De nieuwe Europese privacywetgeving: stand van zaken bijna twee jaar na Commissievoorstel

Mr. H. Hijmans*

In het voorjaar van 2012 heb ik in *NTER*[1] een bijdrage geschreven over de Commissievoorstellen van 25 januari 2012 voor nieuwe Europese wetgeving op het gebied van de gegevensbescherming.[2] De behandeling van deze voorstellen – en dan vooral de voorgestelde verordening – bij de Raad en het Parlement heeft de gemoederen in Brussel en ook in Nederland sterk bezig gehouden, vanwege de grote belangen die ermee gemoeid zijn, en de vaak uiteenlopende meningen over de verordening *an sich* en veel van de specifieke bepalingen die deze bevat. Het meest aansprekende bewijs daarvan zijn de bijna vierduizend amendementen die binnen het EP zijn ingediend in relatie tot de voorgestelde verordening. Bij het beëindigen van deze bijdrage is nog veel onduidelijk over het vervolg van het dossier. Ik wil deze bijdrage dan ook vooral benutten om de voor de lezers van *NTER* meest relevante elementen van het debat in kaart te brengen, in vervolg op mijn bijdrage uit 2012.

* Mr. H. (Hielke) Hijmans is afdelingshoofd Policy & Consultation bij de Europese toezichthouder voor de gegevensbescherming (EDPS). De auteur schrijft dit artikel op persoonlijke titel.

1. Mr. H. (Hielke) Hijmans is afdelingshoofd Policy & Consultation bij de Europese toezichthouder voor de gegevensbescherming (EDPS). De auteur schrijft dit artikel op persoonlijke titel. H. Hijmans, 'Nieuwe Europese regels voor privacy: commissie stelt pakket voor om gegevens ook in het informatietijdperk te beschermen', *NTER* 2012/4, p. 132-139.
2. Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming) (COM/2012/011 def.) en Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens (COM/2012/010 def.).

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/2012/011 def.).

Voorstel voor een richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens (COM/2012/010 def.).

Context

De voorstellen voor een herziene privacywetgeving vormen een technisch ingewikkeld dossier waar veel tijdsdruk op is gezet, om verschillende redenen. In de eerste plaats is het voorstel gepresenteerd[3] als een noodzakelijk antwoord op de snelle technologische ontwikkelingen en de globalisering. Het bestaande systeem met een lappendeken aan nationale wetten – die Richtlijn 95/46/EG[4] op uiteenlopende wijzen omzetten – en soms zwakke bevoegdheden voor toezichthouders is niet voldoende om privacy effectief te kunnen beschermen in de digitale interne markt. De snelheid van de technologische ontwikkeling vergt ook snelheid van de (Europese) wetgever. In de tweede plaats is er veel politieke druk om tot een snel resultaat te komen. Vicepresident Reding van

3. Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's – Privacywaarborging in het online tijdperk. Een Europees gegevensbeschermingskader voor de 21e eeuw (COM/2012/09 def.).
4. 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, *Pb. EG* 1995, L 281/31.

de Europese Commissie heeft aan dit dossier veel van haar politieke lot verbonden en in het Europees Parlement – zeker in de Commissie Fundamentele Vrijheden (verder: LIBE) – is het er velen aan gelegen met een aansprekend resultaat te komen vóór de volgende Europese verkiezingen die in mei 2014 worden gehouden. Uitstel tot na deze verkiezingen zou een langdurende vertraging kunnen opleveren, omdat het draagvlak bij het nieuwe parlement niet noodzakelijkerwijs even groot is. In de derde plaats – en meer recentelijk – wordt de versterking van de Europese privacywetgeving gezien als een Europees antwoord op de onthullingen van onder andere Snowden over de intercepties door de Amerikaanse National Security Agency.
Het is tegen deze achtergrond dat ik in dit artikel enkele belangrijke controverses rond de Commissievoorstellen in kaart breng.

