Nieuwe Europese regels voor privacy: commissie stelt pakket voor om gegevens ook in het informatietijdperk te beschermen

Mr. H. Hijmans*

Dit artikel bespreekt het 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), dat op 25 januari 2012 door de Commissie is aangenomen. Dit voorstel beoogt een ingrijpende vernieuwing van het Europese stelsel voor gegevensbescherming te bewerkstelligen, onder meer door in een verordening gedetailleerde regels te stellen die in de gehele Unie van toepassing zijn. Het artikel eindigt met enkele fundamentele Europeesrechtelijke vragen die het voorstel oproept.

Inleiding

Op 25 januari 2012 heeft de Europese Commissie een pakket maatregelen voorgesteld dat de Europese wetgeving voor de bescherming van persoonsgegevens ingrijpend moet hervormen. Doel van het pakket is ook in de toekomst effectieve bescherming te kunnen bieden, in een wereld die ingrijpend is veranderd en blijft veranderen. Het belangrijkste instrument voor gegevensbescherming, de Privacyrichtlijn 95/46/EG,[1] dateert uit een tijd waar internet nog in de kinderschoenen stond. Het massale, wereldwijde dataverkeer waarmee we nu mee te maken hebben, bestond nog niet in vergelijkbare mate.

Het pakket bestaat in de eerste plaats uit een voorstel voor een algemene verordening gegevensbescherming[2] die de gegevensbescherming beoogt te regelen op het terrein van grof gezegd de voormalige eerste pijler van het Unie-Verdrag. In de tweede plaats wordt een richtlijn voorgesteld voor de voormalige derde pijler.[3] Beide voorstellen geven uitvoering aan artikel 16 VWEU, dat sinds de inwerkingtreding van het Verdrag van Lissabon een nieuwe rechtsgrondslag geeft voor een moderne, integrale benadering van gegevensbescherming en het vrij verkeer van persoonsgegevens. Artikel 16 VWEU geeft de Unie-wetgever de opdracht regels te stellen op dit terrein.

De Commissie legt in een mededeling[4] van dezelfde datum uit wat de achterliggende redenen zijn om dit nieuwe wetgevingspakket voor te stellen. Voor de volledigheid meld ik nog dat in dezelfde context een verslag is gepresenteerd van de toepassing van het huidige regelgevingskader voor politiële en justitiële samenwerking, kaderbesluit 2008/977/JBZ.[5]

Dit artikel richt zich omwille van de omvang op de voorgestelde verordening. De richtlijn geeft specifieke

* Mr. H. Hijmans is afdelingshoofd Policy & Consultation bij de Europese toezichthouder voor de gegevensbescherming (EDPS).

1. 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.
2. 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)11 def.
3. Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012)10 final (nog niet beschikbaar in het Nederlands).
4. 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)9 def.
5. Verslag Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's op grond van artikel 29, lid 2, van het kaderbesluit van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, COM(2012)12 def.

regels voor de strafrechtelijke keten die soms aanzienlijk verschillen van de regels die worden voorgesteld in de algemene verordening. Voor dit verschil is niet steeds een goede rechtvaardiging te geven. Een analyse van de richtlijn zou een apart artikel in *NTER* vergen.[6]

Achtergrond: gegevensbescherming in het Europees recht[7]

De bescherming van persoonsgegevens komt voort uit het recht tot de bescherming van de persoonlijke levenssfeer uit artikel 8 EVRM en is daar nauw mee verbonden.[8] In het Handvest Grondrechten dat sinds de inwerkingtreding van het Verdrag van Lissabon verdragsstatus heeft, is het recht op gegevensbescherming opgenomen als zelfstandig grondrecht (in art. 8 Handvest Grondrechten) naast het recht op privacy dat in artikel 7 van het Handvest Grondrechten is vastgelegd.

De oorsprong van specifieke regels op Europees niveau voor de bescherming van het recht op gegevensbescherming ligt bij de Raad van Europa. Reeds op 28 januari 1981 werd een verdrag gesloten tot bescherming van personen terzake van de geautomatiseerde bescherming van persoonsgegevens (bekend als 'Conventie 108').[9] Alle EU-lidstaten hebben dit verdrag geratificeerd.

De bemoeienis van de Unie op dit terrein – met als belangrijkste product Richtlijn 95/46/EG – werd niet alleen gerechtvaardigd door de intentie fundamentele rechten te beschermen, maar vooral ook door het toegenomen belang van gegevensverkeer in de interne markt. Verschillen in nationale wetgeving – Conventie 108 was te weinig precies om nationale regels gelijk te trekken – leidden tot belemmeringen in het verkeer van gegevens tussen de lidstaten. Richtlijn 95/46/EG en ook de meer specifieke Richtlijn betreffende privacy en elektronische communicatie 2002/58/EG[10] zijn dan ook gebaseerd op het voormalige artikel 95 EG-Verdrag (nu: art. 114 VWEU).

Pas recenter heeft de zorg van de Unie voor de gegevensbescherming zich verbreed tot buiten de interne makt. In het vorige decennium kwam de noodzaak van bescherming in verband met het gebruik van persoonsgegevens door politie en justitie meer centraal te staan.[11] De aanslagen in New York van 11 september 2001 hebben ertoe geleid dat een belangrijk instrumentarium is ontwikkeld dat de internationale uitwisseling van persoonsgegevens moest faciliteren, binnen Europa maar ook met derde landen en in het bijzonder de Verenigde Staten.

