Artikelen

Dr. C.M.K.C. Cuijpers[1]

[PUB=65]

Toepasselijk privacyrecht in de wolk[2]

Cloudcomputing roept door haar grensoverschrijdende karakter vragen op ten aanzien van het toepasselijke recht. In art. 4 van de Wet bescherming persoonsgegevens (Wbp) wordt bepaald wanneer het Nederlandse recht betreffende gegevensbescherming van toepassing is. Doel van deze bijdrage is om meer duidelijkheid te scheppen over de betekenis van art. 4 en de consequenties die dit artikel heeft met betrekking tot de verwerking van persoonsgegevens in de cloud.

1. Inleiding

De Europese Commissie en de Artikel 29-Werkgroep hebben recentelijk gewezen op de vragen die cloudcomputing oproept vanuit privacyperspectief.[3] De Commissie erkent dat cloudcomputing vanuit een oogpunt van gegevensbescherming een uitdaging vormt omdat individuen controle verliezen over potentieel gevoelige informatie wanneer zij hun gegevens opslaan op de hardware van anderen.[4] Ook wijst de Commissie op een recente studie die bevestigt dat privacy- en gegevensbeschermingsrisico´s in relatie tot online-activiteiten toenemen.[5] Een van deze risico´s hangt samen met het complexe vraagstuk van het toepasselijke

---

[1] Dr. C.M.K.C. Cuijpers is als universitair docent verbonden aan het Tilburg Institute for Law, Technology, and Society van Tilburg University.

[2] Dit artikel is gedeeltelijk gebaseerd op een onderzoek dat in opdracht van SURFnet, SURFdirect en Kennisnet is uitgevoerd: Colette Cuijpers, Ronald Leenes, Sandra Olislaegers en Kees Stuurman (2010), *De wolk in het onderwijs. Privacy aspecten bij Cloud computing services*. Rapport is beschikbaar op www.surf.nl/privacy.

[3] European Commission Brussels 4.11.2010, COM(2010) 609 final Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and the Committee of the Regions, '*A comprehensive approach on personal data protection in the European Union'*, http://ec.europa.eu/health/data_collection/docs/com_2010_0609_en.pdf en Artikel 29-Werkgroep, 0836/10/EN, WP 179, Opinion 8/2010 on applicable law, Adopted on 16 December 2010, http://ec.europa.eu/justice/policies/privacy/index_en.htm.

[4] COM(2010) 609 final, p. 2.

[5] Idem, referring to: *Study on the economic benefits of privacy enhancing technologies, London Economics*, July 2010, http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf, p. 14.

gegevensbeschermingsrecht. Aangezien bij cloudcomputing gebruik wordt gemaakt van ´remote servers´ van derde partijen die zich overal ter wereld kunnen bevinden, rijst de vraag of het Nederlandse recht betreffende gegevensbescherming van toepassing is als een Nederlandse entiteit besluit bepaalde diensten uit te gaan besteden aan de cloud. In Nederland is de toepasselijke rechtbepaling wat betreft gegevensbescherming neergelegd in art. 4 van de Wet bescherming persoonsgegevens, hetgeen een vrij letterlijke implementatie van art. 4 van Richtlijn 95/46/EG is.[6] De vragen die gerezen zijn met betrekking tot de uitleg van art. 4 Wbp, volgen dan ook rechtstreeks uit art. 4 Richtlijn. Om deze reden wordt de discussie en de uitleg die gegeven is aan art. 4 Wbp en art. 4 Richtlijn gelijktijdig, en soms door elkaar heen, besproken. Indien nodig wordt uitdrukkelijk aangegeven of het art. 4 Richtlijn of art. 4 Wbp betreft, maar over het algemeen zijn argumenten en meningen relevant voor beide artikelen. Doel van deze bijdrage is om meer duidelijkheid te scheppen over de betekenis van art. 4 en de consequenties die dit artikel heeft met betrekking tot de verwerking van persoonsgegevens in de cloud.

2. Cloudcomputing

In de literatuur zijn verschillende definities van cloudcomputing te vinden.[7] Over het algemeen zijn deze definities opgebouwd uit een aantal kenmerkende aspecten van cloudcomputing. Vanuit het perspectief van toepasselijk recht zijn met name de volgende kenmerken relevant: gebaseerd op diensten, gedeeld (*diensten delen, een verzameling hard- en softwarebronnen, ict-bronnen efficiënt benutten*[8]) en gebruik van internettechnologie.
Met betrekking tot het dienstenaspect kan worden opgemerkt dat bij cloudcomputing doorgaans een onderscheid wordt gemaakt in *software-as-a-service* (SaaS), *platform-as-a-service* (PaaS) en *infrastructure-as-a-service* (IaaS). Bij SaaS gaat het om applicaties die via internet worden aangeboden door een cloudcomputing-serviceprovider (CcSP). Hierbij kan bijvoorbeeld gedacht worden aan diensten als e-mailvoorzieningen (zoals Hotmail), office-achtige applicaties (zoals

---

[6] In deze bijdrage wordt ingezoomd op art. 4, overige bepalingen over de toepasselijkheid van Richtlijn 95/46/EG, dan wel art. 4 Wbp – zoals art. 3 van de Richtlijn en de art. 2 en 3 Wbp betreffende werkingssfeer – blijven buiten beschouwing.

[7] Zie de bijdrage van Ferreira Pires in deze special waarin wordt uitgegaan van de definitie zoals gegeven door *The National Institute of Standards and Technology* (NIST), maar bijvoorbeeld ook definities zoals gehanteerd door de Europese Commissie: '*Internet-based computing whereby software, shared resources and information are on remote servers ("in the cloud")*'. (COM (2010) 609 final) McKinsey: '*Clouds zijn hardwaregebaseerde diensten die reken-, netwerk- en opslagcapaciteit bieden'*, http://resource.onlinetech.com/cloud-computing-defintion-from-mckinsey-company/ en Gartner '*Een computationele stijl waarbij ict schaalbare en elastische mogelijkheden biedt die worden geleverd als dienst aan externe klanten via het gebruik van internettechnologie'*, www.gartner.com/it/page.jsp?id=1035013.

[8] Zie de definitie (met toelichting) van het National Institute of Standards and Technology in het eerste artikel van deze special.

