.J. de Graaf (red.), *Onbegrensde rechtsbeoefening* (Lubach bundel), Den Haag: IBR 2014, p. 42.

116 https://freedom-to-tinker.com/blog/felten/accountable-algorithms/ (geraadpleegd op 3 november 2014).

117 N. Diakopolous, 'Algorithmic accountability reporting: on the investigation of black boxes', http://towcenter.org/wp-content/uploads/2014/02/78524_Tow-Center-Report-WEB-1.pdf, p. 3-10.

8 Conclusie

De snelle ontwikkelingen op het gebied van (informatie)technologie stuwen elkaar vooruit. Afnemende kosten en toenemende mogelijkheden van sensoren, gegevensopslag, gegevensverwerking en het integreren van elektronica in alle dagelijkse objecten en convergentie tussen de neuro-, bio-, informatie- en cognitieve technologie maken dit mogelijk. Big Data, de verwerking van grote hoeveelheden informatie, van verschillende aard, met hoge snelheid ondersteunt deze ontwikkeling.

Met deze ontwikkelingen kunnen fundamentele rechten onder druk komen te staan, maar in gevallen ook versterkt worden. Hierbij dient niet alleen gekeken te worden naar de rechten op bescherming van de persoonlijke levenssfeer en persoonsgegevens, maar ook naar de vrijheid van gedachte, de vrijheid van meningsuiting en het recht op non-discriminatie. In de context van Big Data en aanverwante technologische ontwikkelingen liggen de kansen en risico's in samenhang ten aanzien van deze rechten met name op het vlak van persoonlijke autonomie, keuzevrijheid, integriteit en een vrije stroom van denkbeelden. De bescherming van de persoonlijke levenssfeer en persoonsgegevens maken dat het individu zichzelf kan vormen, onder meer op basis van denkbeelden die hij ontvangen heeft van derden. In de vrijheid van zijn eigen gedachte kan hij keuzes maken over het inrichten van zijn persoonlijke levenssfeer en daar vervolgens zijn gedachten over uiten.

Met de toegenomen mogelijkheden van data-analyse zal anders naar de positie van het individu te midden van Big Data moeten worden gekeken. De burgerlijke identiteit zoals naam, adres en woonplaats zal steeds minder een belangrijke rol vervullen, en tegelijkertijd zal de rol van herken-identiteiten, waarmee een persoon onderscheiden kan worden van anderen, toenemen. Bij de interpretatie van het gegevensbeschermingsrecht zal hier rekening mee moeten worden gehouden, om zo de beschermingsomvang van dit recht niet te ver in te perken.

De vorming van de identiteit van het individu zal steeds meer geautomatiseerd en buiten het zicht van hem plaatsvinden. Waar in het verleden het zwaartepunt lag bij door de betrokkene zelf gegeven informatie en door de verantwoordelijke geobserveerde informatie, worden nu het deduceren, induceren en andersoortig afleiden van informatie van het grootste belang. Aangezien de betrokkene niet direct betrokken is bij deze verwerkingen, zal het belang van het verstrekken van informatie over de verwerking op verzoek in belang toenemen, om zo een te grote informatie-asymmetrie tussen betrokkene en verantwoordelijke tegen te gaan.

Met de steeds verdere inbedding van informatietechnologie in onze alledaagse omgeving wordt de mate van mogelijke sturing via architectuur steeds groter. Zaken zijn immers steeds meer tot in het extreme aanpasbaar en personaliseerbaar. In feite gaat het om geautomatiseerde besluitvorming op basis van geobserveerde, gededuceerde of geïnduceerde gegevens. Vergaande personalisering op basis van profielen brengt het gevaar van inperking van de autonomie van individuen met zich mee. Tegelijkertijd kan echter betekenisvol inzicht in deze profielen juist een versterking van de autonomie van het individu met zich meebrengen, omdat hij op deze wijze inzage krijgt in zijn eigen oordeelsvorming of besluitvormingsproces.

Inzet van Big Data in de context van de overheid moet breder beschouwd worden dan alleen in het kader van privacybescherming. Beleidsvorming op basis van meer (empirische) gegevens kan veel voordelen met zich meebrengen op het vlak van efficiëntie en effectiviteit, maar de grenzen en beperkingen van deze gegevens moeten ook duidelijk in ogenschouw genomen worden. De gegevens zijn immers een model of representatie van de werkelijkheid, waarbij er zich veel vertekeningen kunnen voordoen die, wanneer er blind op geacteerd wordt, ongewenste gevolgen met zich mee kunnen brengen.

Big Data-technieken kunnen, behalve als instrument voor beleidsvorming, ook dienen als instrument voor nieuwe vormen van regulering, zoals *algorithmic regulation*. Hierbij staat niet de materiële rechtsregel centraal, maar het bereiken van een bepaald einddoel. De gewenste uitkomst staat zo centraal, en de invulling van de normen om tot die uitkomst te komen kan variëren.

Aangezien Big Data doorwerkt in alle aspecten van onze maatschappij, zelfs in de wijze waarop deze gereguleerd kan worden, zullen discussies hierover aan de hand van fundamentele rechten moeten worden gevoerd. Zet fundamentele rechten en beginselen daarom centraal, niet de technologische ontwikkeling zelf. De implementatie van techniek is uiteindelijk niet waardevrij, zelfs als de ontwikkeling niet door een specifieke agenda wordt bepaald.

9 Aanbevelingen/stellingen

- Big Data als techniek brengt zowel kansen als risico's ten aanzien van de bescherming van fundamentele rechten met zich mee.
- Big Data en aanverwante technologische ontwikkelingen werken door in alle aspecten van de maatschappij. Stel daarom de fundamentele rechten centraal en niet de technologische ontwikkeling.
- De bescherming van fundamentele rechten in een wereld met Big Data kan niet alleen door het recht en juristen opgelost worden. In het bijzonder ethici, statistici en sociaal psychologen zullen een belangrijke rol moeten vervullen, evenals bestuurders bij overheid en bedrijfsleven en politici.
- De invloed van Big Data en aanverwante technologische ontwikkelingen op persoonlijke autonomie en zelfbeschikking vergt de komende jaren veel aandacht.

Privacy en veiligheid: een oneindig labyrint?

*Mr. M. Belhaj en mr. S. Gün**

* Mr. Mohammed Belhaj en mr. Sultan Gün zijn beiden werkzaam bij de directie Juridische Zaken van Bestuur en organisatie van de gemeente Amsterdam. Dit artikel is op persoonlijke titel geschreven. Zij danken mr. J.E. Hoitink en mr. H.H.L. Krans voor hun commentaren op een eerdere versie van dit artikel.

1 Inleiding

Privacy en veiligheid houden de gemoederen steeds meer bezig. Het onderwerp heeft de laatste jaren verder aan belang(stelling) gewonnen. De publieke opinie laat daarbij geen consistente houding zien. Enerzijds lijkt de roep om 'meer veiligheid' – mede in het licht van internationale ontwikkelingen – sterker te worden. Dat dit onvermijdelijk leidt tot een verdergaande inbreuk op de privacy van overheidswege, lijkt men daarbij voor lief te nemen. Anderzijds brengen bijvoorbeeld de afluisterpraktijken van de Amerikaanse inlichtingendienst en – meer recent – de onzorgvuldige wijze waarop de Nederlandse Zorgautoriteit met gevoelige gegevens omgaat, een golf van kritiek teweeg.

Aan de overheid is de schone taak om deze – op het oog paradoxale – wensen met elkaar te verzoenen. De overheid kiest in dit verband de laatste jaren bij de bestrijding van criminaliteit steeds vaker voor een zogeheten 'integrale aanpak'. Overheidsorganen slaan dan – vaak aangevuld met semipublieke partijen – de handen ineen om de verkokering te doorbreken en criminaliteit zo adequaat mogelijk te bestrijden. In deze samenwerking is effectiviteit het richtsnoer. Waar effectiviteit leidend is, ontstaat evenwel het gevaar dat privacy als spelbreker wordt beschouwd en daarmee onder druk komt te staan.

In Amsterdam is de integrale aanpak inmiddels min of meer een vaste werkwijze geworden bij de bestrijding van criminaliteit en overlast. Dat betekent dat organisaties die aan de preventieve en repressieve zijde betrokken zijn bij criminaliteitsbestrijding, de krachten steeds vaker bundelen. Het uitwisselen van informatie is voor het welslagen van een integrale aanpak steeds van essentieel belang. Dat roept de vraag op of en, zo ja, op welke wijze deze integrale aanpak door privacybelangen wordt begrensd.

Deze vraag blijkt niet eenvoudig te beantwoorden. De oorzaak is voor een belangrijk deel gelegen in de complexiteit van de Nederlandse privacywetgeving. Op een individuele casus zijn vaak meerdere privacywetten van toepassing, die niet altijd uitblinken in helderheid en zelfs op punten tegenstrijdig lijken. Dat de personen die op dagelijkse basis afwegingen maken over informatie-uitwisseling vaak niet juridisch geschoold zijn, draagt aan een soepele uitvoering van de privacywetgeving niet bij. De complexiteit en onduidelijkheid van de privacywetgeving komen reeds aan de oppervlakte wanneer een beperkt aantal partijen bij een gegevensuitwisseling betrokken is – laat staan bij een integrale aanpak, waarbij soms twintig tot dertig partijen betrokken zijn.

In dit preadvies staat de beperkende rol van privacy bij de bestrijding van criminaliteit en overlast centraal. Daarbij dient de Amsterdamse bestuurlijke

praktijk als inspiratiebron. Aan de hand van verschillende praktijkvoorbeelden wordt het spanningsveld tussen veiligheid en privacy in de praktijk inzichtelijk gemaakt en wordt beschreven welke dilemma's zich daarbij voordoen en hoe deze worden opgelost.

Het preadvies bestaat uit twee onderdelen. In het eerste onderdeel wordt aan de hand van een praktijkvoorbeeld van gegevensuitwisseling tussen twee partijen de complexiteit van de privacywetgeving geïllustreerd. Vervolgens wordt aan de hand van de drie samenwerkingsverbanden de Top600, de Treiteraanpak en de Regionale Informatie- en Expertise Centra (RIEC) toegelicht hoe deze complexiteit bij gegevensuitwisseling tussen meerdere partijen verder toeneemt.

In het tweede onderdeel is er aandacht voor de rechtsonzekerheid die het gebruik van open begrippen binnen de privacywetgeving met zich brengt. Open begrippen zijn nodig omdat zij niet snel verouderen en ruimte laten voor maatwerk, maar is de praktijk er voldoende mee geholpen? Tot slot volgen de conclusies, waarbij de verschillende onderdelen met elkaar in verband worden gebracht.

2 Privacywetgeving voor twee

2.1 Het verhaal van de burgemeester en de politiegegevens

De burgemeester is op grond van de Gemeentewet belast met de handhaving van de openbare orde. De burgemeester kan die taak alleen adequaat uitvoeren indien hij ook over de nodige politiegegevens beschikt. In dit verband is relevant dat artikel 16 van de Wet politiegegevens (Wpg) bepaalt dat de verstrekking van politiegegevens aan gezagsdragers, onder wie burgemeesters, slechts is toegestaan voor zover zij deze behoeven in het kader van 'de handhaving van de openbare orde'.

Het is op grond van deze bepaling evenwel onduidelijk op welk *moment* de politie de burgemeester van de desbetreffende politiegegevens dient te voorzien. Immers, over de reikwijdte van het begrip 'handhaving van de openbare orde' kan verschillend worden gedacht. Dat verschil is niet louter theoretisch van belang, maar kan ook voor de praktijk verstrekkende gevolgen hebben. De reikwijdte van het begrip bepaalt immers op welk moment politiegegevens aan de burgemeester verstrekt mogen worden. Dat moment is op zijn beurt bepalend voor de vraag hoe slagvaardig een burgemeester kan optreden. Het bepalen van het juiste moment is bovendien van belang omdat de politie bij een voortijdige verstrekking onrechtmatig handelt – en eventuele juridische stappen door een betrokkene tegemoet kan zien.

2.2 Politiegegevens: nu of straks?

De vraag is derhalve hoe de wetgever de zinsnede 'de handhaving van de openbare orde' in artikel 16 lid 1 sub c onder 2 Wpg heeft bedoeld.

De memorie van toelichting bij deze bepaling verwijst op dit punt naar de toelichting op artikel 15 lid 1 onderdeel a van de Wet politieregisters (Wpr) als voorganger van de Wpg.[1] In de memorie van toelichting bij de Wpr is vermeld dat met de bepaling een reeds langer bestaande wens wordt gehonoreerd om burgemeesters politiële informatie te verstrekken ten behoeve van hun taken bij de handhaving van de openbare orde. Ook wordt opgemerkt dat het voor een behoorlijke uitoefening van de algemene – in de Gemeentewet neergelegde – taak van de burgemeester om de openbare orde te handhaven noodzakelijk is dat de burgemeester acht kan slaan op de gegevens uit politieregisters.[2]

1 *Kamerstukken II* 2005/06, 30327, 3 (MvT), p. 70.
2 *Kamerstukken II* 1996/97, 25298, 3 (MvT), p. 12.

De Wpr en de Wpg verwijzen derhalve naar de Gemeentewet en lijken daarmee de invulling van het begrip in die wet volgen. De Gemeentewet kent evenwel geen definitie van het begrip 'openbare orde'. Wel is in de bijbehorende Kamerstukken vermeld dat het uitgangspunt is dat de openbare orde wordt beheerst door een complex van rechtsregels dat ziet op het gewenste niveau van orde en rust in het openbare leven. Handhaving van de openbare orde betreft dan de zorg voor naleving van die regels. Volgens de Kamerstukken zal met name de gemeenteraad het gewenste niveau van orde en rust moeten bepalen en beïnvloeden door middel van normstelling, bijvoorbeeld in de Algemene Plaatselijke Verordening (APV).[3] Voorts blijkt uit de Kamerstukken dat het begrip 'handhaving van de openbare orde' twee elementen omvat.[4] Enerzijds omvat dit begrip de daadwerkelijke voorkoming en beëindiging van zich concreet voordoende of dreigende verstoringen van de openbare orde. Anderzijds omvat het begrip ook de algemene bestuurlijke voorkoming van strafbare feiten, hetgeen ziet op het beleid inzake preventie van openbare ordeverstoringen. Hieruit blijkt dat de wetgever wel degelijk preventie op het oog heeft gehad bij het in het leven roepen van de genoemde bevoegdheden.