Bij nieuwe instrumenten voor de uitwisseling behoort ook noodzakelijkerwijs een stelsel van bescherming van de justitiabelen wier gegevens worden verwerkt. Het al eerder genoemde kaderbesluit 2008/977/JBZ[12] is het resultaat hiervan. Verder hebben politieke en juridische geschillen over gegevensbescherming in relatie tot bijvoorbeeld de uitwisseling van passagiersgegevens tussen Europese luchtvaartmaatschappijen en de Amerikaanse autoriteiten, de toegang van deze autoriteiten tot Europese bankgegevens en het bewaren van telefoongegevens van Europese burgers de afgelopen jaren veel aandacht gekregen.[13]

Gegevensbescherming werd een onderwerp dat alle private en publieke sectoren betrof en dat daarom een integrale aanpak verdient. Die integrale aanpak is het uitgangspunt van het beleid van de Commissie.[14]

Ook de verdragswetgever lijkt de integrale aanpak tot uitgangspunt te nemen. Het Verdrag van Lissabon heeft het belang van gegevensbescherming aanzienlijk versterkt door het onderwerp op te nemen in het algemene deel van het VWEU. Artikel 16 VWEU geeft een ieder een – in beginsel rechtstreeks werkend – recht op de bescherming van de persoonsgegevens en draagt als gezegd de wetgever op hierover regels te stellen, in beginsel op alle terreinen waarop de Unie bevoegd is. Het recht van een ieder onder artikel 16 lid 1 VWEU is eveneens opgenomen in artikel 8 van het Handvest Grondrechten.

6. Over de richtlijn, zie het zeer kritische advies van de EDPS van 7 maart 2012 (te vinden op <www.edps.europa.eu>) en iets minder kritisch: P. De Hert en V. Papakonstantinou, 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', SCL Forum, te vinden op <www.scl.org>.
7. Meer informatie hierover valt te vinden in H.R. Kranenborg en L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief*, Deventer: Kluwer 2011.
8. Zie bijv. art. 1 lid 1 Richtlijn 95/46/EG. Waarborgen op het gebied van gegevensbescherming strekken ter bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, inzonderheid het recht op persoonlijke levenssfeer.
9. Te vinden op <www.coe.int>.
10. Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (Richtlijn betreffende privacy en elektronische communicatie), *Pb. EG* 2002, L 201/37 (gewijzigd bij Richtlijn 2009/136/EG, *Pb. EU* 2009, L 337).
11. Zie hierover: Hielke Hijmans en Alfonso Scirocco, 'Shortcomings in EU Data Protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?', *Common Market Law Review* 2009, 46, p. 1485-1525. Zie tevens het Luxemburgse proefschrift van Franziska Boehm, *Information sharing and data protection in the Area of Freedom, Security and Justice*, Berlin Heidelberg: Springer Verlag 2012.
12. Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, *Pb. EU* 2008, L 350/60.
13. Zie bijv. HvJ EG 30 mei 2006, gevoegde zaken C-317/04 en C-318/04, *Europees Parlement/Raad* en *Europees Parlement/Commissie*, *Jur.* 2006, p. I-4721, en HvJ EG 10 februari 2009, zaak C-301/06, *Ierland/Europees Parlement en Raad*, *Pb. EU* 2009, C 82/2.
14. Mededeling van de Commissie van 4 november 2010, Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie, COM(2010)609 def. Hiermee stel ik overigens niet dat het pakket dat nu is voorgesteld voldoet aan dit uitgangspunt (zie hieronder onder de kop 'Een nieuw eenvormig instrumentarium').

Kern van het stelsel

Artikel 8 van het Handvest Grondrechten geeft de kern van het rechtsstelsel weer. In de eerste plaats hebben degenen die gegevens verwerken (onafhankelijk of dit bedrijven zijn, *non profit* organisaties of overheidsinstellingen) verplichtingen: gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. In de tweede plaats hebben de betrokken personen individuele rechten, zoals een recht van inzage in de over hen verzamelde gegevens en een recht op rectificatie van die gegevens. Ten derde ziet een onafhankelijke autoriteit – zoals in Nederland het College bescherming persoonsgegevens, in België de Privacycommissie en op EU-niveau de EDPS – erop toe dat deze regels worden nageleefd. Dit onafhankelijk toezicht maakt deel uit van het recht dat de burger heeft op basis van het Handvest Grondrechten en het VWEU. Dit is een uniek element van het stelsel, dat op ander gebieden van het EU-recht niet in deze vorm voorkomt.

Verder heeft het stelsel, vanwege de intrinsieke globale dimensie, extraterritoriale kenmerken. Om de burger effectief te beschermen – zeker in een internetomgeving – is het nodig dat bedrijven uit derde landen die diensten aanbieden aan Europese burgers aan Europese regels gebonden zijn. Dit is in de praktijk ook uitermate belangrijk, omdat – zoals bekend – de grote spelers op het internet in de praktijk vaak bedrijven uit derde landen zijn, en meer in het bijzonder uit de Verenigde Staten. Bovendien moet ervoor worden gezorgd dat bescherming niet ophoudt op het moment dat gegevens uit de Europese Unie worden geëxporteerd. Vanwege deze laatste reden kent het stelsel al sinds langere tijd een streng regime voor de doorgifte van gegevens naar derde landen.

Waarom is aanpassing van het stelsel nodig?

De belangrijkste reden voor aanpassing is dat in een netwerkmaatschappij waar gegevens wereldwijd worden uitgewisseld en waar de fysieke plaats waar gegevens worden verwerkt in beginsel niet van belang is,[15] traditionele *command and control*-wetgeving onvoldoende effectief is. Om die reden is een belangrijk element van het nieuwe pakket het principe dat de voor de verwerking verantwoordelijke in belangrijke mate zelf (organisatorische) maatregelen moet treffen die een goede naleving van de wetgeving bevorderen. Op basis van dit zogenoemde *accountability*-beginsel moeten bedrijven en overheden hun organisatie en hun databases zo inrichten dat de burger daadwerkelijk wordt beschermd.

15. Bijv. vanwege organisaties die gebruik maken van *cloud computing* of die activiteiten uitbesteden (*outsourcen*), vaak ook naar buiten de EU.