De actualiteit

De grote aandacht voor dit dossier is in de tweede helft van oktober 2013 – rond de inleverdatum van dit artikel – tot een ware apotheose gekomen.
Op maandag 21 oktober heeft LIBE compromisteksten aangenomen voor een algemene verordening voor gegevensbescherming en een richtlijn voor gegevensbescherming in de politie- en justitiesector.[5] Deze compromisteksten waren voorbereid door de respectievelijke rapporteurs Albrecht (Duitsland, Groenen) en Droutsas (Griekenland, sociaal-democraten). Deze stemming werd gezien als een doorbraak die moest leiden tot een snelle start van de onderhandelingen met de Raad, en met het doel overeenstemming te bereiken in het voorjaar van 2014 (dus vóór de Europese verkiezingen).
Op woensdag 23 oktober heeft het Europees Parlement een resolutie aangenomen over een dossier dat nauw gelieerd is aan de gegevensbescherming, namelijk het verdrag tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de EU naar de VS ten behoeve van het programma voor het traceren van terrorismefinanciering.[6] In zijn resolutie stelt het EP voor deze resolutie op te schorten vanwege de vermeende toegang van de NSA tot individuele bankgegevens.
Op donderdag 24 oktober vindt de Europese Raad plaats, waarin het onderwerp gegevensbescherming een significant onderwerp van discussie vormt, ditmaal gelieerd aan het onderwerp digitale economie, maar ook zeer nadrukkelijk aan de activiteiten van de NSA, en de noodzaak van een adequate respons. De Commissie zag deze laatste link als een goede gelegenheid om de urgentie van de nieuwe gegevensbeschermingswetgeving in de Raadsconclusies tot uitdrukking te brengen, en de intentie vast te leggen dat de nieuwe wetgeving in het voorjaar van 2014 tot stand zou komen. Echter, de Raadsconclusies stellen het volgende: '(…) The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015.'[7] De Raadsconclusies laten daarmee het tijdstip waarop de wetgeving zou moeten worden vastgesteld in het midden. Ze sporen Raad en EP niet aan spoed te betrachten, maar vragen ook niet om uitstel. Naar verluidt[8] was dit laatste wel de intentie van de Europese Raad, vooral onder druk van de Britse premier Cameron.

De link met de NSA-affaire en de doorgifte van gegevens naar derde landen

In de recente discussies over de NSA-affaire[9] is versterking van de Europese privacywetgeving veelvuldig aangegeven als een belangrijke oplossingsrichting.[10] Indien Europa het eigen huis goed op orde heeft, heeft het een sterkere positie ten opzichte van de Verenigde Staten. Het Commissievoorstel verduidelijkt en verruimt het geografische toepassingsgebied van de Europese privacywetgeving en stelt zeker dat bedrijven uit derde landen onder het toepassingsgebied vallen indien zij goederen of diensten aanbieden aan betrokkenen in de Unie of het gedrag van dezen observeren, zoals een zoekmachine doet wanneer ze zoekgedrag analyseert en vervolgens gebruikt voor gerichte reclames (zie met name art. 3 van het voorstel).
Bovendien versterkt het voorstel in algemene zin de verantwoordelijkheid voor bedrijven om de regelgeving na te leven, onder meer via het beginsel van 'accountability'. Door deze versterkte verantwoordelijkheid zou het gemakkelijker worden om van bedrijven die gegevens doorgeven naar de Verenigde Staten te vergen dat zij ervoor zorgen dat deze gegevens niet automatisch wor-

5. Zie persverklaring van LIBE, <www.europarl.europa.eu/news/en/news-room/content/20131021IPR22706/html/Civil-Liberties-MEPs-pave-the-way-for-stronger-data-protection-in-the-EU>. De compromisteksten van LIBE zijn bij het inleveren van dit artikel nog niet formeel vastgesteld.
6. *Pb. EG* 2013, L 195/5. Deze overeenkomst is algemeen bekend als TFTP of Swift-overeenkomst.
7. Raadsconclusies, pt. 8, <www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf>. Nog geen Nederlandse tekst beschikbaar.
8. Zie samenvatting, te vinden op <www.euractiv.com>.
9. Ik richt me in deze context op de vermeende activiteiten van de NSA en laat de in deze context ook veel genoemde rol van Europese veiligheidsdiensten, zoals de Britse GCHQ, buiten beschouwing. Zie voor een goed overzicht van de gehele problematiek de recente study van Policy Department C van het EP, <www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf>.
10. Voor vicevoorzitter van de Commissie Reding is dit een steeds terugkerend argument. Zie ook de bijdrage van Peter Hustinx (EDPS) voor de onderzoekscommissie van LIBE, <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf>.