Google Docs) en aan online sociale netwerken. De verwerking van persoonsgegevens speelt bij deze vormen van dienstverlening een belangrijke rol.
De kenmerken ´gedeeld´ en ´gebruik van internettechnologie´ zijn relevant met het oog op het toepasselijke recht aangezien deze kenmerken inhouden dat de diensten niet vanuit één land aangeboden hoeven te worden. Hard- en softwarebronnen, waaronder servers, kunnen verspreid zijn over verschillende landen. Cloudcomputing kan daardoor verschillende jurisdicties betreffen, hetgeen de vraag oproept welk recht van toepassing is op de verwerking van persoonsgegevens in de cloud. In deze bijdrage wordt enkel gekeken naar het toepasselijke gegevensbeschermingsrecht en niet naar de toepasselijkheid van andere rechten.

3. Art. 4: inleiding

Zoals hierboven aangegeven vormt art. 4 van Richtlijn 95/46/EG een specifieke bepaling betreffende de toepasselijkheid van het recht op gegevensbescherming.[9] Een dergelijke bepaling is nodig om in geval van grensoverschrijdende persoonsgegevensverwerking het nationale recht te kunnen bepalen dat op deze verwerking van toepassing is. Art. 4 is echter complex van aard en in de literatuur is de uitleg van dit artikel hevig bediscussieerd. Recent heeft zowel de Europese Commissie als de Artikel 29-Werkgroep zich in deze discussie gemengd.[10] Mede onder vermelding van cloudcomputing wijst de Artikel 29-Werkgroep op de noodzaak van een verheldering van art. 4. De groep wijst op de toenemende globalisering en de ontwikkeling van nieuwe technologieën die bijdragen aan de complexiteit van het vraagstuk van toepasselijk recht. Bedrijven opereren steeds vaker in meerdere jurisdicties en verlenen diensten en bieden ondersteuning *around-the-clock*. Het internet maakt het eenvoudig om diensten op afstand te verlenen en om persoonsgegevens te verzamelen en te delen in een virtuele omgeving en cloudcomputing maakt het moeilijk om de locatie van de persoonsgegevens en de middelen die gebruikt worden voor de verwerking van de persoonsgegevens specifiek te kunnen vaststellen.[11]

---

[9] 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, *Publicatieblad* nr. L 281 van 23 november 1995, p. 31-50.

[10] De Commissie in het hierboven al aangehaalde COM(2010) 609 final. In paragraaf 2.2.3 met de titel *´Clarifying the rules on applicable law and Member States' responsibility´*, stelt de Commissie: '*This is particularly the case when a data controller is subject to different requirements from different Member States, when a multinational enterprise is established in more than one Member States or when the data controller is not established in the EU but provides its services to EU residents.*', p. 11. Uit paragraaf 5 zal blijken dat deze omschrijving het standpunt van de Commissie met betrekking tot de uitleg van art. 4 niet geheel duidelijk maakt, aangezien gesproken wordt van ´established in several Member States´ en niet van ´establishments´.

[11] WP 179.

In het navolgende wordt eerst de onduidelijkheid betreffende art. 4 geïllustreerd aan de hand van een discussie die enkele jaren geleden in Nederland gevoerd is over de uitleg van art. 4 Wbp.[12] Daarna wordt aan de hand van een recente opinie van de Artikel 29-Werkgroep aangegeven welke uitleg van art. 4 volgens deze werkgroep gevolgd moet worden. De bijdrage besluit met de consequenties die deze uitleg heeft voor cloudcomputing.

4. De begrippen vestiging, verantwoordelijke en verwerker

Een groot deel van de discussie omtrent art. 4 richt zich op de uitleg van het begrip vestiging. Om die reden beperkt deze paragraaf zich tot het eerste lid van art. 4. Aangezien de Artikel 29-Werkgroep zich ook heeft uitgesproken over de uitleg van de overige leden van art. 4 van de Richtlijn, wordt hier in paragraaf 7 kort nader op ingegaan.
Art. 4 lid 1a Richtlijn 95/46/EG luidt, waarbij de relevante woorden zijn benadrukt.:

1. Elke Lid-Staat past zijn nationale, ter uitvoering van deze richtlijn vastgestelde bepalingen toe op de verwerking van persoonsgegevens indien:
*a) die wordt verricht in het kader van de **activiteiten** van een **vestiging** op het grondgebied van de Lid-Staat van de voor de verwerking **verantwoordelijke**; wanneer dezelfde verantwoordelijke een vestiging heeft op het grondgebied van verscheidene Lid-Staten, dient hij de nodige maatregelen te treffen om ervoor te zorgen dat elk van die vestigingen voldoet aan de verplichtingen die worden opgelegd door de toepasselijke nationale wetgeving;*

In Nederland is deze bepaling als volgt omgezet in art. 4, eerste lid, Wbp:

*Deze wet is van toepassing op de verwerking van persoonsgegevens[13] in het kader van **activiteiten** van een **vestiging** van een **verantwoordelijke** in **Nederland**.*

Enige verduidelijking met betrekking tot art. 4 kan gevonden worden in overweging 19 van Richtlijn 95/46/EG. Deze overweging bepaalt met betrekking tot een vestiging ten eerste dat de rechtsvorm van een vestiging, of het nu gaat om een bijkantoor of om een dochteronderneming met rechtspersoonlijkheid, niet doorslaggevend is. Wel moet het gaan om een 'vaste vestiging'.

---

[12] Zie voor deze discussie E.M.L. Moerel, 'Back to basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008-3, p. 81-91, M.A.H. Fontein-Bijnsdorp, 'Art. 4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', *Computerrecht* 2008-6, p. 285-289, E.M.L.Moerel, 'Art. 4 Wbp revisited; naschrift De nieuwe WP Opinie inzake Search Engines', *Computerrecht 2008-6*, p. 290-298. De discussie is later besproken door G.J. Zwenne en C. Erents, 'Reikwijdte Wbp: enige opmerkingen over de uitleg van artikel 4, eerste lid, Wbp', *P&I* 2009-2, p. 60-67.

[13] Hoewel voor de toepasselijkheid van de Wbp het van groot belang is om na te gaan of sprake is van de ´verwerking´ van ´persoonsgegevens´ ga ik er in deze bijdrage van uit dat dit het geval is, zodat het betoog toegespitst kan worden op de discussie die bestaat omtrent de uitleg van de concepten ´gevestigd´en ´vestiging´.