Een verdere reden is dat de interne markt wordt belemmerd aangezien er – soms aanzienlijke – verschillen bestaan tussen de wetten van de lidstaten. Juist daarom wordt het instrument van verordening voorgesteld, zodat verschillen in toepasselijk recht binnen de Unie zoveel mogelijk worden geëcarteerd. Ook in de sfeer van het toezicht wordt naar eenvormigheid gestreefd. De invoering van mechanismen voor samenwerking en conformiteit moeten ertoe leiden dat de autoriteiten van de lidstaten op vergelijkbare wijze optreden.

Voorts past een eenvormig, strak en efficiënt systeem in het streven van de Europese Unie naar economische ontwikkeling zoals dat onder meer in de Digitale agenda voor Europa[16] is vormgegeven. De verordening moet leiden tot vermindering van de bureaucratie, gepaard aan vergroot vertrouwen van de consument.

Tot slot vergt de opdracht op basis van artikel 16 VWEU dat de burger effectief bescherming wordt geboden. De burger moet zoveel mogelijk zelf kunnen bepalen wat er met zijn gegevens gebeurt.[17]

De belangrijkste elementen van het pakket[18]

Het nieuwe pakket is ambitieus en streeft ernaar de tekortkomingen op een ingrijpende manier aan te pakken. Christopher Kuner, een van de meest vooraanstaande deskundigen op het terrein van gegevensbescherming, gaat zelfs zo ver dat hij het pakket omschrijft als een revolutie van Copernicus op het terrein van gegevensbescherming.[19]

De ontwerpverordening zal aanzienlijke gevolgen voor de rechtspraktijk hebben, ook in Nederland, niet in de laatste plaats omdat de nationale wetgeving op het gebied van de bescherming van persoonsgegevens (in het bijzonder de Wet bescherming persoonsgegevens) zal moeten worden ingetrokken. De verordening treedt daarvoor in de plaats, maar zal weer moeten worden aangevuld met nationale wetgeving die bepaalde aspecten regelt. Te denken valt in dit verband aan de aanwijzing van toezichthoudende autoriteiten of de uitzonderingen op verplichtingen uit de verordening die nodig zijn in het openbaar belang. Ook zal alle wetgeving die verwijzingen naar de Wet bescherming persoonsgegevens inhoudt of die anderszins regels stelt over de verwerking van persoonsgegevens (denk bijvoorbeeld aan regels over openbare registers of over het gebruik van

16. Mededeling van de Commissie van 26 augustus 2010, Een digitale agenda voor Europa, COM(2010)245 def.
17. Zie hierover mededeling van 25 januari 2012, geciteerd in voetnoot 2.
18. Een uitvoerige analyse van het pakket is terug te vinden in het advies van de Europese toezichthouder voor de gegevensbescherming (EDPS) van 7 maart 2012, geciteerd in voetnoot 6. Ook de Artikel 29 Werkgroep (zie voetnoot 30) heeft een advies uitgebracht; zie <www.ec.europa.eu/justice/data-protection/article-29/index_en.htm>.
19. C. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law', Privacy & Security Law Report ISSN 1538-3423, 2012.

het burgerservicenummer) moeten worden doorgelicht en waar nodig aangepast. De lidstaten hebben in het voorstel hiervoor een periode van twee jaar gekregen na de inwerkingtreding van de verordening (art. 91 lid 2 ontwerpverordening).

Een nieuw eenvormig instrumentarium

Het wettelijk instrumentarium wordt ingrijpend gerenoveerd. Richtlijn 95/46/EG wordt vervangen door een verordening die de nationale wetgeving op dit terrein in belangrijke mate overbodig moet maken. In de plaats van Kaderbesluit 2008/977/JBZ wordt een richtlijn voorgesteld, die in beginsel betrekking heeft op alle handelingen met persoonsgegevens in de sfeer van politie en justitie, dit terwijl het huidige kaderbesluit alleen regels stelt voor gegevens die worden uitgewisseld tussen de lidstaten. In strikt nationale situaties waar een grensoverschrijdend element ontbreekt, is dit kaderbesluit niet van toepassing.

Dit nieuwe instrumentarium streeft een integrale aanpak na. Volgens de Commissie[20] zijn moderne, coherente regels nodig om het mogelijk te maken dat gegevens van de ene naar de andere lidstaat kunnen stromen. Deze regels moeten een einde maken aan de nu bestaande gefragmenteerde juridische omgeving, met rechtsonzekerheid en ongelijke bescherming van individuen als gevolg.

Op het terrein waar de verordening van toepassing moet zijn, lijkt de Commissie in haar opdracht geslaagd. Er is een rechtsinstrument voorgesteld dat qualitate qua geldt binnen de gehele jurisdictie van de Unie en dat bovendien – globaal gesteld – voldoende specifieke regels stelt om rechtszekerheid te scheppen. Op veel plekken is daarnaast een zekere flexibiliteit ingebouwd, om ook op langere termijn effectief te blijven. De verordening schept ruime mogelijkheden voor de Commissie om in gedelegeerde of implementatiewetgeving op grond van de artikelen 290 en 291 VWEU de bepalingen van de verordening te specificeren. De verordening bindt de particuliere sector en de overheid wanneer gegevens worden verwerkt.

Dit betekent overigens geen volledige eenvormigheid van de regelgeving. De lidstaten blijven bevoegd om aanvullende – of zelfs afwijkende – regels te stellen wanneer het openbaar belang daarom vraagt en op terreinen waar de culturele verschillen tussen de landen te groot zijn om tot eenvormige regels te komen. Voorbeelden van die laatste terreinen zijn de relatie tussen bescherming van persoonsgegevens en de persvrijheid (art. 80 van de ontwerpverordening) en gegevensverwerkingen in het kader van de arbeidsverhouding (art. 82 van de ontwerpverordening).