den doorgegeven aan de Amerikaanse autoriteiten, in strijd met de zogenoemde *safe harbour*-beginselen.[11]
De door de Commissie voorgestelde verordening laat de regels voor de doorgifte van gegevens naar derde landen in belangrijke mate in stand. Echter, de door LIBE aangenomen tekst bevat een bepaling[12] die tegen moet gaan dat bedrijven op basis van een wettelijke verplichting in een derde land gegevens doorgeven, indien die doorgifte niet is toegestaan op grond van het EU-recht. In concreto, waar het Europees recht doorgifte van gegevens van Europese burgers aan derden (waaronder publieke autoriteiten) verbiedt en bovendien verplicht tot het zorgen voor beveiliging van de gegevens, kan dit verbod niet zo maar opzij worden gezet door de nationale wet van een derde land.
Deze bepaling beoogt een oplossing te bieden voor de situatie waarin een bedrijf geconfronteerd wordt met conflicterende wettelijke verplichtingen, bijvoorbeeld wanneer een internetbedrijf volgens Amerikaans recht verplicht is gegevens van Europese burgers over te leggen, maar dit volgens de EU-regelgeving in beginsel niet is toegestaan. In dat geval moet het bedrijf dit melden aan de bevoegde gegevensbeschermingsautoriteit in de Unie die de rechtmatigheid van het Amerikaanse verzoek beoordeelt.
Ik merk nog op dat in de online omgeving overlappende jurisdicties niet zijn te voorkomen. Gegevens van Europese burgers worden wereldwijd verwerkt (*outsourcing* van *call centers*, *cloud computing*, enzovoort) en de bescherming van gegevens van EU-burgers in derde landen is een inherent deel van de EU-privacywetgeving. Een terugkomend thema in de discussie is of de EU-wetgever bevoegd zou zijn om de toegang van nationale veiligheidsdiensten tot persoonsgegevens te regelen, gelet op het feit dat ingevolge artikel 4 VEU de Unie geen bevoegdheid heeft inzake de nationale veiligheid. Echter, de beperking van de Uniebevoegdheid is in artikel 4 gekoppeld aan de essentiële staatsfuncties van de lidstaten, en heeft naar mijn mening geen betrekking op de nationale veiligheid van derde landen.[13]

De reikwijdte van de verordening

De verordening geeft uitwerking aan een algemeen geformuleerd recht van een individu op gegevensbescherming (zie art. 16 VWEU), dat ook in artikel 8 van het Handvest van de grondrechten is vastgelegd. Dit recht op gegevensbescherming brengt mee dat de gegevens van een individu slechts mogen worden verwerkt als aan een aantal voorwaarden is voldaan. Bovendien heeft de betrokkene rechten, bijvoorbeeld om te worden geïnformeerd over een verwerking en ook om gegevens uit databestanden te laten verwijderen, wanneer deze daar niet meer in horen. Wanneer gegevens als persoonsgegevens moeten worden gekenmerkt, leidt dat dus tot verplichtingen/lasten voor de verwerker.[14]
In Richtlijn 95/46/EG is het begrip persoonsgegeven ruim gedefinieerd als 'iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'.[15] Een ruime definitie wordt in het algemeen gerechtvaardigd door het feit dat het begrip in het VWEU en het Handvest ruim is bedoeld, en dat secundair recht niet de reikwijdte van en het begrip uit het primaire recht kan beperken, en het de Uniewetgever dus niet vrijstaat een beperktere reikwijdte te kiezen.
Deze definitie heeft steeds tot veel controverse geleid, bijvoorbeeld over de vraag of een IP-adres – dat bestaat uit een lange reeks letters en cijfers – een persoonsgegeven is. Het is dan ook niet verbazend dat er druk is uitgeoefend om de reikwijdte van het begrip persoonsgegeven te beperken, en daarmee de reikwijdte van de verordening te beperken. Ook is een groot aantal amendementen ingediend in het EP met het oogmerk een tussencategorie te creëren van zogenoemde pseudoniemen,[16] zijnde gegevens waaruit een persoon niet rechtstreeks kan worden geïdentificeerd, en ten aanzien waarvan een groot aantal verplichtingen uit de verordening niet zou gelden. Een argument daarvoor is dat een zoekmachine vaak niet weet door welke persoon deze wordt gebruikt, en dus ook die persoon niet kan informeren.
Van geheel andere aard is de discussie rond de materiële reikwijdte van de verordening. De diverse amendementen die ertoe strekten bepaalde sectoren (bijvoorbeeld de financiële sector) uit te sluiten, hebben het in het EP niet gehaald.
In de Raad heeft een uitvoerige discussie plaatsgevonden met als thema het mogelijk uitsluiten van de publieke sector.[17] Een aantal lidstaten, waaronder Duitsland, voerde aan dat het belangrijkste argument om de gegevensbescherming bij verordening (en niet via een richtlijn) te regelen is het creëren van een *level playing field*, vooral voor bedrijven die opereren via internet. Dat argument gaat niet op voor de publieke sector. Deze discussie lijkt te zijn afgerond ten faveure van een wijde reikwijdte, hetgeen een voortzetting van de huidige situ-