De Afdeling bestuursrechtspraak van de Raad van State (hierna: de Afdeling) lijkt preventie eveneens te beschouwen als onderdeel van de taak om de openbare orde te handhaven. Zij sprak zich in die richting uit in een kwestie waarin politiegegevens waren verstrekt aan de burgemeester op grond van artikel 16 lid 1 sub c onder 2 Wpg.[5] In bedoelde kwestie weigerde de burgemeester de aanvraag voor een exploitatievergunning op grond van de APV omdat de aanvrager naar zijn oordeel van 'slecht levensgedrag' was. De burgemeester was tot dat oordeel gekomen op basis van de strafrechtelijke antecedenten van de aanvrager, die hij bij de politie op grond van de Wpg had opgevraagd. Van een concrete verstoring van de openbare orde was op het moment van de weigering van de aanvraag derhalve nog geen sprake.

Appellant voerde in hoger beroep aan dat de verstrekking van politiegegevens diende te worden beschouwd als een verstrekking op grond van artikel 20 Wpg (de structurele verstrekking van gegevens aan samenwerkingsverbanden). Appellant stelde dat weliswaar sprake was van een convenant tussen de betrokken partijen, maar dat niet was voldaan aan de daarin geformuleerde voorwaarden voor gegevensverstrekking. De Afdeling oordeelde dat de aanwezigheid van een convenant niet in de weg staat aan de verstrekking van politiegegevens op grond van artikel 16 lid 1 sub c onder 2 Wpg. De Afdeling lijkt daarmee – weliswaar impliciet – te oordelen dat politiegegevens op grond van artikel 16 lid 1 sub c onder 2 Wpg ook kunnen worden verstrekt ten behoeve van het treffen van preventieve maatregelen in het kader van de openbare orde.

Hoewel de Kamerstukken en de Afdeling deze uitleg lijken voor te staan, wordt het begrip 'handhaving van de openbare orde' in de praktijk zowel op precieze als op rekkelijke wijze geïnterpreteerd. De politie is de laatste jaren geneigd vaker te

3 *Kamerstukken II* 1988/89, 19403, 10 (MvA), p. 88 en 89.
4 *Kamerstukken II* 1989/90, 19403,16, (Nota n.a.v. het Eindverslag), p. 38.
5 ABRvS 16 oktober 2013, ECLI:NL:RVS:2013:1523.

kiezen voor de precieze interpretatie. Dat heeft tot gevolg dat de politie alleen bereid is de burgemeester politiegegevens te verstrekken bij concrete verstoringen van de openbare orde. De politie wijst er daarbij op dat het gaat om uiterst gevoelige persoonsgegevens, waarbij de beginselen van proportionaliteit en subsidiariteit zwaar wegen. Burgemeesters – onder wie de burgemeester van Amsterdam – neigen evenwel naar een meer rekkelijke uitleg, waardoor ook preventie als onderdeel van de wettelijke taak om de openbare orde te handhaven wordt beschouwd. In die opvatting zouden burgemeesters dus ook over politiegegevens moeten kunnen beschikken *voordat* een verstoring van de openbare orde zich manifesteert, teneinde een eventuele openbare ordeverstoring te voorkomen. Dit kan, zoals uit voornoemde uitspraak blijkt, bijvoorbeeld voor burgemeesters van belang zijn om een adequaat en effectief horecabeleid te kunnen voeren door een 'levensgedragtoets' voor de exploitant in de regelgeving op te nemen. Het kan tevens voor burgemeesters van belang zijn om te kunnen anticiperen op bijvoorbeeld de komst van hooligans bij voetbalwedstrijden, wanneer de politie weet heeft van ernstige antecedenten van de supporters van de betrokken clubs.

Doordat de wettekst zelf geen duidelijkheid verschaft over dit belangrijke punt, is er in de praktijk een onbedoelde hobbel ontstaan voor de informatieverschaffing tussen politie en burgemeesters. Die wordt niet veroorzaakt door onwil bij de politie, maar door onzekerheid over de geoorloofdheid van het verstrekken van privacygevoelige informatie. Deze onzekerheid kan meebrengen dat de burgemeesters belangrijke informatie wordt onthouden, waardoor adequaat optreden bij dreigende verstoring van de openbare orde wordt bemoeilijkt.

3 Privacy voor meer

Het zal niet verbazen dat het aantal privacygerelateerde dilemma's bij een integrale aanpak verder toeneemt. Hierna worden verschillende dilemma's belicht die aan de orde zijn bij de Amsterdamse samenwerkingsverbanden de Top600 en de Treiteraanpak. De doelen en de werkwijzen van de Top600 en de Treiteraanpak verschillen. Waar bij de Top600 het doel is om criminaliteit te bestrijden door zowel straf- als zorgmaatregelen te treffen, ligt bij de Treiteraanpak vooralsnog de nadruk op sancties om het treiteren te beëindigen. Wel komen de inrichting en het wettelijk kader inzake de uitoefening van bevoegdheden door de betrokken instanties enerzijds en de verwerking van persoonsgegevens anderzijds gedeeltelijk overeen. Daarom zullen deze algemene aspecten eenmaal worden belicht bij de bespreking van de Top600 en zal daar bij de bespreking van de Treiteraanpak, waar nodig, naar worden verwezen.

In dit hoofdstuk komt voorts ook het samenwerkingsverband RIEC aan de orde, waarbij het doel is georganiseerde criminaliteit te bestrijden. Het RIEC wordt separaat besproken, omdat bij dat samenwerkingsverband, in tegenstelling tot de Top600 en de Treiteraanpak, alleen overheidsorganisaties, waaronder de Belastingdienst, partij zijn. Dit roept vanuit het oogpunt van de privacy andere vragen op.

3.1 De Top600

3.1.1 De totstandkoming van de Top600

In 2011 bleek dat op het terrein van de criminaliteit in de regio Amsterdam goed en minder goed nieuws te melden was. Het aantal misdrijven liet een dalende trend zien – dat was het goede nieuws. Het minder goede nieuws was dat de misdrijven steeds ernstiger werden – en dat de daders vaak jong, gewelddadig en moeilijk te bereiken waren. Zo was bijvoorbeeld sprake van een sterke stijging van roofovervallen met grof geweld. Daarbij waren jaarlijks ruim 500 jeugdige personen betrokken. Voor geweldsmisdrijven (mishandeling, bedreiging en openlijk geweld) werden jaarlijks tussen de 2500 en 3000 jeugdige verdachten aangehouden. Daarnaast waren jeugdige verdachten jaarlijks bij circa 170 geweldmisdrijven met een vuurwapen betrokken.

Een groep van circa 600 personen bleek in vijf jaar tijd verantwoordelijk voor 15.000 mutaties in de politieregisters (aanhoudingen als verdachte of mutatie als betrokkene). Deze personen waren vaak al eens veroordeeld. Zij waren in meerderheid tussen de 18 en 24 jaar. Delicten die zij pleegden (overvallen, straatroven,

geweldsmisdrijven en woninginbraken) hadden een grote impact op de slachtoffers en de omgeving.

De politie kwam bij deze misdrijven veelal dezelfde daders tegen. Veel organisaties hielden zich beurtelings of gelijktijdig met deze jongvolwassenen bezig – elk vanuit het eigen institutionele protocol/belang. Alle goede bedoelingen ten spijt bleken de afzonderlijke interventies recidive vaak niet te kunnen voorkomen. Deze jongeren gingen vaak niet meer naar school en hun ouders bleken nauwelijks meer grip op hen te hebben. Zij hadden vaak last van psychische problemen of waren verslaafd aan drank of drugs. Hun jongere broertjes/zusjes volgden meer dan eens hun voorbeeld, omdat crimineel gedrag leek te lonen.

De burgemeester van Amsterdam besloot dat het bij deze stand van zaken tijd was voor een nieuwe aanpak. Daarbij moest een optimale samenwerking tussen de betrokken instanties om de jongere weer op het rechte pad te krijgen, het uitgangspunt zijn. Zo is het fundament voor de Top600 gelegd.

3.1.2 Convenant Top600

De Top600 is een samenwerkingsverband waarbij meer dan dertig instanties betrokken zijn van zowel de preventieve als de repressieve zijde van de criminaliteitsbestrijding. De kernpartners bij de aanpak zijn het college van burgemeester en wethouders van Amsterdam, de burgemeester van Amsterdam, het Openbaar Ministerie te Amsterdam en de Politie Eenheid Amsterdam. Zij zijn tevens de 'verantwoordelijken' voor de verwerking van persoonsgegevens zoals bedoeld in artikel 1 aanhef en onder d van de Wet bescherming persoonsgegevens (Wbp).

De partijen bij de Top600 hebben in 2011 met elkaar het Convenant Aanpak Top600 gesloten. De aanpak is in mei 2013 verlengd met het Convenant Aanpak Top600 II (hierna: het Convenant).[6] Blijkens dit Convenant zijn de betrokken partijen overeengekomen:

> 'de aanpak Top600 voort te zetten en daartoe opnieuw een samenwerkingsverband aan te gaan met enerzijds het doel het aantal high-impact delicten significant terug te dringen door een persoonsgebonden integrale aanpak van degenen die verdacht zijn van of veroordeeld zijn voor deze feiten en bovendien verdere schade aan deze personen, aan hun eventueel aanwezige minderjarige broers, minderjarige zussen en minderjarige kinderen en aan de samenleving te voorkomen en anderzijds de privacy van de betrokkenen zo veel mogelijk te waarborgen'.

Met het samenstellen van de lijst Top600 wordt derhalve beoogd de groep personen die in Amsterdam het vaakst betrokken zijn bij zogeheten *high-impact* delicten in beeld te brengen. In het kader van de Top600 zijn overvallen, straatroven, woninginbraken, zware mishandeling, openlijke geweldpleging en moord/doodslag als high-impact delicten gekwalificeerd. Van deze delicten is

6 Zie voor meer informatie en de tekst van het convenant: www.amsterdam.nl/gemeente/organisatie-diensten/sites/top600/top600-o/top600/.

bekend dat zij een aanzienlijke impact hebben op de slachtoffers – en dat zij daarnaast leiden tot maatschappelijke onrust en gevoelens van onveiligheid. Het doel van de Top600 is het aantal high-impact delicten terug te dringen door de personen op de lijst op maat gesneden zorg en begeleiding aan te bieden teneinde recidive te voorkomen. Het sleutelwoord bij de Top600-aanpak is gedragsverandering. De Top600-aanpak probeert dit te bereiken door invulling te geven aan de eerste twee aspecten van het adagium 'woning, werk, wederhelft'. Binnen deze randvoorwaarden is sprake van 600 verschillende maatwerk-aanpakken. De aanpak van de Top600 valt dan ook in de volgende drie (samenhangende) pijlers uiteen:

– *Pijler 1:* Snel en consequent straffen bij crimineel gedrag en intelligent gebruikmaken van de combinatie straf en zorg.
– *Pijler 2:* Intensieve zorg ter voorkoming van recidive. Tijdens en na de uitvoering van de straf worden op de persoon toegesneden zorg en begeleiding aangeboden.
– *Pijler 3:* Beperken van de instroom en de doorstroom: aandacht voor broertjes en zusjes en/of kinderen van de persoon op de lijst Top600.

3.1.3 Wettelijk kader bij de Top600

Wat betreft het wettelijk kader bij de Top600 is het van belang te onderscheiden tussen de uitoefening van (bestaande) bevoegdheden door de betrokken instanties enerzijds en de verwerking van persoonsgegevens door instanties anderzijds.

3.1.4 De bevoegdheden van partijen

Wat betreft de uitoefening van bevoegdheden geldt dat de Top600 geen nieuwe bevoegdheden creëert. De Top600 is immers niets meer dan een gecoördineerde inzet van gemeente, politie, justitie en andere instanties om crimineel gedrag terug te dringen. De gecoördineerde inzet vindt plaats binnen de daarvoor geldende wettelijke kaders en op basis van reeds *bestaande* taken en bevoegdheden van de deelnemende partijen. Dit betekent bijvoorbeeld concreet dat de burgemeester, de politie en het Openbaar Ministerie bij de aanpak van de Top600 in de uitoefening van hun wettelijke taken en bevoegdheden gebonden zijn en blijven aan de bepalingen uit respectievelijk de Gemeentewet, de Politiewet 2012 en het Wetboek van Strafvordering (Sv). De Reclassering blijft bijvoorbeeld gebonden aan de Reclasseringsregeling 1995 en de Dienst Werk en Inkomen (DWI) aan de Wet werk en bijstand.

Wel wordt, waar mogelijk, *geprioriteerd* binnen de geldende wettelijke kaders. Voor de burgemeester bestaat de mogelijkheid tot prioriteren op grond van de (discretionaire) bevoegdheid van artikel 172 Gemeentewet. Voor de politie bestaat die mogelijkheid op grond van artikel 3 jo. artikel 11 lid 2 jo. artikel 12 lid 2 Politiewet 2012. Het Openbaar Ministerie kan prioriteren op grond van het opportuniteitsbeginsel, zoals neergelegd in artikel 167 jo. artikel 242 Sv. Voor het prioriteren in het kader van de Top600 is ook reden. De personen op de lijst Top600 staan daar niet voor een wissewasje op: zij kunnen worden aangemerkt als de groep

verdachten en/of daders die vaak betrokken zijn (geweest) bij high-impact delicten. Vanwege de aard van de problematiek, de ernst van de gedragingen en het belang van het voorkomen van strafbare feiten wordt prioritering in het kader van de aanpak van de Top600 gerechtvaardigd geacht.

3.1.5 *Privacy en de Top600*

De verwerking van persoonsgegevens is het hart van de Top600. De meerwaarde van de aanpak is dat de betrokken instanties weliswaar bestaande bevoegdheden uitoefenen, maar dat zij die wel op elkaar kunnen afstemmen omdat zij over relevante informatie kunnen beschikken. In het kader van de Top600 delen instanties uit de strafrechtsketen en de zorgketen daarom informatie.

De verwerking van persoonsgegevens begint op het moment dat een betrokkene op de lijst Top600 wordt geplaatst. Voor plaatsing op de lijst Top600 wordt in het kader van transparantie gebruikgemaakt van selectiecriteria, die in het Convenant zijn beschreven. Deze criteria vallen uiteen in politiecriteria enerzijds en justitiële criteria anderzijds.[7] Kort gezegd, houdt het belangrijkste politiecriterium in dat de betrokkene gedurende een bepaald tijdvak minimaal drie keer verdachte moet zijn geweest van een high-impact delict. Daarnaast dient – afhankelijk van de leeftijd van betrokkene – sprake te zijn van één, twee of drie veroordelingen, maatregelen dan wel taakstraffen binnen hetzelfde tijdvak. Vanuit de Top600 wordt elk halfjaar aan deze criteria getoetst. De toetsing leidt ertoe dat bij elke actualisatieronde personen de Top600 instromen en uitstromen.