Voorts mogen de lidstaten op grond van artikel 21 bij wettelijke maatregel de toepassing van een groot aantal verplichtingen uit de verordening beperken, wanneer dit nodig is ter bescherming van openbare belangen zoals de openbare veiligheid, het strafrecht en belangrijke financiële belangen van de staat.[21] De beperkingen moeten in een democratische samenleving noodzakelijk en evenredig zijn. Deze formulering is vergelijkbaar aan de criteria die onder het EVRM gebruikelijk zijn. Benadrukt wordt aldus dat het hier gaat om beperkingen van een fundamenteel recht.

Terreinen waarop de verordening niet van toepassing is

Buiten het terrein waarop de verordening van toepassing is, is van eenvormigheid geen sprake, ondanks het feit dat artikel 16 VWEU niet alleen een eenvormige regeling op (bijna) alle terreinen mogelijk maakt, maar ook de burger een recht op bescherming geeft, dat onafhankelijk is van de actor die de gegevens verwerkt.

Artikel 2 lid 2 van de ontwerpverordening schept een vijftal uitzonderingen op het algemene toepassingsgebied. De eerste uitzondering betreft de gebieden die buiten de werkingssfeer van het EU-recht vallen, in het bijzonder de nationale veiligheid.[22] Dit is een logische uitzondering waarop op zich niets valt af te dingen. In de praktijk echter, maar dat is een probleem dat niet alleen de bescherming van persoonsgegevens raakt, is het niet altijd eenvoudig vast te stellen waar het EU-recht ophoudt en waar de nationale veiligheid begint. De EU heeft in de loop der jaren vele maatregelen vastgesteld die de nationale veiligheid rechtstreeks raken, bijvoorbeeld ter bestrijding van het terrorisme of de georganiseerde grensoverschrijdende criminaliteit.

De tweede uitzondering betreft de activiteiten van de instellingen (en organen, bureaus en agentschappen) van de Unie zelf. Met deze uitzondering wordt de bestaande situatie bevroren. Voor de instellingen geldt thans een specifieke regeling, namelijk Verordening (EG) nr. 45/2001.[23] Aanvullend daarop gelden enkele speciale bepalingen voor Europol en Eurojust.[24]

Deze uitzondering is op zichzelf minder logisch. Uitgangspunt van artikel 286 van het (oude) EG-Verdrag was dat de regels die in de lidstaten gelden ook op de Unie zelf van toepassing zijn.[25] Belangrijker echter, de juridische reden voor een onderscheid tussen het natio-

20. Zie hierover ook de reeds genoemde mededeling van 25 januari 2012, COM (2012)9 def.

21. Art. 21 is niet nieuw; art. 13 van Richtlijn 95/46/EG is van vergelijkbare aard.

22. Nationale veiligheid moet worden onderscheiden van het veel ruimere begrip 'openbare veiligheid' dat de lidstaten de ruimte geeft afwijkingen van bepaalde verplichtingen uit de ontwerpverordening in te voeren, maar dat niet buiten de reikwijdte van de ontwerpverordening valt.

23. 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.

24. Besluit van de Raad van 6 april 2009 tot oprichting van de Europese politiedienst (Europol), *Pb. EU* 2009, L 121/37 (art. 27-35); Besluit van de Raad van 28 februari 2002, 2002/187/JBZ, betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken, *Pb. EG* 2002, L 63/1, gewijzigd bij Besluit 2009/426/JBZ van de Raad van 16 december 2008, *Pb. EU* 2009, L 138/14 (art. 14-25).

25. Dit uitgangspunt is niet meer expliciet verwoord in het verdrag zelf, aangezien met art. 16 VWEU de noodzaak voor een specifieke rechtsbasis voor gegevensbescherming door EU-instellingen is komen te vervallen.

nale niveau en de Unie zelf is vervallen, nu het instrument verordening is gekozen. Een verordening kan evengoed van toepassing zijn op de Unie zelf. Voorts is kritiek op deze uitzondering goed denkbaar: de Unie legt strenge wetgeving op aan de lidstaten maar ontziet zichzelf. De eigen instellingen blijven gebonden aan een veel globaler (en ook nog enigszins verouderd) wettelijk regime. De Commissie zal dan ook een voorstel presenteren om ook de instellingen zelf aan het nieuwe regime te binden. Een datum voor een dergelijk voorstel wordt echter niet genoemd.

De derde uitzondering betreft het Gemeenschappelijk buitenlands- en veiligheidsbeleid. Ook voor dit gebied schrijft het verdrag wetgeving voor, echter niet op grond van artikel 16 VWEU, maar op basis van artikel 39 EU waarbij het Europees Parlement niet als medewetgever optreedt.

Een volgende uitzondering is de verwerking door de autoriteiten van de lidstaten in de sfeer van het strafrecht. Voor dit terrein wordt als gezegd een richtlijn voorgesteld.

De laatste uitzondering is van geheel andere aard: het zogenoemde huishoudelijke gebruik van gegevens. Waar natuurlijke personen zonder commercieel doel gegevens verwerken in de persoonlijke sfeer, of in de sfeer van de eigen huishouding, geldt de verordening niet. Deze uitzondering bestaat reeds in het huidige rechtskader; alleen deze heeft nieuwe betekenis gekregen nu natuurlijke personen actief zijn in sociale online netwerken, zoals Facebook of Hyves, en daarbij gegevens van zichzelf, maar ook van anderen verwerken. Vaak gaat het daarbij alleen om gegevens van vrienden. Het is niet bij voorbaat evident waar de grens ligt van het begrip 'huishoudelijk gebruik', bijvoorbeeld in gevallen waar de kring van vrienden zo groot is (denk aan publieke personen) dat een uitzondering op de toepasselijkheid van de verordening niet gerechtvaardigd zou zijn.