11. 2000/520/EG: Beschikking van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende Vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd, *Pb. EG* 2000, L 215/7.
12. Art. 43a van de door LIBE aangenomen tekst. De bepaling was eerder opgenomen in een uitgelekt ontwerp van de Commissie maar werd uiteindelijk door het college niet aanvaard.
13. Dit Europeesrechtelijk uiterst interessante vraagstuk laat ik in het bestek van dit artikel verder buiten beschouwing.
14. Zie over de nieuwe regelgeving ook H.R. Kranenborg, 'Nieuwe regels voor de bescherming van persoonsgegevens: van belang voor iedereen', *SEW* 2013, p. 309-321.
15. Zie hierover in meer detail Advies 4/2007 over het begrip persoonsgegeven van de Werkgroep Gegevensbescherming Artikel 29, te vinden op de website van DG Justitie.
16. Zie over pseudonomysed data de EDPS-comments van 15 maart 2013, te vinden op de EDPS-website. Zie ook de definitie in art. 4 van de door LIBE aangenomen tekst.
17. Zie bijvoorbeeld Data protection package - Report on progress achieved under the Cyprus Presidency, <http://register.consilium.europa.eu/pdf/en/12/st16/st16525.en12.pdf>.

atie inhoudt (Richtlijn 95/46/EG geldt gelijkelijk voor de publieke en de private sector), maar wel met meer flexibiliteit voor de nationale wetgever om voor de publieke sector specifieke aanvullende regels te stellen.
Tot slot wijs ik erop dat zowel in de Raad als in het EP veel kritiek is geleverd op het feit dat de verordening niet van toepassing is op de Europese instellingen. In het EP heeft dit ertoe geleid dat in de LIBE-tekst de uitzondering op het toepassingsgebied in artikel 3 van het Commissievoorstel is geschrapt (de Raad lijkt naar dezelfde conclusie te tenderen), onder toevoeging van een specifieke bepaling die de verhouding met de bestaande Verordening 2001/45/EG[18] regelt.

Administratieve lasten

Het debat in de Raad en in het EP gaat voor een zeer belangrijk deel over de administratieve lasten die het Commissievoorstel zou meebrengen. Dit is opmerkelijk daar het voorstel juist was gepresenteerd als een bijdage tot het versterken van het concurrentievermogen van de Unie, doordat het de divergerende nationale wetten van de EU vervangt door één uniforme verordening en ook de handhaving coördineert. Bovendien schrapt het voorstel (bureaucratische) notificatieverplichtingen bij de nationale toezichthouders. Echter, zoals de Raad van State ook uiteenzet,[19] tegenover deze lastenverlichtingen staat een mogelijk aanzienlijke lastenverzwaring voor bedrijven en overheden.[20]
De administratieve lasten waren een belangrijk thema gedurende het Ierse voorzitterschap in de eerste helft van 2013.[21] De Raad stelt een aanpak voor die meer is gebaseerd op risico voor het individu ('*risk based approach*') en die een aantal verplichtingen schrapt. Zo was het idee van de Ieren bijvoorbeeld om de privacyfunctionaris – die binnen bedrijven en overheden zorg moet dragen voor de naleving van de privacywetgeving – facultatief te maken. Ook in de door LIBE aangenomen tekst speelt risico een belangrijke rol.[22]

18. Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, *Pb. EG* 2001, L 8/1. Deze verordening is onder andere de rechtsgrondslag voor de EDPS.
19. Voorlichting van de Raad van State aan de Tweede Kamer, 28 juni 2012, *Kamerstukken II* 2011/12, 32 761, nr. 32, p. 23.
20. Zie mijn artikel in *NTER* 2012.
21. Zie o.a. Note from Presidency to the Council, 'General Data Protection Regulation - Key issues of Chapters I-IV', 31 May 2013, 10227/13 and Addendum to the note to from Presidency to the Council, 'General Data Protection Regulation - Key issues of Chapters I-IV', 31 May 2013, 10227/13, ADD.
22. Zie bijvoorbeeld het nieuw voorgestelde art. 32a.

Gedelegeerde en uitvoeringshandelingen

Een gelieerd thema gedurende de onderhandelingen was het grote aantal gedelegeerde en uitvoeringshandelingen als bedoeld in de artikelen 290 en 291 VWEU waarin het voorstel voorzag. Via deze handelingen zouden de administratieve lasten nog eens extra kunnen toenemen. De kritiek op dit grote aantal bevoegdheden dat de Commissie beoogde te creëren had echter een bredere achtergrond. Binnen de Raad en het EP richtte de kritiek zich deels op de bevoegdheidstoeëigening door de Commissie en op het op ondemocratische karakter, dit terwijl de gegevensbeschermingsautoriteiten[23] erop wijzen dat de essentiële elementen van het fundamentele recht op gegevensbescherming in de verordening zelf thuishoren. De verordening zou bijvoorbeeld zelf criteria bevatten voor wat onder ernstige risico's voor privacy wordt verstaan.
Het resultaat is dat dit een onderwerp is waarin alle betrokkenen zich vinden in de kritiek op het Commissievoorstel en voorstellen doen om het aantal handelingen op grond van de artikelen 290 en 291 VWEU aanzienlijk te verminderen.

Het toezichtmechanisme

Het voorstel voor de verordening beoogt een *level playing field* te scheppen, niet alleen door een eenvormige regeling maar ook door het toezicht te stroomlijnen.[24] Ik gebruik met opzet het woord stroomlijnen, en niet harmoniseren of centraliseren, aangezien de optie waarin een Europese toezichthouder bevoegd zou worden gemaakt in zaken met een EU-breed belang[25] niet serieus is besproken. Stroomlijning van het toezicht blijkt een buitengewoon weerbarstige opdracht te zijn, omdat een groot aantal verschillende invalshoeken verenigd moet worden.
Bedrijven die gegevens verwerken in meerdere lidstaten, zoals de grote internetaanbieders, moeten erop kunnen rekenen dat de regelgeving wáár ook in de EU op dezelfde wijze geïnterpreteerd wordt, en dat zij bovendien slechts met één toezichthouder te maken hebben (de '*one stop shop*') die een besluit neemt dat in de gehele Unie rechtskracht heeft.
Burgers wier gegevens verwerkt worden, moeten erop kunnen rekenen dat zij daadwerkelijke bescherming genieten. Zij moeten kunnen klagen bij de gegevensbe-

23. Zie hierover Advies 08/2012 met aanvullende input voor de besprekingen over de hervorming van degegevensbeschermingswetgeving van de Werkgroep Gegevensbescherming Artikel 29, met een analyse van alle bepalingen die delegatie bevatten.
24. Zie hierover uitgebreid mijn artikel in *NTER* 2012/4, p. 132-139.
25. Analoog aan bijvoorbeeld Verordening (EG) nr. 1/2003 van de Raad van 16 december 2002 betreffende de uitvoering van de mededingingsregels van de artikelen 81 en 82 van het Verdrag, *Pb. EG* 2003, L 1/1, die een onderscheid maakt tussen Europees en nationaal mededingingsrecht.

schermingsautoriteit in eigen land en als ze naar de rechter willen stappen moeten zij dit in hun eigen land kunnen doen.[26]

De gegevensbeschermingsautoriteiten moeten erop kunnen rekenen dat zij hun verantwoordelijkheid binnen het eigen rechtsbestel ook kunnen waarmaken, overeenkomstig de eisen van onafhankelijkheid die door het Hof van Justitie zijn gesteld,[27] terwijl zij tegelijkertijd geacht worden hun optreden – ook in individuele zaken – af te stemmen met hun collega's in andere lidstaten, al dan niet in de context van het op te richten Europees Comité voor de gegevensbescherming (European Data Protection Board, EDPB[28]).