Wanneer een betrokkene aan de selectiecriteria voldoet en op de lijst wordt geplaatst, wordt een zogeheten 'basisdossier' van de betrokkene samengesteld. De kernpartners bij de Top600 leveren ten behoeve van het basisdossier relevante informatie over de betrokkene. De politie en het Openbaar Ministerie dragen bijvoorbeeld informatie aan over het strafrechtelijke verleden. De gemeente levert informatie aan over de inschrijvingen, eventuele uitkeringen en de onderwijssituatie. Verder wordt in het basisdossier – een beperkte mate van – informatie uit medische bronnen (waarover later meer) opgenomen, alsmede informatie over de thuissituatie van betrokkene. Het dossier wordt vervolgens besproken in de zogeheten 'Weegploeg'. De Weegploeg is het ambtelijke overlegorgaan waarin de kernpartners zijn vertegenwoordigd. De Weegploeg beslist op basis van de heersende problematiek welke kernpartner een regisseur voor de betrokkene zal leveren.

De regisseur wordt als de spil van de Top600-aanpak beschouwd. Wanneer hij eenmaal een basisdossier onder zijn hoede heeft, stelt hij op basis van de daaruit blijkende problematiek een plan van aanpak vast. Vervolgens selecteert hij de partijen bij de Top600 die hij nodig heeft om het plan van aanpak uit te voeren. Die partners plegen feitelijk de interventies en worden in de wandelgangen daarom ook wel kort als de interventieplegers aangeduid. Het is de regisseur

7 Zie de artikelen 6.11 en 6.3 jo. bijlagen 1 en 2 van het Convenant.

die bepaalt welke informatie welke interventiepleger nodig heeft om zijn taken naar behoren uit te kunnen voeren. Bij die afweging toetst de regisseur steeds aan de eisen van doelbinding, zoals geformuleerd in het Convenant (artikel 7 Wbp) en aan de eis van noodzakelijkheid (artikel 11 Wbp). De interventieplegers rapporteren aan de regisseur over de voortgang en de uitkomsten van de interventies, waardoor de regisseur waar nodig kan bijsturen.

Waar leidt deze werkwijze nu in de praktijk toe? Dat is wellicht het best aan te tonen aan de hand van een hypothetische Top600-casus. Betrokkene – wij noemen hem Jason – is op de lijst Top600 geplaatst. Jason is 18 jaar en is door de jaren heen vele malen met politie en justitie in aanraking geweest. Hij woont in een buurt waar een overlastgevende jongerengroep huishoudt. Jason is ontvankelijk voor sociale druk vanuit deze groep en doet soms ook mee aan het lastigvallen van voorbijgangers, straatroven, geweldplegingen enzovoort. Jason woont samen met zijn ouders en zijn vier zussen en twee broers in een kleine flat. De ouders van Jason hebben een klein inkomen en zelf heeft hij schulden, waaronder meerdere niet-betaalde verkeersboetes. Zijn moeder is de spil van het gezin en probeert zo goed en zo kwaad als het gaat voor een goede opvoeding te zorgen; de vader van Jason is veel weg en nauwelijks bij de opvoeding betrokken. Jason zit op het mbo, maar gaat soms langere periodes niet naar school. Bovendien moet hij om zijn studie af te maken een aantal maanden stage lopen. Het lukt hem mede vanwege zijn strafblad niet een stage te vinden. Verder lijkt Jason tekenen van een persoonlijkheidsstoornis te tonen, maar weigert hij een *screening* van de gemeentelijke gezondheidsdienst (GGD) die aan alle Top600-personen wordt aangeboden om optimaal op de zorgbehoefte in te kunnen spelen. Jason kan bijvoorbeeld uit het niets in woede ontsteken. Hij gedraagt zich vaak erg agressief richting de politie. Hij moet, tot slot, nog in een strafzaak voor de rechter verschijnen.

In dit concrete geval kan de Top600-regisseur van Jason – mits Jason meewerkt – een aantal dingen doen. Zo zal hij bijvoorbeeld inzetten op het vinden van een stage voor Jason, opdat hij zijn diploma kan behalen. Daarvoor kan hij gebruikmaken van bestaande afspraken met verschillende winkelketens/kruideniers, die zich bereid hebben verklaard stageplekken voor personen op de lijst Top600 beschikbaar te stellen. Indien nodig, kan de regisseur Jason een sollicitatietraining aanbieden via de DWI: Jason zal dan met voorrang (vanwege de geldende prioritering) van een dergelijke cursus gebruik kunnen maken. De regisseur weet evenwel vanwege de informatie-uitwisseling dat Jason op korte termijn moet voorkomen in een strafzaak en dat de kans bestaat dat hij een onvoorwaardelijke straf krijgt, waardoor hij feitelijk niet aan zijn stage kan beginnen. De regisseur zal daarom in contact treden met de Reclassering en/of het Openbaar Ministerie om te bespreken of het eisen van een voorwaardelijke straf met bijzondere voorwaarden tot de mogelijkheden behoort. Die voorwaarde kan zijn dat als Jason niet aan zijn stageverplichtingen voldoet, de straf alsnog wordt omgezet in een onvoorwaardelijke straf. Daarnaast zou een voorwaarde kunnen zijn dat Jason een agressiecursus volgt. De voorwaarden zorgen ervoor dat richting Jason een stok achter de deur aanwezig is.

Verder weet de regisseur vanwege de informatie-uitwisseling dat Jason schulden heeft die deels bestaan uit onbetaalde verkeersboetes. De regisseur zou op dit punt met het Centraal Justitieel Incasso Bureau (CJIB) in contact kunnen treden

om een betalingsregeling te organiseren. De regisseur zou op termijn ook het aanbod voor zelfstandig wonen kunnen doen om Jason uit de omgeving te halen waar hij door groepsdruk tot het plegen van strafbare feiten wordt verleid. In dat verband zou de regisseur met de woningbouwcorporaties dan wel met een project als 'Pak je kans' in contact kunnen treden. Jason zou dan door deze organisaties met prioriteit – onder strikte voorwaarden – een (sloop)woning toegewezen kunnen krijgen. Als Jason daarvoor inkomen in de vorm van een uitkering nodig zou hebben, kan de regisseur ondersteunen bij het indienen van de aanvraag en zal de aanvraag met prioriteit door de DWI worden behandeld. Tot slot zou de regisseur de politie bijvoorbeeld kunnen verzoeken Jason te de-prioriteren in de periode dat hij de agressiecursus volgt, of het Preventief Interventie Team kunnen inlichten als er signalen zijn dat een minderjarig broertje of zusje ook in de criminaliteit dreigt verzeild te raken.[8]

De gevolgen van de Top600-aanpak voor een betrokkene worden in belangrijke mate bepaald door zijn bereidheid om mee te werken. Indien de betrokkene laat zien dat hij het criminele pad wil verlaten, behoort alle hiervoor beschreven hulp tot de mogelijkheden. Maar als de betrokkene medewerking weigert, zal hij vooral het zuur van de Top600 moeten aanvaarden. Dat betekent bijvoorbeeld concreet dat hij op meer belangstelling van de politie kan rekenen en dat bij strafbare feiten sprake is van lik-op-stukbeleid. Van coulance vanuit de Top600 is dan geen sprake. Want het uitgangspunt bij de Top600 is ook: voor niets gaat de zon op, of – eveneens huiselijk gezegd – voor wat hoort wat.

Uit voorgaand voorbeeld blijkt dat het delen van informatie, dus, voor het welslagen van de Top600-aanpak van essentiële waarde is. De vraag rijst wel of het delen van al die gegevens is toegestaan en welk juridisch kader daarvoor geldt.

Inmiddels zijn de hoofduitgangspunten van de aanpak Top600 door de rechtbank beoordeeld en rechtmatig bevonden. In een recente zaak heeft de rechtbank Amsterdam, kort en goed, bepaald dat:[9]
- de plaatsing van eiser op de lijst Top600 van belang kan zijn voor het terugdringen van crimineel gedrag, het voorkomen van recidive en re-integratie van eiser;
- de plaatsing op de lijst Top600 ter zake dienend is voor het doel van de gegevensverwerking;
- de selectiecriteria niet te ruim zijn gesteld, omdat daaruit blijkt dat er nog relatief recent sprake is geweest van een strafrechtelijke verdenking.

In een andere recente zaak heeft de (meervoudige kamer van de) rechtbank Amsterdam geoordeeld dat:[10]
- de gegevensuitwisseling in het kader van de Top600 in overeenstemming is met artikel 8 van het Europees Verdrag voor de rechten van de mens (EVRM);

8 Het Preventie Interventie Team is het onderdeel van de Top600 dat verantwoordelijk is voor de uitvoering van pijler 3.
9 Rb. Amsterdam 24 september 2014, zaaknummer AMS 14/2376.
10 Rb. Amsterdam 16 oktober 2014, zaaknummer AMS 12/4896.

– plaatsing op de lijst Top600 geen punitieve sanctie is, waardoor de plaatsing niet in strijd is met de onschuldpresumptie, zoals neergelegd in artikel 6 EVRM;
– het gebruik van aanhoudingen als selectiecriterium voor plaatsing op de lijst Top600 niet in strijd is met artikel 6 EVRM;
– eiser geen rechtsmiddelen dient aan te wenden tegen het samenwerkingsverband Top600, maar tegen de individuele partner als hij van mening is dat sprake is van onrechtmatige bevoegdheidsuitoefening. De context bij dit oordeel is dat eiser stelde dat de politie hem sinds zijn plaatsing op de lijst Top600 stelselmatig benaderde. Volgens eiser handelde de politie daardoor onrechtmatig. De rechtbank kwam evenwel tot het oordeel dat die kwestie zich niet leent voor toetsing in een zaak die in essentie gaat over de gegevensuitwisseling in het kader van de Top600.

Voornoemde uitspraken van de rechtbank Amsterdam stemmen tot tevredenheid. Daarmee zijn evenwel nog niet alle vragen beantwoord, zoals uit een aantal hierna te schetsen dilemma's zal blijken.

3.1.6 Dilemma's

De Top600 is een samenwerkingsverband en beschikt als zodanig niet over 'eigen' gegevens. De gegevens worden, zoals gezegd, aan de Top600 geleverd door de daarbij betrokken instanties (de 'bronleveranciers'), zoals bijvoorbeeld de politie, het Openbaar Ministerie, de DWI en de Reclassering. Wil de informatie van deze bronleveranciers in het samenwerkingsverband Top600 kunnen vloeien, dan dient voor elke afzonderlijke overdracht van informatie een grondslag te zijn in de toepasselijke wetten en regels. Dit betekent bijvoorbeeld dat de politie zich bij het verstrekken van gegevens dient te houden aan de daaraan gestelde voorwaarden in de Wpg, dat het Openbaar Ministerie zich dient te houden aan de Wet justitiële en strafvorderlijke gegevens (WJG), en dat de Reclassering zich dient te houden aan Reclasseringsregeling 1995. De wetten bevatten naast grondslagen voor de verstrekking van gegevens tevens geheimhoudingsverplichtingen ten aanzien van deze gegevens. Daarnaast gelden voor de verschillende bronleveranciers vaak ook nog interne privacyreglementen. Wanneer de betrokken organisatie eenmaal heeft bepaald dat voor het verstrekken van de gegevens een grondslag in de geldende wetgeving bestaat en deze gegevens in de Top600 zijn gevloeid, dan zijn op de verwerking daarvan *binnen* het samenwerkingsverband vervolgens de Wbp en het Convenant van toepassing. De regisseur treedt dan op als de informatiemakelaar bij de individuele aanpak.

Het voorgaande laat zien dat bij gegevensuitwisseling in het kader van een samenwerkingsverband als de Top600 algemene wetgeving, bijzondere wetgeving, convenanten en (eventueel) privacyreglementen of protocollen veelal naast elkaar gelden. Daardoor doemen in de praktijk vanuit privacyrechtelijk oogpunt verschillende dilemma's op. Dat de ruim dertig partijen bij de Top600 aan verschillende wetten zijn gebonden voor het verstrekken van persoonsgegevens aan de Top600, is reeds een uitdaging op zich. Maar ook wanneer die horde is

genomen en de informatie zich eenmaal binnen het samenwerkingsverband bevindt, rijzen nog veel privacygerelateerde vragen.

3.1.6.1 De bijzondere verhouding tussen verschillende privacywetten

Zo is de verhouding tussen een bijzondere privacywet, zoals de Wpg, de Wjsg of de Reclasseringsregeling, enerzijds en de regels voor bijzondere (medische, strafrechtelijke etc.) persoonsgegevens, zoals bedoeld in artikel 16 Wbp, anderzijds niet altijd even duidelijk.

Dit kan wederom het beste worden geïllustreerd aan de hand van de regelgeving die van toepassing is op het verwerken van politiegegevens c.q. strafrechtelijke gegevens.

Artikel 20 Wpg biedt de korpschef van de politie de mogelijkheid een besluit te nemen tot het structureel verstrekken van politiegegevens aan een samenwerkingsverband. De politie verstrekt op deze grondslag structureel politiegegevens aan het samenwerkingsverband Top600. Binnen het samenwerkingsverband Top600 worden deze gegevens vervolgens verwerkt op grond van artikel 22 lid 1 Wbp jo. artikel 22 lid 6 Wbp. Deze artikelen bepalen onder andere dat het verbod op de verwerking van strafrechtelijke persoonsgegevens niet geldt indien deze gegevens zijn verkregen krachtens de Wpg, zoals in het geval van de Top600 dus het geval is. Hieruit lijkt te volgen dat wanneer de strafrechtelijke gegevens eenmaal in het samenwerkingsverband Top600 zijn gevloeid, op de verdere verwerking ervan de Wbp van toepassing is. Dat betekent concreet dat bij de verwerking van de politiegegevens tussen de betrokken partijen *binnen* het samenwerkingsverband en op de verstrekking van politiegegevens *vanuit* het samenwerkingsverband aan derden – derhalve partijen die geen onderdeel vormen van het samenwerkingsverband Top600 – zou moeten worden getoetst aan de eisen van de Wbp.