Toepassing binnen de EU, maar ook daarbuiten

Artikel 3 lid 2 breidt de toepassing van de verordening uit naar bedrijven in derde landen die goederen en diensten aanbieden aan personen binnen de Europese Unie en naar bedrijven in derde landen die het gedrag van individuen observeren. Deze uitbreiding van het geografische toepassingsgebied is met name van belang op internet. Veel van de (grote) aanbieders op internet zijn niet, althans niet primair, in de Europese Unie gevestigd. Met het 'observeren van gedrag' wordt onder meer de praktijk bedoeld van zoekmachines die zoekgedrag van individuen registreren en bewaren en gebruiken voor bijvoorbeeld gerichte advertenties, en daar soms cookies voor plaatsen op computers van gebruikers.

Ten behoeve van de handhaafbaarheid van deze extraterritoriale toepassing zijn de betrokken bedrijven uit derde landen verplicht een vertegenwoordiger aan te wijzen binnen het grondgebied van de Unie (art. 25 van de ontwerpverordening).

In dit verband is ook hoofdstuk V van het voorstel van belang dat de doorgifte van persoonsgegevens *naar* derde landen reguleert. Aan die doorgifte worden eisen gesteld om te voorkomen dat het Europese regime kan worden ondermijnd wanneer organisaties gegevens overbrengen naar derde landen waar geen of onvoldoende bescherming wordt gegarandeerd. Ook het huidige wettelijk regime kent reeds een (vrij ingewikkelde) regeling voor doorgifte naar derde landen (zie in het bijzonder art. 25 en 26 van Richtlijn 95/46/EG).

Uitgangspunt is dat de doorgifte alleen plaats mag vinden naar landen die een adequaat niveau van bescherming bieden, min of meer gelijkwaardig aan het niveau binnen de EU zelf. Dit is voor de praktijk veel te beperkt[26] en daarom worden andere grondslagen geschapen voor doorgifte, zoals bindende bedrijfsvoorschriften of bepaalde contractuele bepalingen. Het stelsel voorziet ook in 'afwijkingen' die specifieke doorgiften moeten mogelijk maken, bijvoorbeeld om gewichtige redenen van algemeen belang. Het voorstel specificeert de huidige regels, maar is op dit punt niet wezenlijk nieuw.

Consolidatie van de bestaande beginselen

Hoofdstuk 2 van het voorstel consolideert de bestaande beginselen van gegevensverwerking. Kort gezegd, gegevens die voor een bepaald doel zijn verzameld mogen niet voor een ander, daarmee onverenigbaar doel worden gebruikt. Alleen de gegevens die nodig zijn voor het doel mogen worden verwerkt en gegevens moeten juist zijn en worden bijgewerkt. Rechtmatigheid, eerlijkheid en transparantie zijn andere belangrijke beginselen die de burger moeten beschermen.

De belangrijkste grond om gegevens te mogen verwerken is een ondubbelzinnige toestemming van de betrokkene. Het voorstel legt vast hoe die toestemming tot stand moet komen. Op internet heeft toestemming een nieuwe dimensie gekregen en hierover heeft veel discussie plaatsgevonden, met name over de vraag of iemand altijd actief toestemming moet verlenen (*opt in*) of dat het soms voldoende is als een website of een zoekmachine de gelegenheid biedt de verwerking te verbieden (*opt out*). De verordening lijkt vrij strenge eisen te stellen. Zo is volgens overweging 25 stilte of inactiviteit niet genoeg voor toestemming. Zij beëindigt de discussie echter niet. Kinderen onder de dertien jaar worden extra beschermd. De ouder of voogd moet toestemming verlenen. De verantwoordelijke gegevensverwerker moet deze toestemming verifiëren, met inachtneming van de beschikbare technologie. Het is interessant te zien hoe deze verplichting in de praktijk gaat werken, zeker nu een individu vaak met een simpele muisklik kan aangeven dat hij of zij een bepaalde leeftijd heeft bereikt.

Tot slot wijs ik er nog op dat de regeling voor gevoelige gegevens waarvoor extra strenge eisen gelden (zoals ras, etnische afkomst, godsdienst of gezondheid) is uitgebreid met genetische gegevens en bepaalde strafrechtelijke gegevens.

26. Slechts een beperkt aantal (westerse) derde landen biedt een dergelijk niveau van bescherming, terwijl persoonsgegevens over de gehele wereld worden uitgewisseld.

Versterking van de rechten van de betrokkene

Een van de pijlers van het stelsel van gegevensbescherming is dat het de betrokkene sterke rechten toekent, die als gezegd deels ook expliciet zijn genoemd in het Handvest Grondrechten. Deze rechten worden aanzienlijk verduidelijkt.

De introductie van een recht van de betrokkene om te worden 'vergeten' (*right of oblivion* of *droit de l'oublie*) heeft veel publiciteit gekregen, ook door de nadruk die Commissaris Reding hierop legt. Dit recht wordt in artikel 17 van de ontwerpverordening voorgesteld in combinatie met een recht om gegevens te laten wissen. Het recht is sterk bekritiseerd, omdat het in een internetomgeving (waar data zich niet op één plek, maar overal tegelijk bevinden) niet realistisch zou zijn. Daarom heeft de Commissie een pragmatische aanpak gekozen (zie in het bijzonder art. 17 lid 2) en dit recht geconcretiseerd in een zorgverplichting voor de verantwoordelijke om binnen het redelijke derden (zoals zoekmachines of *cloud providers*) te verzoeken gegevens te verwijderen. Dit lijkt minder ambitieus dan oorspronkelijk beoogd, namelijk iedere individu een effectief recht te geven om 'vergeten te worden' op internet, maar wellicht is deze aanpak effectiever.