Tegen deze achtergrond heeft LIBE een tekst aangenomen, waarin de volgende oplossingen worden voorzien:[29]

- In zaken met een grensoverschrijdende dimensie is er een leidende authoriteit (zie o.a. art. 54a). Ingeval niet duidelijk is welke autoriteit 'leidend' is, geeft de EDPB hierover een advies.
- De leidende autoriteit is verantwoordelijk voor het toezicht, maar werkt hiertoe nauw samen met de betrokken autoriteiten in andere lidstaten en houdt zo veel mogelijk rekening met de opvattingen van dezen. De aldus tot stand gekomen besluiten zijn bindend voor de andere autoriteiten. Deze laatsten kunnen aangeven dat ze serieuze bedenkingen hebben en de zaak dan voorleggen aan de EDPB (art. 58a).
- Er is een belangrijke rol weggelegd voor het stelsel van conformiteit bij de EDPB. In zaken van algemene strekking heeft de EDPB een adviserende rol.
- Echter, er is ook een taak in individuele gevallen. Artikel 58a voorziet in een intensieve samenwerking tussen de EDPB en de leidende autoriteit die erop gericht is consensus te bereiken. Echter, indien consensus niet mogelijk blijkt, is er als *ultimum remedium* voorzien in een bindende beslissing van de EDPB.[30]

Laatstgenoemde bevoegdheid zal in de praktijk wellicht niet vaak gebruikt worden, maar heeft wel een aantal principiële consequenties. In de eerste plaats verandert het de status van de EDPB van adviesorgaan in een administratief orgaan met besluitvormende bevoegdheid, onder toezicht van het Hof van Justitie. In de tweede plaats kan de vraag rijzen wat de consequentie is voor de betrokken nationale autoriteit. Zijn besluit kan *overruled* worden, en daarmee kan de onafhankelijke taakuitoefening worden aangetast. Betekent dit bijvoorbeeld dat de autoriteit de tegen haar wil genomen beslissing moet verdedigen voor de nationale rechter, en is deze laatste bevoegd om de beslissing (die *de jure* een beslissing is van de EDPB) te vernietigen? In de derde plaats zouden derden van de EDPB kunnen verlangen dat deze gebruikmaakt van zijn bevoegdheid een bindend besluit te nemen. Dit is een terrein waar de – financiële – belangen enorm zijn en waar een klein aantal grote bedrijven zoals Google en Facebook de markt beheerst en de middelen heeft om juridische procedures aan te spannen.

Tot slot is het goed aandacht te geven aan de discussies in de Raad, waar het '*one stop shop*' mechanisme veel aandacht kreeg.[31] De JBZ-Raad van oktober 2013 gaf steun aan dit mechanisme, met de cryptische conclusie dat een meerderheid van de lidstaten accepteert dat een autoriteit besluiten neemt die bindend zijn voor andere autoriteiten, maar voegde daaraan toe dat gezorgd moet worden voor nabijheid ('*proximité*') tussen het individu en het besluitvormingsproces. De achtergrond hiervan is het sterke belang dat met name Frankrijk hecht aan het beginsel van nabijheid. Franse autoriteiten moeten in staat kunnen zijn de grondrechten van Franse ingezetenen te beschermen. Dit verdraagt zich slecht met voor Frankrijk bindende besluiten van autoriteiten in andere lidstaten. Het alternatief dat Frankrijk aandroeg in de Raad was een vorm van co-decisie van verschillende autoriteiten, maar daarvoor bestond weinig steun.