Toch is dat geen uitgemaakte zaak. De wetgever heeft namelijk bepaald dat op verstrekte politiegegevens steeds de geheimhoudingsplicht van artikel 7 lid 2 Wpg van toepassing blijft. Dat artikel bepaalt dat de persoon aan wie politiegegevens zijn verstrekt, verplicht is tot geheimhouding daarvan, behoudens voor zover een bij of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt. In de memorie van toelichting wordt expliciet opgemerkt dat de verplichting tot geheimhouding aan de doorverstrekking van gegevens in de weg staat.[11] Voorts blijkt uit de memorie van toelichting dat de zinsnede 'of zijn taak daartoe noodzaakt' beperkt dient te worden uitgelegd.[12] Dat zou concreet betekenen dat de politiegegevens tussen de partijen binnen het samenwerkingsverband Top600 in beginsel niet zouden mogen worden gedeeld. Want binnen het samenwerkingsverband zou elke betrokken partij moeten nagaan of haar taak noodzaakt tot het maken van een uitzondering op de geheimhoudingsplicht om zodoende dit gegeven met een andere partij binnen het samenwerkingsverband te kunnen delen. Dat is in het kader van een samenwerkingsverband als de Top600, waarbij meer dan dertig verschillende partijen zijn aangesloten, geen eenvoudig hanteerbaar criterium. Bovendien zou de toepasselijkheid van artikel 7 Wpg

11 *Kamerstukken II* 2005/06, 30327, 3, p. 37.
12 Idem.

betekenen dat gegevens ook niet aan derden buiten het samenwerkingsverband mogen worden verstrekt.

Deze constructie van geheimhouding op politiegegevens doet juridisch vreemd aan. De bepaling lijkt haaks te staan op het beginsel dat een bijzondere wet (in dit geval de Wpg) derogeert aan een algemene wet (in dit geval de Wbp). De toepassing van dat beginsel zou in casu moeten betekenen dat ten aanzien van de politiegegevens binnen de Top600 de geheimhoudingsplicht van artikel 7 Wpg geldt – terwijl echter op grond van artikel 22 lid 1 en lid 6 Wbp – de algemene privacywet – het delen van deze gegevens nu juist wel is toegestaan wanneer deze gegevens op grond van de Wpg zijn verkregen en/of er door samenwerkingsverbanden waarborgen ten aanzien van de bescherming van de privacy zijn ingebouwd. Verschieten de politiegegevens eenmaal binnen het samenwerkingsverband nu wel of niet van kleur?

Deze discussie lijkt een hoog theoretisch gehalte te hebben, maar is voor de praktijk wel degelijk van belang. Het is immers bepalend voor het antwoord op de vraag welke maatstaf de partijen in een samenwerkingsverband als de Top600 moeten hanteren bij het uitwisselen van politiegegevens onderling of de verstrekking daarvan aan derden buiten het samenwerkingsverband. Geldt de geheimhoudingsplicht van artikel 7 lid 2 Wpg, die in beginsel aan doorverstrekking in de weg staat? Of kan worden volstaan met een toetsing aan de minder stringente voorwaarden van artikel 22 en de artikelen 7 en volgende van de Wbp, waarin de algemene normen zijn neergelegd voor de uitwisseling van gegevens? Er lijkt sprake te zijn van tegenstrijdige wettelijke bepalingen, die de praktijk in verwarring brengen over wat nu is vereist.

Wat betreft het delen van de politiegegevens binnen samenwerkingsverbanden, wordt vanuit de Top600 gekozen voor de interpretatie dat artikel 22 Wbp jo. artikel 20 Wpg dient te worden gelezen als een uitzondering op de geheimhoudingsplicht van artikel 7 Wpg. Een andere opvatting zou ook haaks staan op de wens van de wetgever om voor samenwerkingsverbanden meer ruimte te creëren door recent in 2012 artikel 22 lid 6 in de Wbp op te nemen.[13] Het zou immers het functioneren van een samenwerkingsverband aanzienlijk bemoeilijken.

Dan rijst de vraag welke betekenis artikel 7 lid 2 Wpg heeft voor het verstrekken van politiegegevens *vanuit* het samenwerkingsverband Top600 aan *derden* die niet betrokken zijn bij het samenwerkingsverband. Moet worden aangenomen dat als de politiegegevens binnen het samenwerkingsverband onder het regime van de Wbp vallen, zij dit blijven doen wanneer zij vanuit het samenwerkingsverband worden doorverstrekt aan derden? Of geldt er voor samenwerkingsverbanden een uitzondering en herleeft bij een doorverstrekking naar partijen buiten het samenwerkingsverband de geheimhoudingsplicht van artikel 7 Wpg?

Vanuit de Top600 wordt zorgvuldigheidshalve voor de laatste – en daarmee voor de meest strikte – interpretatie gekozen en worden derhalve geen politiegegevens aan derden verstrekt zonder toestemming van de betrokkene – ook al zou dit

13 *Kamerstukken II* 2008/09, 31841, 3, p. 9.

behulpzaam kunnen zijn bij het uitvoeren van de doelstellingen van de Top600. Die keuze is ook mede ingegeven doordat het voor de niet-juridisch geschoolde medewerkers van de Top600 nagenoeg ondoenlijk is om bij elke concrete gegevensverwerking richting derden na te gaan of zijn taak als bedoel in artikel 7 Wpg daartoe wel noodzaakt. Indien verstrekking aan een derde toch noodzakelijk wordt geacht en de betrokkene daarvoor geen toestemming verleent, kan een derde overigens worden geadviseerd de politie rechtstreeks om incidentele informatieverstrekking op grond van artikel 19 Wpg te verzoeken. De politie zal dan een nieuwe afweging moeten maken.

De toepasselijkheid van artikel 7Wpg op de verstrekking van politiegegevens aan derden vraagt in de praktijk om juridische creativiteit om toch in het belang van de personen op de lijst Top600 te kunnen handelen. Vanuit de Top600 zijn bijvoorbeeld afspraken gemaakt met enkele werkgevers, die zich bereid hebben verklaard stageplaatsen beschikbaar te stellen aan de personen op de lijst Top600. Daarnaast zijn er bijvoorbeeld afspraken met enkele woningbouwcorporaties, die bereid zijn om (sloop)woningen aan deze personen beschikbaar te stellen. Deze afspraken zijn voor het welslagen van een individuele aanpak van groot belang. Toch brengt de toepasselijkheid van artikel 7 Wpg met zich dat aan de werkgevers en woningcorporaties – die geen convenantpartij zijn en daarmee als 'derden' dienen te worden beschouwd – in beginsel niet mag worden medegedeeld welke personen gebruik zullen maken van het aanbod. De aanduiding 'Top600' kan mogelijk worden beschouwd als een (indirect) politiegegeven in de zin van artikel 1 aanhef en onder a Wpg, of als een (indirect) strafrechtelijk gegeven zoals bedoeld in artikel 16 Wbp, omdat daarmee wordt prijsgegeven dat de persoon in kwestie een strafrechtelijk verleden heeft. Wil men aan deze lastige discussie ontkomen, dan kan het samenwerkingsverband eventueel worden uitgebreid door deze derden te vragen zich daarbij aan te sluiten. Wanneer dit evenwel om welke reden ook op bezwaren stuit, kan aan meer creatieve oplossingen worden gedacht.

Vanuit de Top600 is er bijvoorbeeld voor gekozen in dit soort gevallen met het toestemmingsvereiste te werken (vergelijk artikel 8 aanhef en sub a en artikel 23 lid 1 sub a Wbp). Na een selectie van geschikte personen op de lijst Top600 wordt aan de werkgever of de woningbouwcorporatie medegedeeld dat een persoon vanuit de Top600 zich zal melden voor een gesprek. Wanneer de persoon in kwestie aldaar verschijnt – nadat hij vooraf op de daaraan verbonden consequentie is gewezen –, wordt dit aldus opgevat dat betrokkene toestemming heeft verleend. Daarnaast wordt dit aldus geïnterpreteerd dat de betrokkene door te verschijnen het gegeven dat hij op de lijst Top600 staat (voor zover dit als een bijzonder persoonsgegeven te beschouwen is) ook zelf heeft geopenbaard (vergelijk artikel 23 lid 1 sub b Wbp).

3.1.6.2 De reikwijdte van begrippen: de kwalificatie 'Top600'

In het vorenstaande is impliciet aangenomen dat de kwalificatie 'Top600' een indirect politiegegeven en/of een bijzonder (strafrechtelijk) persoonsgegeven, zoals bedoeld in artikel 16 Wbp, is. Daarom geldt dat het gegeven ofwel niet mag worden doorverstrekt aan personen of instellingen die geen deel uitmaken van het samenwerkingsverband vanwege de geheimhoudingsplicht op grond van

artikel 7 lid 2 Wpg, ofwel omdat daarvoor geen grondslag aanwezig is in de Wbp. Vanuit de Top600 is voor deze interpretatie gekozen om de privacy van de betrokkenen zo veel als mogelijk te waarborgen.

Toch is ook een minder strikte interpretatie van het begrip juridisch verdedigbaar. Betoogd zou kunnen worden dat de kwalificatie 'Top600' geen politiegegeven is omdat deze kwalificatie niet door de politie, maar door het samenwerkingsverband aan de lijst wordt gegeven. Dat zou betekenen dat de geheimhoudingsplicht van artikel 7 lid 2 Wpg überhaupt niet van toepassing is. Daarnaast kan worden betoogd dat deze kwalificatie niet kan worden aangemerkt als een (indirect) 'strafrechtelijk persoonsgegeven', zoals bedoeld in artikel 16 Wbp. Daarvoor kunnen (a contrario) aanknopingspunten worden gevonden in de memorie van toelichting bij artikel 16 Wbp. In de memorie van toelichting wordt een onderscheid gemaakt tussen directe bijzondere persoonsgegevens enerzijds en indirecte bijzondere persoonsgegevens anderzijds. Dit onderscheid wordt als volgt toegelicht:

> 'Conform het huidige artikel 1 BGG wordt in artikel 16 gesproken over persoonsgegevens "betreffende" een aantal met name genoemde categorieën. Hiermee wordt beoogd aan te sluiten bij het thans geldende recht. Zoals de Registratiekamer terecht in zijn advies opmerkt, wordt daarbij uitgegaan van een onderscheid tussen "direct" en "indirect" gevoelige gegevens. Afgezien van gegevens die als zodanig betrekking hebben op een gevoelig kenmerk – aangeduid als "direct" gevoelige gegevens – worden tot de gevoelige gegevens ook gerekend de gegevens die weliswaar als zodanig daarop geen betrekking hebben, maar waaruit wel de aanwezigheid van een gevoelig kenmerk rechtstreeks kan worden afgeleid. Een eerder genoemd voorbeeld van het laatste is de administratie van een kerkgenootschap waarin alle namen en adressen van de leden zijn opgenomen. Weliswaar hebben deze namen en adressen op zichzelf beschouwd geen betrekking op een gevoelig kenmerk, doch uit de opneming van deze gegevens in de administratie van het kerkgenootschap vloeit dwingend voort dat het gaat om gegevens betreffende de godsdienstige overtuiging van betrokkenen. Noodzakelijk is wel dat er een rechtstreeks verband is. Gegevens die hooguit een indicatie geven dat het om een gevoelig kenmerk zou kunnen gaan, vallen – zoals de Registratiekamer terecht stelt – buiten de reikwijdte van de bijzondere regeling voor gevoelige gegevens. Voor een nadere uiteenzetting zij verwezen naar de nota van toelichting van het BGG.'[14]

Dat uit de ledenadministratie van een kerkgenootschap de godsdienst dan wel de levensovertuiging van de leden blijkt en dat dit gegeven daarom een bijzonder persoonsgegeven is, mag niet verbazen. Als dergelijke indirecte gegevens niet als bijzondere persoonsgegevens zouden worden aangemerkt, zou immers de daarvoor geldende bescherming worden uitgehold. Maar daarmee is nog niet gezegd dat de kwalificatie 'Top600' eveneens een indirect strafrechtelijk persoonsgegeven is. Die kwalificatie zegt natuurlijk dat sprake is van een strafrechtelijk verleden – maar meer dan dat ook niet. Het zegt bijvoorbeeld niets over de precieze aard van de afzonderlijke strafbare feiten of over de vraag

14 *Kamerstukken II* 1997/98, 25892, 3, p. 101.

wanneer die strafbare feiten zijn gepleegd en hoe vaak. Dit in tegenstelling tot de eerdergenoemde ledenadministratie van kerk x of y, waaruit niet alleen kan worden afgeleid dat sprake is van een godsdienstige overtuiging, maar ook wélke godsdienstige overtuiging.

Verdedigbaar is dan ook de stelling dat de kwalificatie 'Top 600' te onbepaald is om als (indirect) strafrechtelijk geven te worden beschouwd. Bovendien geldt – hoewel strikt genomen geen juridisch argument – dat dit gegeven door de Top600 alleen wordt gedeeld in het belang van de betrokkene, bijvoorbeeld om in aanmerking te komen voor stage of een onderkomen. In die zin kan men zich afvragen of de benadering bij de Top600 op dit punt niet roomser is dan strikt noodzakelijk.

4 Intimidatie in de woonomgeving: de Treiteraanpak

4.1 De totstandkoming van de Treiteraanpak

De afgelopen jaren hebben zich in Amsterdam – en elders in het land – meer dan eens gevallen van ernstige intimidatie en treiteren in de woonomgeving voorgedaan. De intimidatie wordt daarbij vaak gepleegd door buren of buurtgenoten van het slachtoffer. Het slachtoffer kan zich daarom moeilijk aan het treitergedrag onttrekken en voelt zich niet meer veilig in zijn woonomgeving. Het treiteren bestaat vaak uit een combinatie van overlast en strafbare feiten als bedreiging, belediging en vernieling. Het is lastig gebleken om dit gedrag (alleen) via het strafrecht te bestrijden. Vaak is het bewijs moeilijk rond te krijgen – als het slachtoffer al bereid is aangifte te doen. Tot op heden trok het slachtoffer daarom vaak aan het kortste eind en verhuisde hij naar een andere buurt. Daarop volgde vervolgens – terecht – een golf van publieke verontwaardiging.

Om een einde aan deze situatie te maken is in Amsterdam in 2013 met de Treiteraanpak aangevangen. Daarbij geldt de werkwijze dat wanneer een buurtregisseur of een woningcorporatie er niet in slaagt om zelfstandig ernstige overlast op te lossen, hij of zij de casus voor de Treiteraanpak kan aanmelden. De stadsdeelregisseur bepaalt dan vervolgens aan de hand van enkele cumulatieve criteria of de casus zich ook daadwerkelijk voor deze aanpak leent. Het gaat er dan om of sprake is van herhaaldelijk wangedrag, dat is gericht tegen specifieke personen of huishoudens, dat zich afspeelt in de directe woon- en/of werkomgeving van het slachtoffer, waarbij de vermoedelijke veroorzaker een directe omwonende of persoon uit de buurt is en waarbij het slachtofferschap onbetwist is.