Met betrekking tot dit criterium heeft het Europese Hof bepaald dat sprake is van een vaste vestiging wanneer sprake is van bestendigheid en duurzaam wordt beschikt over personele en technische middelen die noodzakelijk zijn om de betreffende diensten te kunnen verrichten.[14] Tot slot moet het gaan om het effectief en daadwerkelijk uitoefenen van activiteiten. In dit verband heeft de Artikel 29-Werkgroep opgemerkt dat: '*The notion of "context of activities" does not imply that the applicable law is the law of the Member State where the controller is established, but where an establishment of the controller is involved in activities relating to data processing.*'[15] De Artikel 29-Werkgroep stelt voorts dat bij de analyse of sprake is van ´*in the context of the activities*´ de volgende overwegingen in ogenschouw genomen moeten worden: de mate waarin de vestiging betrokken is bij verwerkingsactiviteiten; de aard van de activiteiten; en het doel van de richtlijn, dat gericht is op het waarborgen van effectieve gegevensbescherming aan betrokkenen op een simpele, werkbare en voorzienbare wijze.[16]
Blok verduidelijkt het criterium van ´in de context van activiteiten´ aan de hand van het volgende voorbeeld: '*Als een internetbedrijf vanuit Nederland online zijn diensten aanbiedt in Zweden, is de Wbp van toepassing op de gegevensverwerking in het kader van die diensten, ook al bevinden de webservers zich in Zweden, wordt gebruikgemaakt van een Zweedse domeinnaam, is de site in het Zweeds opgesteld en hebben de verzamelde gegevens uitsluitend betrekking op inwoners van Zweden. (…) Indien een Nederlandse vestiging van een Amerikaans bedrijf bijvoorbeeld uitsluitend toegang heeft tot dat deel van een centraal beheerd klantenbestand dat betrekking heeft op Nederlandse klanten, is de Wbp niet van toepassing op de verwerking van de gegevens van de Amerikaanse klanten.*'[17]
De Wbp is dus, op grond van art. 4, eerste lid, niet van toepassing wanneer geen verwerkingsactiviteiten in een Nederlandse vestiging plaatsvinden en de persoonsgegevens niet beschikbaar zijn binnen deze vestiging. Hierbij is het van belang om op te merken dat een vestiging niet zelf de persoonsgegevens hoeft te verwerken, het gaat om de verwerking *ten behoeve van* de vestiging, hetgeen de vestiging de mogelijkheid geeft de feitelijke

---

[14] Europees Hof van Justitie 4 juli 1985, zaak 168/84, ECR [1985] p. 2251, paragraaf 14 (*Günter Berkholz*), en Europees Hof van Justitie 7 mei 1998, zaak C-390/96, ECR [1998] p. I- 2553 (*Lease Plan Luxemburg/Belgische Staat*). Zie voor een nadere bespreking van deze arresten W.P.J. van Eijk-Nagel, *´Vaste inrichting´: definitie (on)gewenst?*, http://www.europesefiscalestudies.nl/upload/Van%20Eijk.pdf.

[15] WP 179, p. 12.

[16] Idem.

[17] P.H. Blok, 'Privacybescherming in alle staten', *Computerrecht* 2005-6, p. 299. Blok gaat er in dit voorbeeld uiteraard van uit dat ´vanuit Nederland´ een vaste vestiging in Nederland impliceert.

gegevensverwerking buiten de vestiging uit te besteden.[18] In een dergelijke constructie wordt gesproken van '*verwerker*'.[19] Alvorens het begrip '*verwerker*' nader te duiden, is het echter van belang eerst nader in te gaan op het begrip *´verantwoordelijke´*.

´Voor de verwerking verantwoordelijke´ is gedefinieerd in art. 2d van Richtlijn 95/46/EG: '*de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam die, respectievelijk dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer het doel van en de middelen voor de verwerking worden vastgesteld bij nationale of communautaire wettelijke of bestuursrechtelijke bepalingen, kan in het nationale of communautaire recht worden bepaald wie de voor de verwerking verantwoordelijke is of volgens welke criteria deze wordt aangewezen.*'[20] De Artikel 29-Werkgroep heeft in een opinie een nadere inkleuring gegeven aan dit begrip. Hieruit blijkt dat gekozen is voor een feitelijke benadering.[21] In de opinie valt te lezen: '*Wie het "doel" van de verwerking vaststelt, wordt (de facto) aangemerkt als voor de verwerking verantwoordelijk. Het vaststellen van de "middelen" voor de verwerking kan echter door de voor de verwerking verantwoordelijke worden gedelegeerd voor wat betreft technische of organisatorische aspecten. Punten van wezenlijk belang, die een centrale rol vervullen voor de rechtmatigheid van de verwerking – zoals de vraag welke gegevens moeten worden verwerkt, hoe lang zij moeten worden bewaard, wie toegang tot die gegevens heeft enz. – dienen echter door de voor de verwerking verantwoordelijke te worden vastgesteld.*'[22]

De opinie stelt voorts dat de onderneming als zodanig verantwoordelijk is voor de verwerking van gegevens en de verplichtingen die voortvloeien uit de wetgeving voor gegevensbescherming. Gezamenlijke verantwoordelijkheid is mogelijk. Gewezen wordt op het feit dat partijen bij het vaststellen van doelen van, en middelen voor, de verwerking niet altijd een even grote rol en inbreng hebben. In een situatie waarin partijen niet evenveel zeggenschap hebben, zijn zij ook niet in dezelfde mate verantwoordelijk en aansprakelijk. Wanneer slechts één partij doel en middelen vaststelt, maar deze voor de feitelijke verwerking van de gegevens een andere partij inschakelt, wordt gesproken van een *'verwerker'*. Uit de opinie van de Artikel 29-Werkgroep blijken twee centrale voorwaarden om een partij als verwerker aan te kunnen merken: '*1. Het*

---

[18] Zie in dit verband bijvoorbeeld ook Moerel 2008-3, p. 89: '*De conclusie is dat er alle aanleiding is om ook bij bewerkerschap aan te nemen dat de gegevens worden verwerkt in het kader van de activiteiten van de eigen vestiging van de bewerker – waarmee de Wbp ook op deze gegevensvewerkingen van toepassing zou zijn.*'

[19] In de Wbp wordt in art.1e gesproken van bewerker.

[20] Supra noot 11.

[21] Groep Gegevensbescherming Artikel 29, Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker', 00264/10/NL, WP 169, 16 februari 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_nl.pdf.

[22] Idem, p. 37.

betreft een aparte rechtspersoon, die los van de voor de verwerking verantwoordelijke staat; 2. Persoonsgegevens worden namens de voor de verwerking verantwoordelijke verwerkt.'[23] Ook geeft de opinie een overzicht van criteria die een nuttige rol kunnen vervullen bij het vaststellen van de hoedanigheid van de diverse bij de verwerking betrokken partijen: '*de mate waarin de voor de verwerking verantwoordelijke tevoren opdrachten heeft gegeven; de bewaking door de voor de verwerking verantwoordelijke van de kwaliteit van de dienst; de zichtbaarheid voor betrokkenen; de deskundigheid van de partijen; en de autonome beslissingsbevoegdheid waarover de diverse partijen nog beschikken.'*[24] Zie voor meer informatie het artikel 'De verantwoordelijke en de bewerker in de cloud ' in deze special.