Een andere noviteit is het recht van gegevensoverdraagbaarheid (art. 18). Dit recht houdt in dat een betrokkene het recht heeft een kopie te ontvangen van de gegevens die over hem verwerkt worden en over te stappen naar een andere aanbieder, zonder daarbij te worden belemmerd door de oorspronkelijke aanbieder. Dit recht is vooral bedoeld voor sociale netwerken en voor de relatie tussen een klant en een internetprovider.[27]

Een fundamentele verandering: de verantwoordingsplicht van bedrijven en overheden

Artikel 22 van het voorstel bepaalt dat verantwoordelijken (bedrijven, overheden maar ook *non profit* organisaties) passende maatregelen moeten nemen waarmee zij er niet alleen voor zorgen maar ook kunnen aantonen dat de verordening wordt uitgevoerd. Deze algemene verplichting moet er bijvoorbeeld toe leiden dat in de organisatie van een onderneming gegevensbescherming wordt ingebed en dat bedrijven openbaar verslag doen over hun beleid daarover. Op deze wijze wordt de primaire verantwoordelijkheid bij de betrokken bedrijven of organisaties gelegd. Waar overheden in een wereldwijde omgeving niet bij machte zijn naleving van wetgeving in detail te controleren, moeten de betrokken bedrijven of organisaties dat zelf doen op een wijze die past bij hun omvang en status.

De verplichting wordt uitgewerkt in een groot aantal meer specifieke regels, die soms minder streng zijn voor het midden- en kleinbedrijf (het voorstel hanteert op verschillende plekke een grens van 250 werknemers) en voor overheden. Deze specifieke regels – die soms in detail zijn neergelegd in het voorstel – hebben betrekking op zaken als *privacy by design* en *privacy by default*, het bewaren van documentatie over verwerkingen van persoonsgegevens, beveiliging, het verplichte uitvoeren van een privacy-effectbeoordeling voordat een systeem in werking wordt gesteld en de aanwijzing van een interne functionaris voor de gegevensbescherming die binnen een organisatie in de gaten houdt hoe de verordening wordt uitgevoerd.[28]

Toezichthoudende autoriteiten krijgen tanden en moeten samenwerken

In het arrest *Commissie/Duitsland*[29] heeft het Hof van Justitie strenge eisen gesteld aan de onafhankelijkheid van de onafhankelijke autoriteiten. Artikel 28 van Richtlijn 95/46/EG eist dat de autoriteiten hun taken vervullen in volledige onafhankelijkheid. Deze onafhankelijkheid sluit volgens het Hof van Justitie niet enkel elke beïnvloeding door de organen waarop toezicht wordt uitgeoefend uit, maar ook elk bevel of elke andere beïnvloeding van buitenaf, zij het rechtstreeks of indirect. De ontwerpverordening codificeert de eisen die het Hof van Justitie stelt en werkt deze uit (art. 47-49). De onafhankelijkheid brengt onder meer mee dat de autoriteiten over passende menselijke, technische en financiële middelen moeten beschikken.

Onafhankelijkheid is één, sterke taken en bevoegdheden is twee. Hier leidt de verordening tot een essentiële verandering met de bestaande situatie. De lidstaten moeten de autoriteiten de bevoegdheid geven bindende maatregelen op te leggen aan verwerkers (zoals een verbod gegevens te verwerken), schendingen van de verordening voor de rechter te brengen en administratieve boetes op te leggen (art. 51-54). Die boetes kunnen zeer hoog zijn (zie art. 79). Een overtreding die opzettelijk of uit nalatigheid is begaan kan worden bestraft met een boete tot € 1 miljoen of, in geval van een onderneming, tot 2% van de jaarlijkse wereldwijde omzet.

Het is goed te beseffen dat onder de huidige richtlijn de bevoegdheden van de nationale autoriteiten sterk uiteenlopen en dat in een aantal lidstaten harde bevoegdheden ontbreken.

Het is opmerkelijk dat in het voorstel de nationale autoriteiten niet alleen tot taak hebben de naleving van de verordening te controleren maar ook gehouden zijn een bijdrage te leveren aan de uniforme toepassing van de verordening in de hele Unie. Zij moeten met elkaar en met de Commissie samenwerken. Deze tweede taak geeft de autoriteiten een verantwoordelijkheid met EU-brede implicaties. Deze verantwoordelijkheid houdt onder meer in dat de autoriteiten ontwerpen van maatregelen aan een conformiteitstoetsing onderwerpen. Bovendien moeten ze samen werken in de op te richten European Data Protection Board (in het Nederlands: 'Europees Comité voor gegevensbescherming'; vermoedelijk echter zal de Engelse benaming de gangbare zijn).

27. Het recht dient (zie ook overweging 55) vooral om de controle van het individu over zijn gegevens te versterken en is enigszins vergelijkbaar met de nummerportabiliteit uit de telecommunicatiewetgeving.

28. Zie hfdst. IV van de ontwerpverordening.

29. HvJ EU 9 maart 2010, zaak C-518/07, *Europese Commissie/Bondsrepubliek Duitsland*, *Pb. EU* 2010, C 113, p. 3, in het bijzonder punt 30. Zie over deze zaak uitgebreid Kranenborg in *SEW* 2010, p. 419-423.

Deze Board is de opvolger van de Artikel 29 Werkgroep.[30]

Leidende autoriteit, conformiteit en European Data Protection Board (EDPB)

Een belangrijke vernieuwing is dat bij bedrijven die in meerdere lidstaten gevestigd zijn en dus in beginsel aan meerdere toezichthouders onderworpen zijn, er één autoriteit zal zijn die leiding geeft aan het toezicht. Ingevolge artikel 51 lid 2 jo. artikel 4(13) van het voorstel is dit de autoriteit van 'de belangrijkste vestiging'. Dit is in beginsel de autoriteit van het land van de vestiging waar de belangrijkste besluiten over de gegevensbescherming genomen worden. Deze vernieuwing heeft veel aandacht gekregen omdat deze '*one stop shop*' een aanzienlijke lastenverlichting moet meebrengen voor multinationals (al dan niet opererend vanuit derde landen). Waar deze ondernemingen nu vaak met verschillende autoriteiten (en verschillende regels) van doen hebben, hebben deze straks nog slechts te maken met één toezichthouder.