Tot slot

Ik heb een selectie toegepast van thema's die een wijdere Europeesrechtelijke relevantie hebben. Er is echter meer:

- Ik heb in dit artikel de begrippen privacy en gegevensbescherming door elkaar heen gebruikt, terwijl het Handvest voor de grondrechten deze twee rechten onderscheidt, en meer en meer wordt erkend dat dit onderscheid geen puur symbolische betekenis heeft.[32] Het recht op privacy wordt gezien als een klassiek grondrecht dat in de eerste plaats een afweerrecht is tegen de overheid, terwijl het recht op gegevensbeschrming een recht is dat vooral de spelregels voor de gegevensverwerking geeft. Dit onderscheid zou ook in de context van de nieuwe verordening een rol kunnen spelen, bijvoorbeeld waar een op risico gebaseerde benadering wordt nagestreefd. Risico voor het individu is dan met name een privacyrisico.
- Veel van de onderhandelingen gingen over het veronderstelde niveau van bescherming, bijvoorbeeld over

26. In de Raad is dit een *hot item*, omdat met name Frankrijk van oordeel is dat een autoriteit volledig bevoegd moet zijn zaken te onderzoeken indien dit burgers van het eigen land treft, en niet verplicht moet worden deze onderzoeken over te laten aan autoriteiten in andere lidstaten.
27. HvJ EU 9 maart 2010, zaak C-518/07, *Commissie/Duitsland*, *Jur*. 2010, p. I-1885 en HvJ EU 16 oktober 2012, zaak C-614/10, *Commissie/Oostenrijk*, n.n.g. Nog aanhangig is zaak C-288/12, *Commissie/Hongarije*.
28. Zie over de EDPB uitgebreid mijn artikel in *NTER* 2012.
29. De tekst van LIBE volgt in belangrijke mate de inbreng van de Werkgroep Gegevensbescherming Artikel 29.
30. Dit laatste is overigens niet in overeenstemming met de inbreng van de Werkgroep Gegevensbescherming Artikel 29, die als *ultimum remedium* een beslissing van de Commissie voorzag, op voordracht van de EDPB.
31. <www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/138924.pdf>.
32. Zie J. Kokott en C. Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR', *International Data Privacy Law* 2013, 3 (4), p. 222-228. Zie ook het pleidooi van de EDPS in gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland and Others*, <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2013/13-07-09_Pleading_notes_Joint_Cases_C-23912_and_C-59412_EN.pdf>.

het 'recht vergeten te worden', specifieke bepalingen voor het maken van persoonsprofielen, en ook over de verzwakking van de fundamentele beginselen van gegevensbescherming, zoals de doelbinding en het vereiste van expliciete toestemming.[33] Over dit beschermingsniveau is veel gesproken, bijvoorbeeld over de vraag of een 'recht vergeten te worden' realistisch is op internet en over de vraag of iemand altijd expliciet toestemming moet verlenen voor iedere verwerking, bijvoorbeeld als hij zoekt op een zoekmachine.

- De voorgestelde richtlijn voor de politie- en justitiesector heeft in het debat een ondergeschikte rol gespeeld, terwijl er nu wel een tekst is aangenomen in LIBE met een aantal zeer specifieke bepalingen die de gegevensbescherming op dit gevoelige terrein aanzienlijk zouden kunnen versterken.[34]
- De relatie tusen de verordening en nationale wetgeving is een terrein dat nog verder moet worden verkend, bijvoorbeeld in relatie met de flexibiliteit voor de publieke sector (zie hierboven), maar ook vanwege de relatie met andere rechtsgebieden (zoals bijvoorbeeld het gezondheidsrecht of het arbeidsrecht). De indeling van nationale regels in vier categorieën die de EDPS heeft gemaakt in zijn advies van 15 maart 2013 geeft een goed kader, ook voor andere EU-verordeningen.[35]
- Het is duidelijk dat de verordening, die onder andere de Wet bescherming persoonsgegevens moet vervangen, fors zal ingrijpen in de nationale wetgeving.

33. Informatie hierover is te vinden in verspreide bronnen, zoals de websites van de EDPS en DG Justitie/werkgroep gegevensbescherming, alsmede in documenten van de Raad en het Parlement (zoals de in voetnoot 5 geciteerde persverklaring van LIBE), en voor Nederland Kamerstukken met nummer 32 761.
34. Zie bijvoorbeeld art. 4 t/m 9 van de LIBE-tekst, die specifiek regelen hoe politie en justitie met gegevens kunnen omgaan.
35. Zie met name punten 50-53 van het advies, te vinden op de EDPS-website (in het Engels). Een Nederlandse samenvatting is gepubliceerd in *Pb. EU* 2013, C 192/5.