5. De discussie omtrent de uitleg van art. 4 Wbp

In deze paragraaf wordt, aan de hand van een discussie die een aantal jaar geleden in Nederland gevoerd is, geïllustreerd dat art. 4 lid 1 Wbp op twee manieren kan worden uitgelegd. In Nederland is deze discussie met name gevoerd door Moerel,[25] die een ruime uitleg van art. 4 voorstaat, en Fontein-Bijnsdorp,[26] die heeft gepleit voor een beperkte uitleg. Bijzonder in dezen is dat Fontein-Bijnsdorp haar pleidooi houdt uit naam van de Nederlandse toezichthouder, het College bescherming persoonsgegevens (CBP).[27]
Bij een beperkte uitleg is de Wbp alleen van toepassing als de verantwoordelijke voor de gegevensverwerking in Nederland is gevestigd, en *niet* als de verantwoordelijke een vestiging in Nederland heeft.[28] De ruime uitleg van art. 4, eerste lid, van de Wbp houdt in dat de wet ook van toepassing is als de verantwoordelijke slechts een vestiging in Nederland heeft.[29] Het grote verschil bij deze benaderingen zit hem in het feit dat bij een beperkte uitleg een Nederlandse entiteit die in meerdere lidstaten vestigingen heeft maar gevestigd is in Nederland, alleen hoeft te voldoen aan de eisen die de Wbp stelt. Bij een ruime uitleg moet diezelfde entiteit voldoen aan de nationale wetgeving betreffende gegevensbescherming van elke lidstaat waar deze entiteit een vestiging heeft. Zowel Moerel als Fontein-Bijnsdorp grijpen voor de uitleg van art. 4 Wbp terug op de overwegingen 18 en 19 van Richtlijn 95/46/EG. Het feit dat de auteurs mede op basis van deze overwegingen tot een tegenovergestelde visie komen, geeft al aan dat deze onvoldoende houvast bieden.
De beperkte uitleg wordt door Fontein-Bijnsdorp voorts voornamelijk gebaseerd op een betere aansluiting bij de doelstellingen van de richtlijn: harmonisatie van nationaal gegevensbeschermingsrecht en het bevorderen van de interne markt. In haar conclusie stelt zij:

---

[23] Idem, p. 38.

[24] Idem.

[25] Supra noot 14.

[26] Idem.

[27] Zwenne en Erents 2009. Zie ook het citaat van Fontein-Bijnsdorp later in deze paragraaf.

[28] Zwenne en Erents 2009, p. 60.

[29] Moerel 2008-3, p. 81.

'*Dat leidt het CBP tot een interpretatie waarbij doorslaggevende betekenis wordt toegekend aan de rol die partijen spelen bij een specifieke verwerking van persoonsgegevens. Beslissend is welke vestiging verantwoordelijk is voor een specifieke verwerking van persoonsgegeven. Daarmee wordt een functionele invulling gegeven aan het toepasselijk recht. Het enkele feit dat er een "vestiging" van de verantwoordelijke in Nederland bestaat, wordt daarbij niet van doorslaggevende betekenis geacht.*'[30] Belangrijkste argument vormt het tegengaan van cumulatie van wetgeving en het voorkomen van lacunes, waar volgens Fontein-Bijnsdorp deze beperkte uitleg het best aan tegemoetkomt.[31]
Moerel baseert een ruime interpretatie van art. 4 op de uitleg die in andere lidstaten aan art. 4 gegeven wordt, op het feit dat verschillende auteurs deze ruime interpretatie ondersteunen en Moerel wijst er bovendien op dat de bewuste keuze van de wetgever voor de cumulatie van de nationale privacywetten blijkt uit het feit dat zelfs achteraf de Europese Commissie in haar evaluatie van Richtlijn 95/46/EG aangeeft (nog) niet aan de invoering van het land-van-oorsprong-beginsel te willen beginnen: '*Wat de op het land van herkomst gebaseerde bepaling betreft, voorziet de richtlijn reeds in de mogelijkheid om de verwerking te organiseren onder één voor de verwerking verantwoordelijke, hetgeen betekent dat alleen hoeft te worden voldaan aan de gegevensbeschermingswet van het land waar de verantwoordelijke is gevestigd. Dit geldt uiteraard niet wanneer een onderneming ervoor heeft gekozen haar recht van vestiging in meer dan één lidstaat uit te oefenen.*' [32] In een naschrift naar aanleiding van het artikel van Fontein-Bijnsdorp versterkt Moerel haar argumenten met een uitvoerige bespreking van de totstandkomingsgeschiedenis van Richtlijn 95/46/EG en wijst zij op de uitleg die de Artikel 29-Werkgroep geeft aan art. 4 in haar opinie over zoekmachines.[33] Moerel vat haar conclusie als volgt samen: '*Voor toepasselijkheid van artikel 4 lid 1 onder a in de Definitieve Richtlijn*[34]*:*

(i) behoeft de verantwoordelijke zelf niet meer in de EU gevestigd te zijn;
(ii) kan de verwerking zelf ook buiten de EU plaatsvinden;
(iii)is aanknopingspunt of de gegevensverwerking in "het kader van de activiteiten van een vestiging (van de verantwoordelijke) in de EU plaatsvindt";
(iv) *is het land-van-oorsprong beginsel verlaten. Op een verwerking kan als gevolg het recht van meer lidstaten van toepassing zijn.*'[35]

---

[30] Fontein-Bijnsdorp 2008, p. 289.

[31] Idem, p. 286.

[32] Eerste verslag over de toepassing van de Richtlijn gegevensbescherming (95/46/EG), Brussel 15 mei 2003. COM(2003) 265 definitief, p. 19.

[33] Moerel 2008-6 en Groep Gegevensbescherming Artikel 29, Advies 1/2008 over gegevensbescherming en zoekmachines, 00737/NL, WP 148, Goedgekeurd op 4 april 2008, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_nl.pdf.

[34] Richtlijn 95/46/EG, supra noot 11.

[35] Moerel 2008-6, p. 293.