Indien dit het geval is, krijgt de treiteraar een zogeheten ‘gele kaart’ en worden interventies gepleegd om het treiteren te beëindigen. Voor de interventies wordt optimaal gebruikgemaakt van (een combinatie van) strafrechtelijke, bestuursrechtelijke en civielrechtelijke instrumenten. Daarbij kan worden gedacht aan het opleggen van boetes, dwangsommen, cameratoezicht enzovoort. Wanneer deze interventies niet tot succes leiden, volgt een zogeheten ‘rode kaart’. Dit betekent dat de treiteraar gedwongen wordt te verhuizen. Daartoe kan bijvoorbeeld de woningbouwstichting in een kort geding de ontbinding van de huurovereenkomst vorderen. Want in het kader van de Treiteraanpak geldt dat áls er uiteindelijk iemand moet verhuizen, dit de treiteraar moet zijn – en niet het slachtoffer. Het slachtoffer krijgt in het kader van de Treiteraanpak waar nodig hulpverlening en ondersteuning aangeboden.

4.2 Convenant Treiteraanpak

Bij de Treiteraanpak zijn achttien partijen betrokken, die gezamenlijk als verantwoordelijke zijn aangemerkt in de zin van artikel 1 aanhef en onder d Wbp. Partij zijn bijvoorbeeld de burgemeester en het college van B&W van Amsterdam, de politie, het Openbaar Ministerie en enkele woningbouwcorporaties. De partijen bij de Treiteraanpak hebben zich blijkens het Convenant Treiteraanpak ten doel gesteld:[15]

> 'Een samenwerkingsverband aan te gaan met het doel om enerzijds op effectieve en integrale wijze tot een aanpak van treiteren of intimidatie in de woon- of werkomgeving te komen teneinde een adequate bijdrage te leveren aan de vermindering van treiteren of intimidatie zodat slachtoffers van intimidatie in de woon- of werkomgeving worden beschermd, treiteraars hun gedrag veranderen en stoppen met intimideren en de woon- en werkomgeving en de openbare orde en veiligheid in Amsterdam in belangrijke mate wordt verbeterd en anderzijds de privacy van de betrokkenen zoveel mogelijk te waarborgen.'

Voor het bepalen en afstemmen van de juiste interventies is informatiedeling, net als bij de Top600, van essentiële waarde. De bij de Treiteraanpak betrokken organisaties wisselen onderling binnen de kaders van de wet gegevens uit om de ernst van het geval in kaart te brengen en de juiste interventies te bepalen. Daarbij kan bijvoorbeeld van belang zijn te weten welk soort strafbaar gedrag de treiteraar vooral vertoont, de ernst daarvan, of het overlastgevende gedrag mogelijk voortkomt uit psychische problemen, enzovoort.

De Treiteraanpak creëert geen nieuwe bevoegdheden. Evenals bij de Top600 geldt dat de betrokken organisaties elk hun eigen wettelijke bevoegdheden blijven uitoefenen, maar daarbinnen wel prioriteren.

4.3 Dilemma's

Hierna zullen aan de hand van praktijkvoorbeelden enkele privacygerelateerde dilemma's worden behandeld die zich bij de Treiteraanpak voordoen.

4.3.1 De achterdeur

In het kader van de Treiteraanpak wordt, waar nodig, ook strafrechtelijk gehandhaafd. Ten behoeve van een strafzaak kan de officier van justitie het Nederlands Instituut voor Forensische Psychiatrie en Psychologie (NIFP) verzoeken onderzoek te doen naar de persoon van de verdachte (de treiteraar). Het NIFP brengt vervolgens een (gedragsdeskundig) rapport uit, waarin ook veel medische informatie is opgenomen. Het gaat dan bijvoorbeeld om diagnoses over de geestelijke gesteldheid van de verdachte.

15 www.afwc.nl/templates/afwc/images/Convenant_Treiteraanpak_2013.pdf.

De Treiteraanpak-regisseur van de verdachte is vaak bij een dergelijke zitting aanwezig. Normaliter mag de regisseur van deze medische informatie geen kennis dragen, omdat die informatie vanwege het beroepsgeheim niet binnen het samenwerkingsverband wordt gedeeld en bovendien artikel 21 Wbp verwerking daarvan in beginsel verbiedt. Tijdens de zitting wordt echter door de rechtbank, de officier en de verdachte vrijelijk uit deze medische gegevens geput – en raakt dus ook de regisseur daarvan op de hoogte.

Hoe dient de regisseur nu met deze wetenschap om te gaan? Mag hij die informatie (verder) verwerken binnen het samenwerkingsverband ten behoeve van de verdere aanpak van de treiteraar? Moet de rechtspleging worden gezien als een algemene uitzondering op de privacyregels voor het medisch beroepsgeheim? Of kan worden gesteld dat de verdachte heeft ingestemd met het openbaar maken van de gegevens door aan het onderzoek deel te nemen? Juridisch valt voor beide argumenten iets te zeggen. Maar zelfs in het geval deze vragen bevestigend dienen te worden beantwoord, blijft het gevoel over dat de regisseur via de achterdeur aan informatie is gekomen waar hij anders niet over had mogen beschikken. Want hoe vrijwillig is deelname aan een dergelijk onderzoek eigenlijk? En wil de verdachte daarmee niet enkel en alleen zijn belang tijdens de strafzaak dienen?

Regisseurs worstelen met deze vragen. Sommigen delen deze informatie zekerheidshalve niet, terwijl anderen vinden dat verdere verwerking wel is toegestaan. Hoewel laatstgenoemd standpunt juridisch dus (om voornoemde argumenten) verdedigbaar is, rijst de vraagt of de wet op dit punt niet meer helderheid zou moeten verschaffen.

4.3.2 *De dubbele pet*

Een ander dilemma dat bij de Treiteraanpak – maar ook bij andere samenwerkingsverbanden – aan de orde is, heeft betrekking op de kwestie van de 'dubbele pet'. In het kader van de Treiteraanpak worden individuele casus besproken in een zogeheten 'uitvoeringsoverleg', waarbij de bij de aanpak betrokken partijen om tafel zitten. Tijdens dit overleg worden gegevens over betrokken individuen gedeeld. Daardoor ontstaan in wezen twee informatiestromen: de stroom van informatie vanuit de betrokken organisaties naar de Treiteraanpak enerzijds, en de stroom van informatie die de betrokken partijen vanuit het uitvoeringsoverleg vervolgens weer kunnen meenemen naar de eigen organisaties anderzijds. Concreet betekent dit bijvoorbeeld dat een politiemedewerker in het overleg politiegegevens kan inbrengen, maar ook dat de politie aldaar (in het kader van de Treiteraanpak) verkregen informatie mee terugneemt naar de politie.

De eerste informatiestroom wordt in beginsel gedekt door het besluit van de korpschef op grond van artikel 20 Wpg.[16] Dit is slechts anders als niet wordt voldaan aan de voorwaarden van het besluit van de korpschef dan wel de vereisten

16 In artikel 20 Wpg is bepaald dat op basis van een besluit van de korpschef structureel politiegegevens aan een samenwerkingsverband kunnen worden verstrekt.

van de Wbp, zoals het noodzakelijkheidsvereiste. De tweede informatiestroom is juridisch – en praktisch – evenwel lastiger te duiden. De tweede informatiestroom kan immers leiden tot de situatie dat de politiemedewerker de verkregen informatie nie alleen inzet ten behoeve van zijn taken in het kader van de Treiteraanpak, maar ook in het kader van de uitvoering van de reguliere politietaak, zoals opsporing. De vraag is dus in essentie of de politiemedewerker de informatie die hij tot zich neemt in het kader van de Treiteraanpak ook mag gebruiken in zijn rol als politieagent. Mag hij die informatie bijvoorbeeld delen als bewijs in een eventuele strafzaak? Of mag hij eventueel zelf melding maken van een strafbaar feit of een aandachtsvestiging noteren naar aanleiding van hetgeen hij tijdens het overleg heeft vernomen? Gebruikt hij daarmee de gegevens niet voor een ander doel – het uitvoeren van de Treiteraanpak – dan waarvoor hij ze heeft gekregen? En los van de juridische (on)mogelijkheden: is het überhaupt te voorkomen dat de politiemedewerker de informatie in zijn beide hoedanigheden inzet? Het is immers de vraag of het menselijkerwijze wel mogelijk is (de herkomst van) informatie binnen hetzelfde brein te scheiden – zeker waar het gaat om dagelijks politiewerk, waarbij soms snel beslissingen moeten worden genomen.

Het lijkt er op grond van een uitspraak van (de strafkamer van) het gerechtshof Arnhem-Leeuwarden (hierna: het hof) op dat de politiemedewerker niet behoeft te worden opgezadeld met deze zware opgave.[17] In bedoelde uitspraak stond een man terecht die werd verdacht van, kort gezegd, het bezit van een grote hoeveelheid softdrugs en witwassen. De politie had in het kader van de opsporing informatie over de verdachte bij de Belastingdienst opgevraagd. De politie had deze gegevens opgevraagd op grond van het Regionaal Convenant Geïntegreerde Decentrale Aanpak Georganiseerde Misdaad regio Midden-Nederland. Bij dit convenant (waarover hierna meer) was zowel de politie als de Belastingdienst – naast andere overheidsinstanties – partij. De verdachte voerde aan dat de politie het bewijs over witwassen onrechtmatig had verkregen, omdat ze hiervoor niet het convenant had mogen gebruiken, maar de bevoegdheid van artikel 126nd Sv had dienen aan te wenden. Anders dan de rechtbank, oordeelde het hof dat de politie deze informatie wel op grond van het convenant mocht opvragen – simpelweg omdat de tekst van het convenant zelf dit niet uitsloot. Dat de politie via de officier van justitie deze gegevens ook op grond van artikel 126nd Sv – waarvoor zwaardere eisen gelden – had kunnen vorderen, maakte dit volgens het hof niet anders. Uit de uitspraak lijkt te volgen dat in het kader van de verkrijging van gegevens ten behoeve van de vervulling van reguliere politietaken ook gegevens mogen worden gebruikt die in het kader van een samenwerkingsverband zijn of kunnen worden verkregen. De politie behoeft daarvoor, met andere woorden, niet per se zelfstandige bevoegdheden in te zetten.

17 Gerechtshof Arnhem-Leeuwarden 8 november 2013, ECLI:NL:GHARL:2013:8478.

5 Regionale Informatie- en Expertise Centra (RIEC)

5.1 Totstandkoming RIEC

Vanuit de georganiseerde criminaliteit wordt steeds vaker gebruikgemaakt van verschillende diensten en producten van de overheid om criminele activiteiten te ondersteunen. Criminelen vragen in dit verband bijvoorbeeld vergunningen en subsidies aan en dingen mee naar overheidsopdrachten. Wanneer overheidsorganen elkaar niet informeren, ontstaat daarmee het gevaar dat zij deze illegale praktijken faciliteren. Zo kan het zijn dat een slecht geïnformeerde gemeente vergunningen verleent aan een bedrijf waarvan de politie weet dat het als dekmantel dient om criminele gelden wit te wassen. Dit is vanuit het oogpunt van de integriteit en de geloofwaardigheid van de overheid niet aanvaardbaar. Het RIEC is opgericht om de georganiseerde criminaliteit te bestrijden door te bevorderen dat afzonderlijke overheidsorganen door een betere informatiedeling optimaal kunnen samenwerken. In Nederland zijn op dit moment tien (RIEC's) actief. Zij zijn onderverdeeld in tien regio's, die congrueren met de politieregio's en de indeling van de gerechtelijke kaart. Het Landelijk Informatie- en Expertise Centrum (LIEC) verleent in dit verband ondersteuning en is verantwoordelijk voor de verbinding en coördinatie tussen de verschillende RIEC's.

5.2 Convenant RIEC

Binnen het RIEC wordt, als gezegd, door de betrokken partijen informatie gedeeld. Daarmee wordt gezorgd voor een completer beeld van de omvang, werkwijze en 'leden' van criminele organisaties. Op deze wijze wordt een optimale, integrale, bestuursrechtelijke, strafrechtelijke en fiscale aanpak van de georganiseerde criminaliteit gefaciliteerd.

Ten behoeve van de uitwisseling van persoonsgegevens is landelijk een convenant opgesteld, waarin de minister van Veiligheid en Justitie een aantal landelijke thema's heeft benoemd. Het gaat om de thema's mensenhandel, woonfraude, misbruik binnen de vastgoedsector en witwassen.[18] Daarnaast is in het convenant bepaald dat op regionaal niveau zogeheten 'handhavingsknelpunten' kunnen worden benoemd. Handhavingsknelpunten zijn aangewezen personen of een groep personen over wie of een gebied of branche waarover verschillende

18 www.riec.nl/doc/oostbrabant/Convenant%20Bestuurlijke%20en%20Geintegreerde%20Aanpak%20Georganiseerde%20Criminaliteit.pdf.

overheden of bestuursorganen signalen bereiken dat de vigerende regelgeving structureel niet wordt nageleefd. De handhavingsknelpunten verschillen per (regionale) RIEC en kunnen door de RIEC's zelf benoemd worden. De landelijke thema's en de regionale handhavingsknelpunten kunnen worden beschouwd als het (algemene) doel van de gegevensverwerking, zoals bedoeld in artikel 7 Wbp.

Bij de RIEC's zijn – in tegenstelling tot de Top600 en Treiteraanpak – uitsluitend overheidsorganisaties partij. Het gaat om gemeenten, provincies, Belastingdienst, douane, Fiscale inlichtingen en opsporingsdienst, Immigratie- en Naturalisatiedienst, Inspectie Sociale Zaken en Werkgelegenheid, Koninklijke Marechaussee, Openbaar Ministerie en de politie.

De reden om alleen overheidsinstanties toe te laten is gelegen in de gevoeligheid van de materie, ter waarborging van de betrouwbaarheid van de informatie en – niet in de laatste plaats – om de Belastingdienst aan tafel te kunnen krijgen. De Belastingdienst kan alleen deelnemen aan samenwerkingsverbanden waarbij uitsluitend overheidsorganisaties partij zijn.[19] Bij de Top600 en de Treiteraanpak – waarbij ook niet-overheidspartijen zijn betrokken – is de Belastingdienst daarom geen partij.