Toch wordt het idee van de '*one stop shop*' ook bekritiseerd, vooral van Franse zijde,[31] omdat het de afstand tussen de burger en de toezichthoudende autoriteit te zeer zou vergroten. Indien iemand een klacht heeft tegen een bedrijf dat in een andere lidstaat de belangrijkste vestiging heeft, wordt die klacht in beginsel behandeld door de autoriteit van laatstgenoemde lidstaat.

Tegen deze kritiek valt in te brengen dat ingevolge artikel 73 iedere betrokkene het recht heeft een klacht in te dienen bij de toezichthoudende autoriteit in het land waar hij of zij woont (en trouwens ook in andere landen). Belangrijker echter: de gedachte achter de constructie van een '*one stop shop*' is dat de leidende autoriteit het aanspreekpunt is voor de verantwoordelijke, maar besluiten niet alleen neemt. Hij doet dit in samenwerking met andere betrokken autoriteiten, al dan niet in het kader van de EDPB.

Dit brengt mij bij het stelsel van conformiteit[32] (art. 57-63). De nationale autoriteiten zijn verplicht bepaalde maatregelen met mogelijk aanzienlijke grensoverschrijdende effecten vóór vaststelling voor te leggen aan de Commissie en de EDPB.[33] Het belangrijkste type maatregelen waaraan valt te denken zijn handhavingsmaatregelen tegen bedrijven die grensoverschrijdend goederen of diensten aanbieden. Als voorbeeld in de discussie over het nut van dit stelsel wordt vaak Google Street View genoemd. Bij gebreke aan afstemming tussen de autoriteiten werd in de lidstaten zeer verschillend met deze dienst omgegaan.

De EDPB brengt over de maatregel die aan hem is voorgelegd advies uit aan de voorleggende autoriteit. Deze is gehouden het advies in aanmerking te nemen en te rapporteren aan de EDPB en de Commissie hoe het advies is uitgevoerd. De Commissie heeft ruime bevoegdheden in dit stelsel en kan ter verzekering van de correcte en consequente toepassing van de verordening ingrijpen in de procedure. De Commissie kan een advies vaststellen dat de betrokken autoriteit *zo veel mogelijk*[34] in aanmerking moet nemen; bovendien kan zij de vaststelling van een ontwerpbesluit schorsen als dat nodig is om uiteenlopende standpunten te verzoenen of om zelf een uitvoeringshandeling vast te stellen.

Het kan worden betwijfeld of dit ingrijpen van de Commissie in de besluitvorming van een onafhankelijke autoriteit in individuele gevallen verenigbaar is met de strenge vereisten die worden gesteld aan onafhankelijkheid.[35] Toegegeven, ingevolge artikel 17 lid 3 EU is ook de Commissie volledig onafhankelijk en mogen externe instructies niet worden aangenomen. Daar staat echter tegenover dat de Commissie in verschillende rollen zelf betrokken is bij de verwerking van persoonsgegevens en ook – net als iedere nationale overheid – politieke verantwoordelijkheid draagt.

Tot slot is aandacht voor de op te richten EDPB op zijn plaats (art. 64-72). De EDPB is als gezegd opvolger van de Artikel 29 Werkgroep en is te onderscheiden van de EDPS, de Europese toezichthouder. Ook de EDPB treedt onafhankelijk op en heeft als hoofdtaak zorg te dragen voor de consequente toepassing van de verordening. Naast de uitvoering van het boven omschreven stelsel van conformiteit is de EDPB vooral een adviesorgaan met een uitgebreide taakomschrijving.

Teneinde een goede uitvoering van de taken mogelijk te maken is ook een aantal institutionele voorzieningen getroffen. Er komt een presidium bestaande uit een vaste voorzitter en twee vicevoorzitters die voor een eenmaal verlengbare termijn van vijf jaar worden gekozen. De EDPS maakt deel uit van dit presidium, zo is de bedoeling. De EDPB krijgt bovendien een vast secretariaat met eigen taken. Dat secretariaat wordt verzorgd door de EDPS.

Rechtsmiddelen en sancties

Het voorstel bevat een reeks van rechtsmiddelen voor de burger (art. 73-77). Hij kan klagen bij de toezichthouder, hij kan beroep instellen tegen de toezichthouder en hij kan rechtstreeks naar de rechter stappen zonder tussenkomst van de toezichthouder. Belangrijke noviteiten zijn dat nu ook belangengroepen rechtsingang zullen hebben en dat een betrokkene in iedere lidstaat een klacht kan indienen bij de nationale autoriteit.