Hoewel, in de woorden van Moerel, de poging van het CBP om cumulatie van toepasselijke wetgeving te voorkomen lovenswaardig is, wordt dit volgens haar niet bereikt door een beperkte uitleg van art. 4 Wbp. Sterker nog, Moerel wijst erop dat deze uitleg tot ongewenste resultaten leidt zoals het niet van toepassing zijn van de Wbp wanneer een bedrijf dat niet gevestigd is in de EU, in een Nederlandse vestiging persoonsgegevens verwerkt ten behoeve van de buiten de EU gevestigde moedermaatschappij.[36] Volgens Moerel kan de cumulatieproblematiek alleen worden opgelost door een wijziging van de Privacyrichtlijn waarbij het land-van-oorsprong-beginsel wordt ingevoerd.[37]
In een bespreking van de door Moerel en Fontein-Bijnsdorp gevoerde discussie scharen Zwenne en Erents zich achter de argumenten en het standpunt van Moerel dat art. 4 Wbp ruim moet worden uitgelegd.[38] Hoewel zij zich op het standpunt stellen dat de beperkte uitleg van art. 4 het probleem van meervoudige toepassing van privacywetgeving mogelijk oplost, plaatsen zij daarbij tegelijkertijd de kanttekening dat deze uitleg direct nieuwe problemen met zich brengt zoals de onduidelijkheid over de territoriale werking van de wet en het afwijken van de in andere staten gehanteerde uitgangspunten.[39]
Hoewel inhoudelijk de kaarten lijken te zijn geschud in het voordeel van de ruime uitleg, blijft een lastig punt in deze discussie dat juist het CBP, de autoriteit die in Nederland belast is met de handhaving van de naleving van de Wbp, een andere uitleg voorstaat. Toch lijkt, met het oog op een recente opinie van de Artikel 29-Werkgroep, ook het CBP overstag te moeten wat betreft een ruime uitleg van art. 4.

6. De zienswijze van de Artikel 29-Werkgroep

Eind 2010 heeft de Artikel 29-Werkgroep een opinie uitgebracht met als titel '*Applicable law*'.[40] Met deze opinie is de discussie omtrent de uitleg van art. 4 voorlopig beslecht in het voordeel van de ruime uitleg. Dit blijkt duidelijk uit de mededeling van de Artikel 29-Werkgroep dat het belangrijkste criterium om het toepasselijk recht vast te stellen niet de plaats is waar de verantwoordelijke zijn belangrijkste vestiging heeft, maar de plaats waar de verantwoordelijke een vestiging heeft.[41] De werkgroep verduidelijkt haar standpunt door uit te leggen dat de toepasselijkheid van het recht van een lidstaat samenhangt met de locatie van een vestiging van de verantwoordelijke in die lidstaat. Hierbij geeft de werkgroep aan dat de locatie van vestigingen van de verantwoordelijke in andere lidstaten de toepasselijkheid van de wetgeving

[36] Aangezien art. 4 lid 2 alleen van toepassing is als een verantwoordelijke buiten de EU geen vestiging heeft in een van de lidstaten, biedt dit artikel ook geen uitkomst. Moerel 2008-3, p. 86.

[37] Moerel 2008-3, p. 91.

[38] Zwenne en Erents, p. 61, 65 en 66.

[39] Zwenne en Erents (2009: 66) wijzen erop dat in andere staten art. 4 ruim wordt uitgelegd, en dat de beperkte uitleg van het CBP dus een afwijkend uitgangspunt vormt.

[40] WP 179.

[41] Idem, p. 7.

van deze andere lidstaten met zich kan meebrengen.[42] Dat hierdoor meerdere nationale wetten tegelijk van toepassing kunnen zijn, wordt door de Artikel 29-Werkgroep dus expliciet bevestigd. In dit verband wordt cloudcomputing zelfs genoemd als rechtvaardiging voor de keuze voor de plaats van vestiging in plaats van de locatie van een bestand. Immers, bij cloudcomputing is het vaak moeilijk, of zelfs onmogelijk, om de exacte locatie van een bestand op een bepaald moment vast te stellen.[43]
Met het oog hierop ziet de Artikel 29-Werkgroep de voordelen van het '*country of origin principle*' (land-van-oorsprongbeginsel). Dit beginsel houdt in dat alle vestigingen van een verwerker binnen de EU onderworpen zijn aan hetzelfde recht, namelijk het recht van toepassing op de hoofdvestiging, ongeacht de locatie van de dochtervestigingen. Volgens de Artikel 29-Werkgroep kan het overgaan op dit beginsel echter enkel bewerkstelligd worden wanneer een alomvattende harmonisatie van nationale wetgeving is bereikt, inclusief harmonisatie van de veiligheidsverplichtingen.[44]
Om lacunes en onnodige overlap van rechtsregels te voorkomen geeft de Artikel 29-Werkgroep twee criteria. Ten eerste, als de verantwoordelijke één vestiging heeft, dan is er één wet van toepassing voor de gehele EU/EEA, afhankelijk van de locatie van deze vestiging. In de tweede plaats, wanneer er meerdere vestigingen zijn, hangt de toepasselijkheid van de nationale wetgeving af van de specifieke activiteiten van elk van die vestigingen. De toepassing van deze criteria moet voorkomen dat er meerdere nationale wetten van toepassing zijn op dezelfde verwerkingsactiviteiten.[45]
In de opinie over toepasselijk recht besteedt de Artikel 29-Werkgroep ook aandacht aan het verschil tussen toepasselijk recht en jurisdictie. Dit met het oog op de bevoegdheden van nationale toezichthoudende autoriteiten. De groep wijst er uitdrukkelijk op dat de uitleg van art. 28 lid 6 van Richtlijn 95/46/EG met zich brengt dat ook wanneer het recht van een andere lidstaat van toepassing is, een toezichthoudende autoriteit zijn bevoegdheden mag uitoefenen met betrekking tot de verwerking van perspoonsgegevens die plaatsvindt op het territoir waar de toezichthoudende autoriteit gevestigd is.[46]
De Artikel 29-Werkgroep grijpt terug op de uitleg van het concept 'verwerking van persoonsgegevens' (WP 169) om aan te geven dat de verwerking van persoonsgegevens gefaseerd kan plaatsvinden en dat per fase een ander recht van toepassing kan zijn. Om te bepalen of een of meerdere wetten van toepassing zijn op een specifieke verwerking van persoonsgegevens, is het volgens de Artikel 29-Werkgroep van belang om het overkoepelende plaatje van de verwerkingsactiviteiten goed voor ogen te houden. Verschillende handelingen verricht door verschillende partijen die allen een en hetzelfde doel dienen, kunnen er onder

[42] Idem, p. 12.

[43] Idem, p. 8.

[44] Idem, p. 31.

[45] Idem, p. 9.