5.3 De Belastingdienst

De positie van de Belastingdienst binnen het RIEC verdient vanuit het oogpunt van de privacy zelfstandige bespreking. De reden is dat de regeling voor de verstrekking van belastinggegevens in de Algemene wet inzake rijksbelastingen (AWR) van een andere aard is dan die geldt voor bijvoorbeeld politiegegevens in de Wpg. In het geval van de politiegegevens is eerder toegelicht dat in de Wpg bijzondere verwerkingsgrondslagen zijn genoemd voor verstrekkingen aan derden (partijen buiten de politie). Voorts geldt een geheimhoudingsplicht ten aanzien van de verstrekte politiegegevens. Ook de Wbp kent een bijzondere regeling voor de verwerking van strafrechtelijke gegevens. Beide wetten bepalen onder welke voorwaarden aan wie gegevens mogen worden verstrekt. Zoals eerder aangegeven, rijst daardoor de vraag hoe de Wpg en de Wbp zich op dit punt tot elkaar verhouden. De geheimhoudingsplicht voor belastinggegevens leidt evenwel tot andere vragen – om nog maar een variatie op het thema complexiteit in te brengen.

De Belastingdienst kan aan het RIEC alleen gegevens verstrekken wanneer is voldaan aan artikel 67 AWR. Artikel 67 lid 1 AWR bepaalt dat het eenieder verboden is om hetgeen hem uit of in verband met enige werkzaamheid bij de uitvoering van de belastingwet over de persoon of zaken van een ander blijkt of wordt meegedeeld, verder bekend te maken dan noodzakelijk is voor de uitvoering van de belastingwet of voor de invordering van enige rijksbelasting als bedoeld in de Invorderingswet 1990. Artikel 67 lid 2 AWR bevat een aantal uitzonderingen op deze geheimhoudingsplicht. Blijkens dit artikel geldt de geheimhoudingsplicht niet indien bij regeling van de minister is bepaald dat

19 Dit vloeit voort uit artikel 67 AWR jo. artikel 43c Uitvoeringsregeling Algemene wet inzake rijksbelastingen 1994.

bekendmaking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak van een bestuursorgaan.

Een dergelijke regeling is bijvoorbeeld de Uitvoeringsregeling Algemene wet inzake rijksbelastingen 1994 (hierna: Uitvoeringsregeling). Artikel 43c Uitvoeringsregeling bepaalt dat eerdergenoemde geheimhoudingsplicht onder een aantal strikt omschreven voorwaarden niet geldt. Het gaat er daarbij om dat een bepaalde categorie van belastinggegevens mag worden verstrekt aan een bepaalde categorie bestuursorganen voor een beperkt aantal publiekrechtelijke taken. Artikel 43c lid 1onder m Uitvoeringsregeling bepaalt vervolgens dat de geheimhoudingsplicht niet geldt voor verstrekking aan gemeenten, provincies, de politie, de officier van justitie, de minister van Sociale Zaken en Werkgelegenheid, de Koninklijke Marechaussee, de Inspectie Sociale Zaken en Werkgelegenheid, de Sociale verzekeringsbank of het Uitvoeringsinstituut werknemersverzekeringen, (slechts) voor zover de gegevens nodig zijn om de samenwerking in het kader van de integrale toepassing en handhaving van overheidsregelingen effectief en efficiënt te laten verlopen en (slechts) voor zover daartoe een convenant met de bestuursorganen is gesloten. De verstrekking van persoonsgegevens aan het RIEC door de Belastingdienst vindt op deze grond plaats.

Artikel 43c lid 1onder m Uitvoeringsregeling heft derhalve voor de Belastingdienst ten aanzien van het RIEC de geheimhoudingsplicht van artikel 67 AWR op. Daarmee is het verhaal evenwel niet uit: de opheffing van de geheimhoudingsplicht betekent immers niet dat ongebreideld informatie aan het RIEC mag worden verstrekt. De vraag rijst dan ook aan welk regime de Belastingdienst gebonden is voor de verstrekking van de gegevens nadat hij de horde van de geheimhouding heeft genomen. In tegenstelling tot bijvoorbeeld de Wpg en de WJG – die zelf voorwaarden voor verstrekkingen bevatten – geldt dat de Belastingdienst op dat moment dient te toetsen aan de eisen van de Wbp. Wanneer de belastinggegevens vervolgens binnen het samenwerkingsverband RIEC zijn gevloeid, is enkel de Wbp van toepassing. De onduidelijkheid die zich voordoet over de reikwijdte van de geheimhoudingsverplichting uit de Wpg, doet zich derhalve bij de geheimhoudingsplicht van de AWR niet voor.

6 Open begrippen: open eind?

6.1 Open begrippen

De wetgever heeft er bewust voor gekozen om in de Wbp met open begrippen te werken. De gedachte daarbij is dat open begrippen niet (snel) verouderen – en dat is gezien de snelheid van technologische ontwikkelingen een relevante afweging. Ook zijn dergelijke begrippen van belang om maatwerk te kunnen leveren en rekening te kunnen houden met de omstandigheden van het geval. Het neveneffect is evenwel dat het gebruik van open begrippen de praktijk vaak in de weg zit en tot patstellingen kan leiden.

6.2 Zelfbeperking

Het gebruik van open begrippen doet zich bijvoorbeeld voor bij de doelomschrijving van de verwerking van persoonsgegevens. Op grond van artikel 7 Wbp kunnen persoonsgegevens alleen worden verzameld in het kader van een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. De wet biedt derhalve geen inhoudelijke maatstaven om te bepalen wanneer een doel welbepaald en gerechtvaardigd is. Het is aan de verantwoordelijke om aan deze begrippen inhoud te geven.

Dit gegeven leidde enige tijd geleden tot een patstelling tussen de gemeente Amsterdam en het CJIB. De gemeente Amsterdam heeft de afgelopen jaren stevig ingezet op het beëindigen van de misstanden in de taxibranche. De gemeente wenste niet alleen de klantvriendelijkheid te verbeteren, maar ook de verkeersveiligheid te bevorderen en andere wanordelijkheden te voorkomen. De gemeente wilde ten behoeve van dit doel gebruikmaken van persoonsgegevens waarover het CJIB de beschikking had, zoals verkeersovertredingen en boetes.

Het CJIB weigerde evenwel deze gegevens aan de gemeente te verstrekken. Het CJIB stelde dat het de bedoelde persoonsgegevens (slechts) had verzameld ten behoeve van de administratieve afhandeling van verkeersboetes. Dat (strikte) doel was volgens het CJIB niet verenigbaar met het doel waarvoor de gemeente deze gegevens wenste verder te verwerken, zijnde het op orde brengen van de taxibranche in Amsterdam door de klantvriendelijkheid, de verkeersveiligheid enzovoort te bevorderen. Volgens het CJIB stond derhalve artikel 9 Wbp (het verbod op verdere verwerking bij onverenigbare doelen) aan de verstrekking van de verlangde gegevens in de weg.

De vraag is evenwel of de doelen waarvoor het CJIB en de gemeente deze gegevens (willen) verwerken daadwerkelijk onverenigbaar zijn. Strikt geredeneerd, valt voor het standpunt van het CJIB wel iets te zeggen. De twee doelomschrijvingen komen op het eerste oog ook niet overeen. Het min of meer standaard verwerken van gegevens in het kader van de oplegging van verkeersboetes is immers ook iets anders dan het gebruiken van die gegevens om bijvoorbeeld notoire overtreders (al dan niet tijdelijk) te kunnen uitsluiten van het beroep van taxichauffeur.

Toch zou kunnen worden gesteld dat deze twee instanties als onderdeel van de overheid een algemeen gemeenschappelijk (ruimer) doel hebben om de verkeersregels te handhaven dan wel de (verwachte) overtreding daarvan te voorkomen. Daarnaast wordt de formele aard van deze patstelling onderstreept wanneer men bedenkt dat de gemeente bijvoorbeeld via de eerdergenoemde samenwerkingsverbanden mogelijkheden heeft om informatie te krijgen over het strafrechtelijke verleden van personen. Het is in dat licht niet goed te beredeneren waarom het CJIB deze informatie in dit geval niet met de gemeente zou mogen delen.

De vraag rijst ook of het in dit soort gevallen niet mogelijk zou moeten zijn advies te vragen aan een instantie zoals het College bescherming persoonsgegevens (CBP). In de praktijk bestaat, zoals uit vorenstaand voorbeeld ook blijkt, soms grote behoefte aan een opinie van een gezaghebbend, deskundig en onpartijdig orgaan om impasses te doorbreken. Het CBP lijkt daarvoor evenwel zelf weinig ruimte te zien.

6.3 Buitenkantinformatie

Open begrippen worden niet alleen in de wet gebruikt. In de praktijk worden wettelijke bepalingen vaak nader uitgewerkt in een convenant, waarbij ook weer nieuwe (buitenwettelijke) open begrippen worden geïntroduceerd. Het doel is dan om een oplossing te bieden voor de dilemma's die men binnen de praktijk van samenwerkingsverbanden ervaart – doch dat doel wordt vaak maar ten dele bereikt. Dit wordt hierna toegelicht aan de hand van het gebruik van het begrip 'buitenkantinformatie' binnen samenwerkingsverbanden.

Samenwerkingsverbanden leggen in de praktijk de werkafspraken tussen de betrokken partijen vast in een convenant. In het convenant worden ook de verplichtingen uit de Wbp en eventuele andere privacywetten uitgewerkt. Zo wordt daarin bijvoorbeeld bepaald wie als de verantwoordelijke dient te worden beschouwd, wat het doel van de gegevensuitwisseling is, welke waarborgen in het kader van de proportionaliteit en de subsidiariteit worden ingebouwd, welke bewaartermijn wordt gehanteerd, wat de rechten van de betrokkenen zijn, enzovoort. Daarnaast is een convenant raadzaam omdat politie en justitie dan eerder genegen zijn tot structurele gegevensverstrekking over te gaan.

Een convenant is derhalve een uitgelezen kans om open begrippen uit de wet nadere inhoud te geven. Toch creëert een convenant vaak onduidelijkheden door op zijn beurt ook weer open begrippen te introduceren. Dit is ingegeven door de

vrees dat door het hanteren van enge definities onnodige barrières bij de informatiedeling worden opgeworpen.

Het CBP heeft dit probleem bijvoorbeeld gesignaleerd bij het verwerken van medische gegevens, waarvoor in het algemeen naast de regeling van artikel 16 jo. artikel 21 jo. artikel 23 Wbp een beroepsgeheim geldt. Het kan bijvoorbeeld van belang zijn dat de GGD als partij bij een samenwerkingsverband informatie deelt met andere onderdelen van de gemeente, de politie, de woningbouwcorporatie of de geestelijke gezondheidszorg om verdere hulpverlening te organiseren of om de juiste bejegening van een betrokkene te bevorderen. Zo kan het zijn dat de GGD in het kader van de Top600 constateert dat een betrokkene lijdt aan schizofrenie. Het is dan raadzaam om die informatie met de Top600-regisseur te delen, omdat die bijvoorbeeld de politie kan instrueren de betrokkene niet op regelmatige basis aan te spreken. Schizofrenie kan immers gepaard gaan met achtervolgingswanen, die door proactief politieoptreden zouden kunnen worden gevoed. Dit zou tot gevaarlijke situaties kunnen leiden. Maar in een minder dramatisch voorbeeld kan dergelijke informatie ook van belang zijn voor de DWI bij het vinden van passend werk voor de betrokkene of in het kader van de bestrijding van woonoverlast door een woningbouwcorporatie. Toch mogen dergelijke diagnoses in beginsel niet worden gedeeld.

Het CBP heeft geprobeerd om de praktijk in dezen tegemoet te komen door de term 'buitenkantinformatie' te introduceren.[20] Een precieze definitie is er niet, maar het komt neer op het min of meer abstraheren van medische informatie. Dat betekent in voornoemd geval dat de GGD niet mededeelt dat sprake is van schizofrenie, maar dat sprake is van 'onvoorspelbaar agressief gedrag'. Het betekent ook dat niet wordt gesproken over 'licht verstandelijk beperkt' (LVB), maar over 'traagheid van begrip'. Het gaat derhalve om het op een abstract niveau beschrijven van symptomen of karakteristieken van een aandoening, zonder de medische aanduiding van die aandoening te gebruiken. Volgens het CBP is het delen van buitenkantinformatie alleen geoorloofd in uitzonderingsituaties en indien dit in het belang van de betrokkene is. Het is steeds aan de beroepsbeoefenaar om te bepalen of van die situatie sprake is.

Hoewel de inzet van het CBP te prijzen is, brengt de introductie van een open begrip als 'buitenkantinformatie' niet de gewenste verlichting. Medische beroepsbeoefenaren tonen zich nog vaak terughoudend in het verstrekken van informatie. Zij vinden dat zij onvoldoende vaste grond onder de voeten hebben met dit begrip, terwijl het maken van een verkeerde afweging vergaande gevolgen kan hebben. Bovendien laat de voorwaarde dat sprake moet zijn van een 'uitzonderingssituatie' zien dat het niet de bedoeling is buitenkantinformatie op structurele wijze te verstrekken, terwijl dit wel bij het karakter van een samenwerkingsverband past. Daar kan tegenover worden gesteld dat een samenwerkingsverband ook alleen in bijzondere gevallen wordt opgericht.

20 Informatieblad CBP, nummer 31A, februari 2012.

7 Conclusie

De overheid is belast met het bevorderen van de veiligheid van haar burgers. Met het bestrijden van criminaliteit en overlast dient de overheid dan ook het algemeen belang.

Uit dit preadvies is evenwel gebleken dat privacywetgeving aan het dienen van dit algemeen belang soms (onbedoeld) in de weg kan staan.

De reden is onder meer gelegen in de fragmentatie van de overheid. Binnen een en dezelfde overheidsorganisatie kunnen verschillende onderdelen belast zijn met de uitvoering van verschillende wetten. Zo geldt bijvoorbeeld binnen de gemeente Amsterdam dat de DWI de Wet werk en bijstand uitvoert, dat de Dienst Wonen, Zorg en Samenleven de Wet maatschappelijke ondersteuning uitvoert, dat de Dienst Maatschappelijke Ontwikkeling de onderwijswetgeving uitvoert, enzovoort. Deze diensten verwerken derhalve elk als verantwoordelijke gegevens voor verschillende doeleinden. Dit betekent dat zij (hoewel zij alle worden verondersteld het algemeen belang te dienen) deze gegevens – binnen een en dezelfde gemeente – niet zonder meer met elkaar mogen delen. Zij zullen immers steeds moeten toetsen of sprake is van verenigbaarheid van de doeleinden van de gegevensverwerking. Dit is niet altijd het geval. Dit is niet per se omdat de wetgever het oogmerk heeft gehad het delen van de informatie uit te sluiten, maar omdat de wet de toelaatbaarheid van uitwisseling van gegevens verbindt aan de doelomschrijving – en die zal soms onvermijdelijk onverenigbaar zijn met een andere doelomschrijving. Het dienen van het algemeen belang wordt hierdoor, hoewel niet de bedoeling, soms sterk bemoeilijkt. Het dienen van het algemeen belang wordt zelfs een zwaardere opgave wanneer verschillende soorten overheidsorganisaties gegevens met elkaar willen delen. Wanneer de gemeente samen wenst te werken met bijvoorbeeld de politie en/of het Openbaar Ministerie en/of de Belastingdienst, is het hebben van een verenigbaar doel niet voldoende. Er dient steeds in een toepasselijke bijzondere wet een grondslag voor het verstrekken van gegevens aanwezig te zijn.