Opmerkelijk is artikel 74 lid 4: een individu kan vragen aan de autoriteit in de lidstaat waar hij verblijft om namens hem een beroep tegen een autoriteit van een

30. Overlegorgaan van de Europese privacytoezichthouders onder art. 29 van Richtlijn 95/46/EG.
31. Zie persbericht van de Commission nationale de l'information et des libertés (CNIL) van 26 januari 2012 en resoluties in dezelfde richting van de Assemblée nationale en de Senaat, te vinden op <www.cnil.fr>.
32. In de Engelse tekst wordt gesproken over '*consistency*', in het Frans en Duits over '*cohérence*' en '*Koherenz*'. Deze termen lijken mij beter de essentie weergeven dan 'conformiteit'.
33. Het stelsel is veel uitgebreider/genuanceerder dan ik hier beschrijf.
34. Let op de nuance. In de Engelse versie 'shall take *utmost* account', in het Frans 'tient le plus grand compte', in het Duits 'trägt so weit wie möglich Rechnung'. Hieruit blijkt evident dat het advies van de Commissie een sterkere mate van binding heeft dan het advies van de EDPB.
35. Ingevolge art. 8 van het Handvest Grondrechten en zoals uitgelegd in *Commissie/Duitsland*, zie voetnoot 29. Zie ook EDPS-advies van 7 maart 2012, geciteerd in voetnoot 6, par. 248-255.

andere lidstaat in te stellen. Het is echter niet duidelijk hoe de geschillen die hieruit voort kunnen komen zich verhouden tot de verplichting van de autoriteiten om samen te werken. Een centraal element van het voorstel is immers dat autoriteiten nauw met elkaar moeten samenwerken in zaken met grensoverschrijdende gevolgen.

Tot slot zij nog gewezen op het voorgestelde sanctiemechanisme. Ik meldde al in de context van de aanscherping van de bevoegdheden van de autoriteiten dat de hoogte van de administratieve sancties behoorlijk kan oplopen. Artikel 79 lid 2 bepaalt dat bij het vaststellen van de sanctie rekening wordt gehouden met onder meer de aard, de ernst en de duur van de inbreuk. Dit lijkt erop dat de autoriteiten een discretionaire ruimte hebben bij het vaststellen van sancties. Echter, die ruimte ontbreekt bij overtredingen die opzettelijk zijn gepleegd of uit nalatigheid. De tekst van artikel 79 (lid 4-6) wijst erop dat in die gevallen automatisch een sanctie moet worden opgelegd, die als gezegd erg hoog kan uitvallen. De vraag kan worden gesteld of enige flexibiliteit niet te prefereren is.[36]

Europeesrechtelijke vragen

De voorgestelde verordening is niet alleen interessant omdat de Commissie ernaar streeft een effectief stelsel van gegevensbescherming te scheppen dat over langere tijd werkzaam moet zijn in een turbulente, snel veranderende omgeving van ICT en wereldwijd gegevensverkeer. Het roept ook meer algemene vragen op die voor de Europees jurist uitdagend zijn en die vermoedelijk in de wetgevingsprocedure bij Raad en Parlement een rol zullen spelen. Ik noem er een paar:

1. De Commissie kiest voor het instrument van een gedetailleerde verordening op een onderwerp dat ingrijpt in brede terreinen van nationaal recht. De coexistentie tussen Europees en nationaal recht is niet evident. In hoeverre kunnen de lidstaten de verordening aanvullen? Een voorbeeld: artikel 14 lid 1 stelt dat de verantwoordelijke *ten minste* de volgende informatie aan een betrokkene moet verstrekken. Mogen de lidstaten in specifieke wetgeving de lijst met informatie-elementen aanvullen?
2. De verordening beoogt een fundamenteel recht te beschermen. Gevolg zou kunnen zijn dat de bescherming in zekere mate wordt onttrokken aan het nationale (constitutionele) recht en de nationale (constitutionele) rechter. In Duitsland heeft dit tot de vraag geleid of het Bundesverfassungsgericht zijn taak nog wel volledig kan uitvoeren[37] en of daarmee de verordening niet strijdt met de Duitse Grondwet.
3. Dit grondrecht wordt op EU-niveau beschermd, terwijl de bescherming van andere grondrechten aan de nationale wetgever blijft. Hoe kan de voorrang van het Unierecht worden verzoend met de noodzaak botsende grondrechten af te wegen? Artikel 80 van het voorstel beoogt dit te regelen voor de vrijheid van meningsuiting, doch bij andere grondrechten geeft het voorstel geen antwoord.
4. De autoriteiten zijn verplicht met elkaar samen te werken en rekening te houden met adviezen van de EDPB en de Commissie. Anderzijds zijn het nationale bestuursorganen die onafhankelijk zijn en wier besluiten slechts onderworpen zijn aan toezicht door de nationale rechter. Hoe kan de onafhankelijkheid van de nationale autoriteiten worden verzoend met het voorgestelde stelsel van conformiteit, waarin de Commissie bovendien nog kan ingrijpen?
5. Is er rechtsbescherming tegen activiteiten van de EDPB? De Commissie heeft dit opgelost door aan de EDPB geen besluitvormende bevoegdheid toe te kennen. Niettemin moeten de adviezen van de EDPB een grote rol gaan spelen en aanzienlijke consequenties hebben voor betrokken bedrijven en burgers.

Deze opsomming is verre van volledig maar strekt ertoe een eerste illustratie te geven van de vragen die het voorstel oproept. Het voorstel heeft een dermate ingrijpend karakter dat ik ervan uitga dat het nog tot veel debat aanleiding zal geven, naar ik hoop ook buiten de kringen van de specialisten op het gebied van de gegevensbescherming.

In ieder geval heeft de Commissie voor een ambitieuze aanpak gekozen. Met het voorstellen van een vrij gedetailleerde verordening wordt stevig ingegrepen in nationale wetgeving en structuren. Naar mijn oordeel rechtvaardigt het onderwerp – alleen al om op internet effectief een grondrecht te beschermen en tegelijkertijd Europa meer concurrerend te maken – deze aanpak. Een lichte aanpassing van het bestaande stelsel is niet voldoende en daar heeft de Commissie ook niet voor gekozen.

36. Zie ook EDPS-advies van 7 maart 2012, geciteerd in voetnoot 6, par. 284-290.
37. Rechter Massing van het Bundesverfassungsgericht in Süddeutsche Zeitung, 'Ein Abschied von den Grundrechten', 9 januari 2012. Hij stelt voornamelijk dat het recht van iedere burger om een *Verfassungsbeschwerde* in te dienen bij het Duitse Constitutionele Hof aan waarde verliest.