[46] Idem, p. 10.

omstandigheden toe leiden dat slechts één nationale wet van toepassing is omdat het concept '*context of activities*' bepalend is en niet de locatie van de data.[47]
Aan het begin van deze paragraaf heb ik met opzet geschreven dat de discussie voorlopig beslecht is. De Europese Commissie is namelijk voornemens om in 2011 met een wetsvoorstel te komen om Richtlijn 95/46/EG te wijzigen.[48] De noodzaak om art. 4 betreffende toepasselijk recht te vereenvoudigen wordt hierbij expliciet genoemd. Hierbij wordt aangegeven dat het nodig kan zijn de bepalende criteria te wijzigen.[49] Ook in dit verband wordt cloudcomputing als voorbeeld genoemd om de noodzaak van vereenvoudiging van art. 4 te illustreren.[50]

7. Art. 4 lid 1c en art. 4 lid 2[51]

Om te voorkomen dat verantwoordelijken zich buiten de EU gaan vestigen om toepasselijkheid van het Europese gegevensbeschermingsrecht te ontlopen, bevat art. 4 nog een ander criterium op grond waarvan de toepasselijkheid van het gegevensbeschermingsrecht bepaald wordt.[52] De relevante woorden zijn benadrukt.

Art. 4 lid 1c van Richtlijn 95/46/EG luidt:
c) de voor de verwerking verantwoordelijke persoon niet gevestigd is op het grondgebied van de Gemeenschap en voor de verwerking van persoonsgegevens ***gebruik maakt van*** *al dan niet geautomatiseerde* ***middelen*** *die zich* ***op het grondgebied van genoemde Lid-Staat*** *bevinden,* ***behalve*** *indien deze middelen op het grondgebied van de Europese Gemeenschap* ***slechts voor doorvoer*** *worden gebruikt.*

Het tweede lid van art. 4 Wbp vormt de implementatie van art. 4 lid 1c en luidt:

---

[47] Idem, p. 12.

[48] Idem, p. 18.

[49] COM(2010) 609 final, p. 11.

[50] Idem.

[51] Art. 4 lid 1b van de richtlijn luidt: *de voor de verwerking verantwoordelijke niet gevestigd is op het grondgebied van de Lid-Staat, maar in een plaats waar de nationale wet uit hoofde van het internationale publiekrecht van toepassing is.* Dit lid blijft in deze bijdrage buiten beschouwing. Volgens de uitleg in WP 179 gaat het met name om specifieke gevallen van toepasselijk recht zoals bij ambassades, consulaten, schepen of vliegtuigen.

[52] Zie voor deze achterliggende reden overweging 20 van Richtlijn 95/46/EG: '*Overwegende dat de vestiging in een derde land van de voor de verwerking verantwoordelijke de bescherming van personen waarin de onderhavige richtlijn voorziet, niet in de weg mag staan; dat in dit geval de verwerking moet worden geregeld door het recht van de Lid-Staat waarin de gebruikte middelen zich bevinden, en dat gewaarborgd moet worden dat de rechten en verplichtingen waarin de onderhavige richtlijn voorziet, in de praktijk worden geëerbiedigd.*'

2. Deze wet is van toepassing op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die ***geen vestiging heeft in de Europese Unie****, waarbij* ***gebruik wordt gemaakt van*** *al dan niet geautomatiseerde* ***middelen*** *die zich* ***in Nederland*** *bevinden,* ***tenzij*** *deze middelen* ***slechts*** *worden gebruikt* ***voor de doorvoer*** *van persoonsgegevens.*

Dat ook art. 4 lid 1c verduidelijking behoeft, werd reeds in 2003 door de Europese Commissie erkend.[53] In het eerste verslag over de toepassing van Richtlijn 95/46/EG merkt de Commissie op dat het criterium '*gebruik van middelen*' in de praktijk misschien niet gemakkelijk te hanteren is en dus verder moet worden verduidelijkt. De Commissie gaat zelfs zover om te stellen dat wanneer een verduidelijking niet volstaat, mogelijk gezocht moet worden naar een andere verbandsfactor om het toepasselijk recht te bepalen.[54]
Zover is het tot op heden niet gekomen. Met opinie WP 179 heeft de Artikel 29-Werkgroep wel een nadere inkleuring gegeven aan het bestaande criterium '*gebruik van middelen*'.[55] In de eerste plaats wordt duidelijk gesteld dat art. 4 lid 1c alleen van toepassing kan zijn als art. 4 lid 1a niet van toepassing is, dus wanneer de verantwoordelijke geen vestiging heeft op Europees grondgebied die daadwerkelijk betrokken is bij de verwerking van persoonsgegevens.[56] In de tweede plaats wordt gewezen op een opinie daterend van 30 mei 2002 waarin de Artikel 29-Werkgroep al duidelijk heeft gemaakt dat de terminologie '*gebruik maken van middelen*' twee elementen impliceert*: 'een vorm van activiteit die door de verantwoordelijke wordt uitgeoefend en het voornemen persoonsgegevens te verwerken. Dit betekent dat niet elk "gebruik" van "middelen" in de Europese Unie tot toepassing van de richtlijn leidt.'*[57] Dit is relevant in relatie tot cloudcomputing, zeker aangezien de Artikel 29-Werkgroep er uitdrukkelijk op wijst dat het voor toepasselijkheid niet noodzakelijk is dat de verantwoordelijke '*de middelen bezit of er eigenaar van is*'.[58]
Uit de opinie van de Artikel 29-Werkgroep blijkt bovendien dat de term 'middelen' ruim geïnterpreteerd moet worden. In de opinie wordt er uitdrukkelijk op gewezen dat deze ruime uitleg er onder omstandigheden toe kan leiden dat het Europese gegevensbeschermingsregime van toepassing is, zelfs wanneer de verwerking van persoonsgegevens geen daadwerkelijke link

---

[53] Eerste verslag over de toepassing van de Richtlijn gegevensbescherming (95/46/EG), COM/2003/0265 def., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:NL:HTML.

[54] Idem, p. 19.

[55] WP 179, p. 18-23.

[56] Idem, p. 19.

[57] Groep Gegevensbescherming Artikel 29, 5035/01/NL/def., WP 56, Werkdocument betreffende de internationale toepassing van de gegevensbeschermingswetgeving van de EU op de verwerking van persoonsgegevens op internet door websites van buiten de EU, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_nl.pdf, P. 10-11.