Het formeren van samenwerkingsverbanden is een mogelijkheid om dit probleem (enigszins) te ondervangen en het algemeen belang adequaat te dienen. Daarbij geldt immers voor alle betrokken organisaties één doelomschrijving. Bovendien gelden voor samenwerkingsverbanden bijzondere wettelijke voorzieningen om het delen van informatie te vergemakkelijken. Artikel 20 Wpg en artikel 22 Wbp zijn er bijvoorbeeld in essentie op gericht het strenge wettelijke regime voor het uitwisselen van strafrechtelijke gegevens in het geval van samenwerkingsverbanden te vereenvoudigen. Niettemin is uit dit preadvies gebleken dat de wetgever in dat streven, ondanks de goede bedoelingen, niet volledig is geslaagd. De organisaties bij een samenwerkingsverband blijven immers gebonden aan de

bijzondere privacywetgeving en de eigen privacyreglementen bij het verstrekken van gegevens aan het samenwerkingsverband. Bovendien is onduidelijk welke wet van toepassing is wanneer de gegevens eenmaal aan het samenwerkingsverband zijn verstrekt. De wetgever heeft op dit punt geen duidelijkheid verschaft en heeft daarmee een belangrijke kans laten liggen. Samenwerkingsverbanden worden immers juist geformeerd om het algemeen belang zo goed mogelijk te kunnen dienen.

Voorts is uit dit preadvies gebleken dat het gebruik van open begrippen in de privacywetgeving – hoewel onvermijdelijk om maatwerk mogelijk te maken – de praktijk niet altijd dient. Zij leiden soms tot grote voorzichtigheid, omdat overheidsorganisaties vrezen een ongeoorloofde inbreuk op de privacy te maken. Enerzijds kan die houding als zorgvuldig worden beschouwd. Anderzijds kan dit ertoe leiden dat overheidsorganen hun bevoegdheden niet adequaat kunnen uitvoeren – terwijl de burger dit wel verwacht – omdat zij niet over de daarvoor vereiste informatie beschikken. Bij dergelijke patstellingen wordt in de praktijk het gemis gevoeld van een deskundig en onpartijdig orgaan, dat kan worden geraadpleegd dan wel een doorslaggevend oordeel kan geven. Het bestaan van een dergelijk orgaan kan ertoe bijdragen dat de privacywetgeving voor de overheid niet gaat fungeren als een oneindig labyrint, waaruit uiteindelijk niemand meer weet te ontsnappen.

Zakelijk verslag van de vergadering van de Jonge VAR van 12 december 2014

De Jonge VAR vond dit jaar op 12 december 2014 plaats op het advocatenkantoor van Pels Rijcken & Droogleever Fortuijn. De vergadering werd voorgezeten door prof. mr. Ben Schueler, voorzitter van de VAR. De preadviseurs hebben tijdens de vergadering hun preadviezen gepresenteerd en de vragen vanuit het publiek over hun presentaties beantwoord. Aan het einde van de middag heeft Ben Schueler de discussie naar aanleiding van de preadviezen geleid. De middag werd feestelijk afgesloten met een borrel. Dit verslag beschrijft de vragen die door het publiek aan de preadviseurs zijn gesteld en de discussies die naar aanleiding van de preadviezen zijn gevoerd.

Grensoverschrijdende gegevensuitwisseling en privacy

Preadvies van Marte van Graafeiland en Nina Bontje

Jeroen de Jong (ministerie van Veiligheid en Justitie, directie Wetgeving) betuigt in de eerste plaats zijn respect aan alle preadviseurs voor het nemen van de moeite om het moeilijke terrein van privacy binnen de grenzen van het bestuursrecht te trekken. Hij vraagt aan de beide preadviseurs, Marte van Graafeiland en Nina Bontje, of zij de rechter vanuit hun praktische beroepsoefening hulp zouden kunnen bieden bij het toepassen van de bepalingen in de Algemene Verordening Gegevensbescherming (AVG). De Jong wijst erop dat mogelijk meer wetgeving nodig zal zijn om de AVG uit te kunnen voeren. Zo ontbreekt een equivalent van artikel 21 lid 2 AVG in de Privacyrichtlijn en de Wet bescherming persoonsgegevens (Wbp), waarin staat dat lidstaten wettelijke maatregelen kunnen treffen om de reikwijdte van bepaalde rechten en plichten te beperken. De Jong werpt vervolgens de vraag op of artikel 21 lid 2 AVG dwingt tot het aannemen van meer wetgeving en het afstappen van artikel 43 Wbp, waarin wordt gesproken van zowel beperkingen als uitzonderingen. **Nina Bontje** geeft aan dat zij en Van Graafeiland ook hebben nagedacht over deze vragen. Als er een specifieke bepaling op nationaal niveau zou moeten komen om bijvoorbeeld de informatieplicht te beperken, dan is het heel lastig om al van tevoren te bepalen hoe een afweging met betrekking tot de beperking moet plaatsvinden. Hoe een afweging moet worden gemaakt, is namelijk gevalsafhankelijk. Bovendien laten de huidige regeling in de Wbp en ook de andere bepalingen in de AVG veel ruimte voor de verantwoordelijke instanties om afwegingen te maken. Het zou niet in lijn zijn met deze beoordelingsvrijheid liggen om heel specifiek aan te geven hoe een afweging moet worden gemaakt. **Marte van Graafeiland** vult aan dat zij en Bontje de verantwoordelijke instantie het beste in staat achten om van geval tot geval te beoordelen hoe een afweging moet plaatsvinden. **Jeroen de Jong** stelt in reactie daarop voor dat ook per clusters van

wetgeving, bijvoorbeeld socialezekerheidswetgeving, een modelbepaling zou kunnen worden ontwikkeld waarin voor de uitvoeringsinstanties wordt weergegeven welke afwegingen zij moeten maken. Zo zou in een dergelijke modelbepaling kunnen worden aangegeven van welke rechten en verplichtingen een verantwoordelijke instantie zou kunnen afwijken. **Marte van Graafeiland** geeft aan dat een modelbepaling weliswaar indenkbaar is, maar dat het bestaan daarvan ook tot gevolg zal hebben dat in elke wet waarin de verwerking van persoonsgegevens aan de orde is, een dergelijke bepaling moet worden opgenomen. Daarnaast merkt Van Graafeiland op dat zij en Bontje geen aanwijzingen hebben gevonden dat er bezwaren bestaan tegen de eigen afweging die de verantwoordelijke instantie op dit moment al onder de Wbp moet maken. Hieruit volgt dat er ook geen aanleiding bestaat om op dit punt veranderingen door te voeren.

Fokke Jan van der Tol vraagt zich af of er voldoende garanties bestaan om gegevensuitwisseling tussen landen te waarborgen. Gegevensuitwisseling vindt pas plaats als een passend beschermingsniveau kan worden geboden. Daarnaast kan er een zwaarwegend belang bestaan om gegevens uit te wisselen, bijvoorbeeld op het terrein van fiscaal recht en mededingingsrecht. Van der Tol vraagt de preadviseurs of er niet meer waarborgen zouden moeten komen om veilige gegevensuitwisseling in het kader van een zwaarwegend belang te garanderen. Hij wijst daarbij op de situatie dat gegevens worden uitgewisseld met landen die op basis van formele wetgeving weliswaar garanties bieden, maar die in de praktijk corrupt kunnen zijn en gegevensbescherming onvoldoende waarborgen. Hierdoor kunnen uitgewisselde gegevens alsnog openbaar worden. **Marte van Graafeiland** antwoordt dat als Nederlandse autoriteiten al op voorhand weten dat gegevens worden verstrekt aan derde landen die niet op de juiste wijze met die gegevens zullen omgaan, bijvoorbeeld omdat ze niet geheim worden gehouden of omdat ze voor een ander doel worden gebruikt, die Nederlandse autoriteiten zich zouden moeten afvragen of ze de gegevens wel kunnen verstrekken. Volgens Van Graafeiland staat voorop dat Nederlandse autoriteiten zelf verantwoordelijk zijn voor de afweging of sprake is van een passend beschermingsniveau. Mocht de buitenlandse autoriteit de ontvangen persoonsgegevens ondanks de gemaakte inschatting vervolgens toch verkeerd gebruiken, dan kan er een vraag van een andere orde opkomen. Namelijk wat het gevolg van dat verkeerde gebruik is. Die vraag zou in een rechterlijke procedure beoordeeld kunnen worden. **Fokke Jan van der Tol** wijst op de discussies die plaatsvinden in het vreemdelingenrecht over de vraag of een land van herkomst voldoende veilig is. Hij vraagt zich af of op dit terrein zich niet ook de situatie zou kunnen voordoen dat gegevens worden uitgewisseld met een land, terwijl de bescherming van die gegevens niet voldoende kan worden gewaarborgd. Volgens **Marte van Graafeiland** kan het voor de verantwoordelijke autoriteit heel lastig zijn om op voorhand te beoordelen of gegevensuitwisseling veilig is. Bij sommige landen ben je daar zekerder over dan bij andere landen. Maar het risico op onjuist gebruik van gegevens blijft bestaan.

Privacy en veiligheid: een oneindig labyrint?

Preadvies van Mohammed Belhaj en Sultan Gün

In het publiek is naar aanleiding van de presentatie van de preadviseurs Belhaj en Gün een vraag gesteld over het uitwisselen van informatie in samenwerkingsverbanden.

De preadviseurs hebben tijdens hun presentatie een casus toegelicht om de (on)mogelijkheden van het delen van gegevens in een samenwerkingsverband weer te geven. Uit het publiek komt de vraag of het opvragen van informatie bij een bepaalde instantie binnen een samenwerkingsverband niet in feite een fishing expedition is. Wat is de verdenking en wat is de wettelijke basis om informatie op te vragen over een bepaalde persoon? **Mohammed Belhaj** antwoordt dat de casus die hij heeft geschetst puur fictief is. De casus is een extreem voorbeeld. Als de casus zich in het echt zou voordoen, zou er heel zorgvuldig om worden gegaan met het delen en zoeken van informatie. De reden om verder te zoeken naar informatie zal grondig worden onderzocht. **Fokke Jan van der Tol** merkt op dat het onderwerp ook aan de orde is in een zaak die momenteel bij het gerechtshof dient. De juridische vraag in deze zaak is of de politie op basis van de bevoegdheden van de Belastingdienst onderzoek had mogen doen om informatie te verkrijgen ten behoeve van een strafrechtelijk dossier tegen een persoon. Deze casus maakt de mogelijke risico's zichtbaar van het vermengen van bevoegdheden. Van der Tol merkt op dat de wijze waarop de gemeente Amsterdam handelt, bij het gerechtshof of de Hoge Raad mogelijk onrechtmatig zal worden bevonden. **Sultan Gün** stelt dat dit misschien het geval is, maar wijst ook op een uitspraak van het gerechtshof Arnhem-Leeuwarden van vorig jaar, waarin werd geoordeeld dat informatie die via een instantie zoals de Belastingdienst in een samenwerkingsverband terechtkomt, door de politie gebruikt mag worden zonder dat daar zelf onderzoek naar wordt gedaan.

Anita van den Berg (advocaat Amsterdam) geeft aan dat zij enigszins aangeslagen was door de opmerking van de preadviseurs dat gegevens binnen de gemeente gemakkelijker gedeeld moeten kunnen worden om het algemeen belang binnen de gemeente te kunnen dienen. Zij vraagt zich af of het specialiteitsbeginsel daardoor niet in gevaar zal komen. Het algemeen belang is een heel breed begrip dat bestaat uit allerlei deelbelangen die zijn uitgewerkt in wet en regelgeving. In dat kader heeft de overheid allerlei bevoegdheden en kunnen allerlei gegevens worden vergaard. De overheid heeft een hele sterke positie omdat zij met de vergaarde gegevens eenzijdig verstrekkende verplichtingen kan opleggen. De burger wordt daar onder andere tegen beschermd doordat de overheid alleen haar bevoegdheden mag uitoefenen met het oog op het doel waarvoor de bevoegdheid is verleend. Volgens Van den Berg geldt het specialiteitsbeginsel ook voor gegevens die in het kader van een dergelijke bevoegdheid zijn vergaard. Zij vraagt de preadviseurs of het specialiteitsbeginsel rekkelijker moet worden bezien als het gaat om de vergaring en gebruikmaking van persoonsgegevens. **Sultan Gün** benadrukt dat zij niet pleit voor het zonder enige grens uitwisselen van gegevens. Wat zij en Belhaj vooral duidelijk willen maken is dat daar waar de overheid met het delen van informatie beoogt om iemand te helpen, privacywetgeving daaraan in de weg kan staan. Gün noemt als voorbeeld de jongeren die op de Top600-lijst staan en die op zoek zijn naar werk. De gemeente Amsterdam maakt afspraken met werkgevers om stages aan deze jongeren aan te kunnen bieden. Daarvoor is alleen wel nodig dat de gemeente aan werkgevers kan vertellen dat het om jongeren gaat die op de Top600-lijst staan. En dat is op grond van de huidige privacywetgeving in beginsel niet toegestaan, terwijl de jongere in kwestie wel graag wil werken en belang heeft bij de gegevensuitwisseling. **Anita van den Berg** merkt op dat zij het met Gün in dat opzicht eens is, maar geeft ook aan dat het hier om een andere situatie gaat dan die tijdens de presentatie werd geschetst. Toen ging het om gegevens die in

het kader van de Wet maatschappelijke ondersteuning worden vergaard en vervolgens voor andere doeleinden worden ingezet. In het voorbeeld van de Top600 heeft de jongere zelf ook een bepaald belang bij het delen van gegevens, en bovendien ligt er dan nog een convenant aan ten grondslag. Dat is niet zo bij het delen van gegevens binnen de gemeentelijke organisatie. **Sultan Gün** vult aan dat het door haar geschetste probleem zich ook kan voordoen binnen diensten, bijvoorbeeld als de Dienst Werk en Inkomen iemand aan werk wil helpen en er informatie wordt gedeeld over iemands handicap. Daarmee kun je passende arbeid aanbieden en mogelijk onnodig ontslag voorkomen. In die situatie is het vaak lastig om informatie uit te wisselen en daar loopt de gemeente Amsterdam tegenaan. **Addie Timmer-van der Hoeven** merkt op dat in de laatste situaties die Gün schetst, er heel duidelijk sprake is van een overlegsituatie; de betrokkene heeft iets te winnen en gaat akkoord met de informatie-uitwisseling. Maar er zijn ook situaties waarin dat niet het geval is. Timmer geeft het voorbeeld van een man die bij een ministerie aan de balie werd aangehouden omdat zijn oom betrokken was geweest bij Occupy. De man heeft vervolgens gezegd dat hij al jaren niet meer met die oom omgaat en werd daardoor alsnog toegelaten tot het ministerie. Dit voorbeeld schetst de vergaande consequenties van gegevensuitwisseling in de situatie dat de betrokken persoon niet zelf een afweging kan maken over de gegevensuitwisseling. De man in kwestie kon niet zelf instemmen met de gegevensuitwisseling en dat deugt niet. **Sultan Gün** benadrukt dat zij geen pleidooi heeft willen houden voor onbegrensde gegevensuitwisseling binnen de overheid. De geschetste situatie is onwenselijk. Zij geeft voorts aan dat instemmen met het delen van gegevens niet de enige grond is op basis waarvan gegevens uitgewisseld kunnen worden.