[58] Idem, p. 11.

heeft met de EU/EEA.[59] De ruime interpretatie omvat menselijke en technische intermediairen. Als voorbeeld wordt gewezen op enquêtes, wanneer gegevens verzameld worden door middel van (online-)vragenlijsten, dan is het recht van het land waar deze vragenlijsten worden aangeboden van toepassing.[60] In de opinie uit 2002 was er reeds op gewezen dat ook cookies en javascript banners de toepasselijkheid van art. 4 lid 1c met zich mee kunnen brengen.[61] Aangezien diensten die via een webbrowser worden benaderd bijna ondenkbaar zijn zonder cookies, leidt dit ertoe dat vrijwel iedere buiten de EU gevestigde cloudcomputing-serviceprovider op basis van art. 4 lid 1 onder c derhalve onder de toepasselijkheid van Richtlijn 95/46/EG valt. Dat wil zeggen dat een aanbieder, zoals Google, die voor het leveren van diensten in Nederland (zoals Google Docs) gebruik maakt van cookies wat betreft die dienst (Google Docs) moet voldoen aan de voorwaarden die de Wbp stelt.[62] Met andere woorden, de locatie van de cloudcomputing-serviceprovider doet er vrijwel niet toe, de Wbp, of een met de Wbp vergelijkbare nationale uitwerking van Richtlijn 95/46/EG, is hoe dan ook van toepassing. In de recente opinie over toepasselijk recht heeft de Artikel 29-Werkgroep aandacht besteed aan de vergaande consequenties die deze ruime uitleg van het ´gebruik van middelen'-criterium met zich brengt. De groep merkt in dit verband op dat de toepasselijkheid van de richtlijn alleen gesteund moet worden zolang er een daadwerkelijke en niet slechts onbeduidende link met de EU bestaat. *Onbeduidend* wordt uitgelegd als onopzettelijk gebruik van middelen in een lidstaat. Volgens de Artikel 29-Werkgroep kan het de rechtszekerheid verhogen als aan het criterium 'gebruik van middelen' het criterium 'gericht op individuen' wordt toegevoegd.[63] Alleen wanneer het gebruik van middelen gericht is op de individuen in een lidstaat zou art. 4 lid 1c van de Richtlijn dan leiden tot de toepasselijkheid van het recht van die lidstaat.
In tegenstelling tot het concept 'middelen' moet de uitzondering 'tenzij voor doorvoer' volgens de Artikel 29-Werkgroep beperkt worden uitgelegd. Hiervan lijkt volgens de werkgroep ook steeds minder sprake te zijn gezien de vele *value added services*, zoals *spam filtering*, die meer en meer aan doorvoer verbonden worden.[64]

8. Een kort uitstapje naar België

Wat betreft België heb ik geen literatuur kunnen ontdekken waarin de bepaling omtrent de toepasselijkheid van het Belgische privacyrecht ter discussie staat. Dit hangt waarschijnlijk samen met de gekozen bewoording in de Belgische implementatie van art. 4 van Richtlijn 95/46/EG. Hierin wordt uitdrukkelijk gesproken van 'effectieve en daadwerkelijke activiteiten

---

[59] WP 179, p. 2.

[60] Idem, p. 20.

[61] WP 56, p. 11 e.v.

[62] Supra noot 1, p. 19.

[63] WP 179, p. 24. In dit verband spreekt de Artikel 29-Werkgroep op p. 31 van de 'service oriented approach'.

[64] WP 179, p. 23.

van een vaste vestiging van de voor de verantwoordelijke voor de verwerking op het Belgisch grondgebied'. Zie in dit verband art. 3bis van de Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.[65] Het tweede lid van art. 3bis betreft het gebruik van middelen. De bewoording is vrijwel identiek aan die van art. 4 lid 1c van Richtlijn 95/46/EG en roept dus geen verdere vragen op. De hierboven beschreven uitleg van art. 4 geldt dan ook onverkort voor het Belgische art. 3bis.

9. Conclusie: toepasselijk recht en cloudcomputing

Hoewel vaak ten onrechte gedacht, is de locatie van gegevens niet bepalend voor de toepasselijkheid van het Europese, of een daarop gebaseerd nationaal, regime betreffende de verwerking van persoonsgegevens. Met de recente opinie van de Artikel 29-Werkgroep is de wijze waarop toepasselijk gegevensbeschermingsrecht moet worden bepaald, uitdrukkelijk vastgesteld: '*De belangrijkste criteria om het toepasselijke recht te bepalen zijn de vestiging van de verantwoordelijke en de locatie van de middelen. Dit betekent dat noch de nationaliteit, noch de plaats waar betrokkene gevestigd is, noch de fysieke locatie van de persoonsgegevens, een beslissend criterium vormt bij het vaststellen van het toepasselijke recht.*'[66] Wat de gevolgen van deze uitleg zijn voor cloudcomputing, wordt in deze conclusie kort besproken.
De uitleg van art. 4 leidt ertoe dat wanneer een Nederlandse verantwoordelijke gebruik gaat maken van clouddiensten, deze verantwoordelijke, maar ook de ingeschakelde CcSP, wat betreft de verwerking van persoonsgegevens al snel gebonden is aan de Wbp. Dit ongeacht de locatie waar de CcSP de data verwerkt en opslaat. De verantwoordelijke moet niet alleen zelf de regels van de Wbp naleven, maar moet er bovendien zorg voor dragen dat deze wet ook door de CcSP wordt nageleefd.[67]

Hoewel de locatie van de opgeslagen en verwerkte data niet bepalend is voor de toepasselijkheid van de Wbp, kan de locatie van de gegevensopslag vanuit een ander perspectief wel degelijk van belang zijn. De toepasselijkheid van lokale wet- en regelgeving kan namelijk samenhangen met de plaats waar gegevens verwerkt en opgeslagen worden. CcSPs kunnen gebruik maken van datacenters in privacy-onvriendelijke landen zoals China, Rusland en de VS.[68] Als een datacenter of een CcSP zich bijvoorbeeld in de VS bevindt, dan kan de Amerikaanse overheid op basis van federale antiterrorisme-wetgeving toegang krijgen tot die data, zonder dat de gebruiker van de clouddienst of de betrokkene hierover wordt ingelicht. In dit verband kan bijvoorbeeld gewezen

---

[65] Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (B.S., 18 maart 1993) – Geconsolideerde versie (01/08/2007), http://www.privacycommission.be/nl/static/pdf/wetgeving/wet_persoonlijke_levenssfeer_.pdf.

[66] Vrije vertaling van WP 179, p. 8. De groep wijst erop dat deze uitleg strookt met hoe het toepasselijke recht in het kader van Richtlijn 2000/31/EG (eCommerce) wordt uitgelegd. Ook hier is de plaats van vestiging van de verantwoordelijke het bepalende criterium.

[67] Art. 14 Wbp.

[68] Vgl. *Computable, Vraagtekens bij eigenaarschap clouddata*, 28 juli 2010.

worden op de USA PATRIOT Act.[69] Deze wet is van toepassing op gegevens die zijn opgeslagen op Amerikaans grondgebied, en kan verstrekkende privacyconsequenties hebben. Op basis van deze wet kan de Amerikaanse overheid gegevens opeisen zonder gerechtelijk bevel, althans met beperkte gerechtelijke toetsing,[70] zonder toestemming of wetenschap van betrokkene, en in bepaalde gevallen zelfs zonder geconcretiseerd doel.[71] Hoewel de USA PATRIOT-Act alleen van toepassing is in de VS, kan het zo zijn dat wanneer in de VS data- en communicatieverkeer gescand of gesurveilleerd wordt, ook 'Europese data' in die surveillance wordt betrokken omdat die data op Amerikaanse servers staat.[72]

In dit verband is het interessant om erop te wijzen dat grote cloudcomputing-serviceproviders zoals Google en Microsoft in hun beleid uitdrukkelijk hebben bepaald dat zij zullen voldoen aan wettelijke verplichtingen en rechtsgeldige verzoeken van de overheid om informatie.[73] Google stelt in de Gmail privacy policy bijvoorbeeld: '*Google complies with valid legal process, such as search warrants, court orders, or subpoenas seeking account information. These same processes apply to all law-abiding companies. As has always been the case, the primary protections you have against intrusions by the government are the laws that apply to where you live.*'[74] En ook de privacy policy van Microsoft bevat een dergelijke bepaling: '*We may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process.*'[75] Het voldoen aan wettelijke verplichtingen is vanuit een oogpunt van de Wbp ook niet problematisch. Art. 8 sub c staat de verwerking van persoonsgegevens uitdrukkelijk toe wanneer deze verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is.

Ook los van de mogelijkheden die de PATRIOT Act biedt, is het overigens maar de vraag hoe het in de VS gesteld is met de bescherming van persoonsgegevens. Hoewel de Europese Unie geprobeerd heeft haar regime betreffende persoonsgegevensverwerking via de Safe Harbor Principles te exporteren naar de VS, heeft recent onderzoek aangetoond dat Amerikaanse

---

[69] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

[70] Electronic Privacy Information Center. Zie onder 'Pen Registers, the Internet and Carnivore', http://epic.org/privacy/terrorism/usapatriot/.

[71] Electronic Privacy Information Center. Zie onder 'Liberalized Use of Pen Register/Trap and Trace Devices under FISA' en 'Multi-Point ('Roving Wiretap') Authority', http://epic.org/privacy/terrorism/usapatriot/.

[72] Supra noot 1, p. 32.

[73] Tene, Omer, *What Google Knows: Privacy and Internet Search Engines* (October 1, 2007). Utah Law Review, Forthcoming, SSRN, http://ssrn.com/abstract=1021490, p. 25.

[74] Zie: http://mail.google.com/mail/help/about_privacy.html.

[75] Zie: http://privacy.microsoft.com/en-us/fullnotice.mspx.

bedrijven al jarenlang frauderen met het Safe Harbor-keurmerk.[76] Niet alleen krijgen bedrijven die niet of beperkt aan de Safe Harbor Principles voldoen toch het certificaat, soms wordt het certificaat zelfs gebruikt door bedrijven die niet eens zijn aangesloten bij de Safe Harbor. De oorzaak is gebrek aan toezicht vanuit de US Departement of Commerce, de instantie die gaat over Safe Harbor, zowel bij de toegang tot als de controle op de naleving van de Safe Harbor-beginselen.[77]

Hoewel eerder vastgesteld is dat het Europese gegevensbeschermingsregime vrijwel altijd van toepassing is wanneer een Nederlandse entiteit gebruik gaat maken van cloudcomputing, is het maar de vraag hoe betekenisvol dit gegeven in de praktijk is. Buiten de kosten en de tijd die het afdwingen van recht in derde landen met zich meebrengt, is het überhaupt maar de vraag in hoeverre buitenlandse overheden, private partijen en gerechten zich gebonden zullen achten aan het Europese recht. Handhaving van dit recht ter plaatse zal dan ook niet verwacht moeten worden, en handhaving vanuit Europa zal, zoals aangegeven, problematisch zijn. Hoewel de rol en het belang van contracten bij cloudcomputing de reikwijdte van deze bijdrage te buiten gaat, kan er hier wel op gewezen worden dat het mogelijk is gegevensbeschermingsregels in een contract met een CcSP op te nemen.[78] Een contract is juridisch bindend tussen partijen en nakoming kan dus direct bij de wederpartij gevorderd worden. Het is dan ook verstandig om essentiële gegevensbeschermingsregels in een contract op te nemen wanneer een Europese entiteit te maken heeft met een buitenlandse CcSP die persoonsgegevens zal (laten) verwerken in derde landen. Van belang hierbij is dat in een contract de regels van de Wbp niet omzeild kunnen worden door te kiezen voor toepasselijkheid van buitenlands recht, zoals het recht van de Verenigde Staten.[79]

Hoewel dus de locatie van gegevens in beginsel niet bepalend is voor de toepasselijkheid van de Wbp, is het toch noodzakelijk dat bij de overstap naar clouddiensten rekening wordt gehouden met de locatie waarnaar persoonsgegevens doorgegeven, verwerkt en opgeslagen worden. Dit met het oog op de risico's die beperktere toezichts- en handhavingsmogelijkheden en toepasselijke lokale wetgeving betreffende vorderings- en monitoringsrechten, met zich meebrengen. Of de locatie van de gegevens een reden vormt om te kiezen voor een bepaalde CcSP of zelfs van clouddiensten af te zien, is echter een vraag die in een veel bredere context beoordeeld moet worden. Relevante vragen hierbij zijn: hoe groot is het risico van onrechtmatige persoonsgegevensverwerking; hoe groot zijn de gevolgen als het risico zich manifesteert; en in hoeverre wegen de risico´s en gevolgen zwaarder dan de voordelen om te kiezen voor een bepaalde CcSP?

---

[76] A.U. De Haes (2010), 'Grootschalige privacyfraude tussen EU en VS'. *Webwereld*, http://mobile.webwereld.nl/nieuws/67936/grootschalige-privacyfraude-tussen-eu-en-vs.html.

[77] Export.gov. Safe Harbor List, https://safeharbor.export.gov/list.aspx.

[78] Zie met betrekking tot cloudcomputing en contracten de bijdrage in deze special van Kristof De Vulder en Antoon Dierick, 'Contracteren in de cloud'.

[79] Zie supra noot 2, hoofdstuk 5, voor meer informatie over cloudcomputing, contracten en privacy.