Menno Spiertz vraagt aan de preadviseurs waartoe hun eerste stelling – over de fragmentarisatie van privacywetgeving en de belemmering van de doelbinding – zou moeten leiden. Is dat een pleidooi om meer gebruik te maken van de mogelijkheden die de Wbp al biedt voor verdere verwerking van persoonsgegevens? Of betreft de stelling een pleidooi gericht aan de wetgever? **Mohammed Belhaj** antwoordt dat de stelling een pleidooi is richting de wetgever. De preadviseurs merken op dat aan de eisen van doelbinding in de praktijk invulling wordt gegeven door het werken met de integrale aanpak; daarmee wordt afgebakend voor welke doelen men werkt. Wat de preadviseurs merken is dat de privacywetgeving van nu niet is geschreven voor het delen van informatie in samenwerkingsverbanden, maar meer voor het delen van informatie tussen twee overheidsinstanties. De preadviseurs zouden willen pleiten voor regelingen en convenanten die specifiek zien op het delen van informatie in samenwerkingsverbanden. Dat zou weliswaar betekenen dat er nog meer regelgeving bij komt, maar als daarmee meer helderheid kan worden verschaft, dan zijn de preadviseurs daar groot voorstander van.

Paneldiscussie

Ben Schueler stelt voor om de discussie breder te trekken en daartoe eerst aandacht te schenken aan het thema van Arjan de Jong. De ontwikkeling van Big Data doet de vraag rijzen wat persoonsgegevens eigenlijk zijn. Schueler vraagt de zaal hoe zij daar tegenaan kijkt. Wat moeten we gaan verstaan onder

persoonsgegevens en neemt het aantal persoonsgegevens toe of blijft het aantal persoonsgegevens gelijk? **Somayeh Djafari (PhD-student Open Universiteit en lid van de Nationale Denktank)** denkt dat het aantal persoonsgegevens zal toenemen. In haar eigen onderzoek is gebleken dat persoonsgegevens niet alleen meer uit burgerservicenummers bestaan, maar ook uit gegevens afkomstig uit digitale processen, zoals kenmerken. Djafaribenoemt de verschuivingen in onze manier van denken over Big Data en de strategieën die worden toegepast om privacy en persoonsgegevens te beschermen. De meerwaarde van Big Data ligt niet zozeer bij hun primaire gebruik, maar bij de onvoorzienbare secundaire toepassing. Zo kan uit gegevens over energieverbruik niet alleen worden afgeleid hoe efficiënt iemand met zijn energie omgaat, maar ook wat het dagelijkse leefpatroon van die persoon is. Djafari vraagt De Jong of het klopt dat we een nieuwe strategie nodig hebben waarin de moderne benadering van privacy centraal staat. Is er een verschuiving gaande van de randvoorwaarden van privacy naar de verandering van de aard van het probleem? **Arjan de Jong** antwoordt dat in het privacyrecht veel randvoorwaarden geformuleerd zijn die zijn gericht op de voorspelbaarheid. Het dient tot op zekere hoogte voorspelbaar te zijn voor de betrokkene dat persoonsgegevens over hem verwerkt worden. Dit wordt mede vormgegeven door duidelijke verwerkingsgrondslagen, doelbinding en informatieplichten. Belangrijke verwerkingsgronden zijn *informed consent* en uitvoering van een overeenkomst, maar ook bijvoorbeeld de wet en de publiekrechtelijke taak van bestuursorganen kunnen als grondslag dienen. Daarnaast versterkt doelbinding eveneens de voorspelbaarheid, omdat de betrokkene kan weten binnen welke context de gegevens worden verwerkt. Bij Big Data is er sprake van het grootschalig verzamelen van gegevens uit verschillende bronnen en het hieruit deduceren of induceren van nieuwe informatie. Hierdoor kunnen door de verantwoordelijke inzichten en informatie worden verkregen die je als betrokkene redelijkerwijs niet kon voorzien. De Jong stelt voor dat ter compensatie hiervan meer transparantie nagestreefd zou kunnen worden. Hoe die transparantie kan worden geboden en hoe betekenisvolle invulling kan worden gegeven aan de informatieplicht, met name bij gegevens die op afstand zijn verzameld en verwerkt, is echter lastig. Vooral voor grote Big Data-bedrijven die miljoenen gegevens verzamelen is het lastig om te bedenken hoe de betrokken personen actief geïnformeerd zullen worden. Er is momenteel wel een trend gaande waarbij grote bedrijven portals aanbieden waarin personen zelf kunnen zien welk profiel er van hen is aangemaakt en waarin ze eventueel correcties kunnen laten aanbrengen. Het probleem met Big Data is echter dat kenmerken vaak op basis van correlatie aan personen worden toegedicht. Dat geeft een inherente onzekerheid over de juistheid van de data. Dit maakt, in het bijzonder wanneer er gebruikgemaakt wordt van niet maatschappelijk gangbare kenmerken, het voor de betrokkene bovendien lastig om de correctheid van de gegevens te betwisten. Samenvattend zijn derhalve verbeterde transparantie, inzage en de mogelijkheid om op verzamelde data te kunnen reageren, de belangrijkste aandachtspunten voor een nieuwe benadering van privacy.

Ben Schueler stelt voor om alle vijf preadviseurs dezelfde vraag te stellen. Wat zou het betekenen als de ontwikkeling zoals De Jong die heeft geschetst zich daadwerkelijk zal voltrekken? Heeft dat tot gevolg dat Big Data, door de combinatie van gegevens, tot zoveel informatie kan leiden dat een deel van de problemen die Sultan en Mohammed hebben geschetst, kan worden opgelost? En moet

daardoor het onderwerp van Van Graafeiland en Bontje ook anders worden bekeken, gelet op het feit dat Big Data niet aan landsgrenzen is gebonden? Is het uitwisselen van gegevens over de grens nog een probleem als er zoveel gegevens beschikbaar komen voor mensen die daar handig mee om kunnen gaan? **Marte van Graafeiland** geeft aan dat het niet zozeer de vraag is hoeveel gegevens worden vergaard en of die gegevens over de grens worden verstrekt. Wat voorop moet staan is dat er privacyregels zijn en dat die worden nageleefd. Daartoe is niet relevant hoeveel gegevens je kunt verzamelen. **Ben Schueler** vraagt De Jong of het klopt dat naarmate Big Data toeneemt, er steeds meer informatie uit kan worden afgeleid die volgens de regels vertrouwelijk zou moeten zijn. **Arjan de Jong** is van mening dat dit klopt. Als je informatie naast informatie uit een andere database kunt leggen en de informatie kunt combineren, dan kunnen daar nieuwe inzichten en uitkomsten uit voortvloeien. **Ben Schueler** vraagt Belhaj en Gün of er binnen de gemeente Amsterdam al wordt geprobeerd, bijvoorbeeld in het kader van de Top600, om via algemeen toegankelijke informatie achter allerlei kennis over een bepaalde persoon te komen. **Sultan Gün** merkt op dat binnen de gemeente Amsterdam geen gebruik wordt gemaakt van Big Data. Maar kijkt men naar de ontwikkelingen omtrent Big Data, dan lijkt het niet ondenkbeeldig dat er over vijftig jaar wellicht een gedachtepolitie is die kan zien wanneer iemand van plan is om een strafbaar feit te plegen. Dat lijkt haar overigens volstrekt onwenselijk. De gemeente Amsterdam is op dit moment wel van plan om de Top600 vanwege zijn succes uit te breiden naar een Top1000. De bedoeling is dat in die Top1000 mensen worden opgenomen die nog geen zware criminaliteit hebben gepleegd, maar die wel het risico lopen te zullen doorstromen naar de Top600. Voor dit soort personen wil de gemeente Amsterdam een voorspeller gaan gebruiken, waarbij gegevens die al over een persoon bekend zijn bij bijvoorbeeld de politie worden afgewogen en gebruikt om de kans te voorspellen dat die persoon een strafbare feit zal plegen.

Ben Schueler stelt voor om als laatste naar een van de stellingen van Van Graafeiland en Bontje te gaan. Hij vraagt aan de preadviseurs om de tweede stelling – over de toespitsing van verstrekkingsbepalingen op de verwerking van bijzondere persoonsgegevens – nader toe te lichten. Volgens **Nina Bontje** zijn verstrekkingsbepalingen nu zo algemeen geformuleerd, dat toezichthouders voor lastige afwegingen komen te staan. Die situatie doet zich bijvoorbeeld voor als de Nederlandse toezichthouder in het kader van een onderzoek naar een bestuurder gegevens heeft verzameld over de antecedenten van die bestuurder. Vervolgens verhuist de bestuurder naar Frankrijk om daar een nieuw, vergelijkbaar bedrijf te beginnen. De Franse toezichthouder wil vervolgens graag informatie over deze bestuurder ontvangen van de Nederlandse toezichthouder. De Nederlandse toezichthouder dient zich dan af te vragen of de algemene verstrekkingsplicht ook toelaat dat informatie over strafrechtelijke antecedenten wordt gedeeld. Wanneer de wetgever, zoals in dit voorbeeld, niet duidelijk aangeeft wanneer welke gegevens mogen worden gedeeld, dan moet de toezichthouder zelf de lastige afweging maken of gevoelige informatie gedeeld kan worden. **Ben Schueler** vraagt aan de zaal hoe men denkt over het voorstel van de preadviseurs om concretere normen te creëren. **Jessica Hoitink** heeft niet zozeer een antwoord op die vraag, maar wil wel graag een voorstel doen. De stelling van Van Graafeiland en Bontje kan wellicht gecombineerd worden met de stelling van Belhaj en Gün. De preadviseurs pleiten namelijk alle vier voor verheldering in de wet, maar erkennen

ook dat privacywetgeving vraagt om het nemen van gevalsbeslissingen. Is het niet een idee om een adviesorgaan in het leven te roepen dat kan worden geraadpleegd in geval van twijfel over de toepassing van een norm? Het College bescherming persoonsgegevens (CBP) is een toezichthouder geworden, dus dat kan niet meer om advies gevraagd worden. **Nina Bontje** antwoordt dat zij een dergelijk adviesorgaan geen slecht idee zou vinden. De toepassing van normen zou echter ook al enigszins geconcretiseerd kunnen worden in de wetsgeschiedenis. Verder blijven normen altijd algemeen en vereisen zij altijd een afweging in geval van toepassing. **Marte van Graafeiland** merkt aanvullend op dat zij niet echt weet of een adviesorgaan een hele goede oplossing zou zijn. In de verstrekkingsbepalingen wordt niet specifiek aangegeven dat ook bijzondere persoonsgegevens verstrekt kunnen worden. Die bepalingen formuleren een algemene verplichting of bevoegdheid tot verstrekking van gegevens. Dat betekent in feite dat bijzondere persoonsgegevens niet verstrekt mogen worden. De preadviseurs denken dat een oplossing beter gezocht zou kunnen worden in het creëren van duidelijkere bepalingen in de toekomst of het scheppen van duidelijkheid in de toelichting bij die bepalingen. **Ben Schueler** merkt op dat een nieuwe bepaling een adviesorgaan niet uit hoeft uit te sluiten. Hij vraagt de preadviseurs Belhaj en Gün of een adviesorgaan aan hun bezwaren tegemoet zou komen. Zou een adviesorgaan kunnen helpen bij het invullen van open normen, gelet op het feit dat dit adviesorgaan ook advies kan geven dat je eigenlijk liever niet wilt horen? **Mohammed Belhaj** geeft aan dat hij groot voorstander is van organen die iets adviseren waar hij zelf helemaal geen groot voorstander van is. Belhaj vindt dat de discussie in een bredere vorm moet plaatsvinden en daarvoor biedt de presentatie van Arjan de Jong een goed aanknopingspunt. Op het moment dat gegevens worden gedeeld met ondernemingen die alleen maar winstmaximalisatie tot doel hebben, dan doen we niet zo moeilijk over het delen van informatie. We accepteren de voorwaarden en lezen eigenlijk niet eens wat er staat. Belhaj geeft op persoonlijke titel aan dat hij het problematisch vindt wanneer iemand een beroep doet op de overheid, bijvoorbeeld bij de aanvraag van een uitkering, en dat daarbij vervolgens wordt nagegaan of die persoon niet toch over vermogen beschikt. Belhaj wil graag meer aandacht voor het feit dat de Wbp niet alleen ziet op de overheid, maar ook op ondernemingen. **Ben Schueler** merkt op dat Belhaj ons ter afsluiting een spiegel voorhoudt: terwijl we de hele middag discussiëren over de overheid, nemen we zelf als consumenten ook heel bewust deel aan het creëren van gegevens.

Het zijn de laatste afsluitende opmerkingen van de bijeenkomst. Ben Schueler dankt de preadviseurs voor hun prachtige adviezen en de begeleiding die hun bij het schrijven is geboden. Dankbetuigingen gaan uit naar Marije Batting, Rob Widdershoven, Jessica Hoitink, Herman Krans, Cécile Bitter en Reimer Veldhuis. De bijdragen hebben prachtige resultaten opgeleverd en tijdens deze plezierige middag tot hele interessante discussies geleid. De zaal bedankt de preadviseurs dan ook met een groots applaus.