Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie : over de openbaarheid van persoonsgegevens

Kranenborg, H.R.

3 Bescherming van persoonsgegevens in de EU en de Raad van Europa

> '[I]ncreased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data'.[1]

3.1 INLEIDING

De eerste regels over gegevensbescherming werden opgesteld na de introductie van de computer, die het mogelijk maakte om gegevens automatisch te verwerken. De verwerking van gegevens moest aan voorwaarden worden onderworpen, zodat onrechtmatige afbreuk aan het privé-leven van de burgers werd vermeden. Uiteraard namen de mogelijkheden om gegevens (automatisch) te verwerken enorm toe door de zeer snelle ontwikkeling van informatietechnologie in de afgelopen vijftien jaar. Gegevens waren steeds makkelijker en beter op te slaan, het werd eenvoudiger om gegevens te koppelen of tussen verschillende personen en instanties uit te wisselen. Overheid en burger maakten ook steeds meer gebruik van deze mogelijkheden. Vooral sinds de aanslagen van 11 september in New York zijn overheden er bijvoorbeeld meer en meer toe overgegaan om voor de opsporing van (potentiële) misdadigers gegevens van burgers vast te leggen en te koppelen. Deze ontwikkelingen legden druk op de privacybescherming van burgers. Niet voor niets wees het EHRM er in 2004 in het weergegeven citaat op dat bij al deze ontwikkelingen extra waakzaamheid betracht moet worden ten aanzien van de bescherming van het privéleven.

In Europa is de bescherming van persoonsgegevens steeds meer van het nationale naar het Europese niveau getild. Zowel binnen de Raad van Europa als de EU zijn bindende rechtsinstrumenten over de bescherming van persoonsgegevens aangenomen. Uniforme regels in de Europese landen moesten leiden tot een stabiel beschermingsniveau voor de burger, maar ook voor een vrije grensoverschrijdende uitwisseling van gegevens.

Het is een stuk lastiger om de regels over de bescherming van persoonsgegevens binnen de EU weer te geven dan de regels over toegang tot documenten. Geldt voor toegang tot documenten binnen de gehele EU het regime van de Eurowob, voor bescherming van persoonsgegevens ontbreekt een uniform

---

1 EHRM 24 juni 2004, *Von Hannover t. Duitsland*, r.o. 70.

kader. Er zijn verschillende regels van kracht in de eerste pijler en in de tweede en derde pijler. Ook de relatie tussen deze rechtsinstrumenten en de regels die binnen de Raad van Europa zijn opgesteld, is van een andere orde. Liep de EU voor op de Raad van Europa bij toegang tot documenten, bij bescherming van persoonsgegevens is dit andersom. De verschillende regels over gegevensbescherming in de EU zijn namelijk sterk geïnspireerd door het Verdrag van Straatsburg dat binnen de Raad van Europa is gesloten.[2] In dit verdrag zijn regels over de bescherming van persoonsgegevens neergelegd. Ook de jurisprudentie van het EHRM onder artikel 8, waarin het recht op privacy is neergelegd, heeft directe invloed op deze regels van de EU.

Een ander verschil tussen toegang tot documenten en bescherming van persoonsgegevens in de EU is dat de eerste communautaire stappen ten aanzien van de bescherming van persoonsgegevens genomen werden op basis van de bevoegdheid om de totstandkoming van de interne markt te bewerkstelligen. Een vrij verkeer van gegevens behoorde tot deze interne markt. De eerste EG-regelgeving op dit gebied is daarom gericht tot de lidstaten.[3] Pas later werden dwingende regels over bescherming van persoonsgegevens aan de communautaire instellingen zelf opgelegd.[4] De Eurowob was uiteraard alleen en direct tot de instellingen van de EU gericht.

In dit hoofdstuk worden de gegevensbeschermingsregels binnen de EU en de Raad van Europa in kaart gebracht. De nadruk zal liggen op regelgeving die van belang is voor de verwerking van persoonsgegevens door de instellingen en organen van de EU. Relevante regels over gegevensverwerking op nationaal niveau worden genoemd, maar verder niet in detail besproken. In § 3.2 wordt een overzicht gegeven van de ontwikkeling van de regels over bescherming van persoonsgegevens binnen de Raad van Europa en de EG/EU. Daarna volgt in § 3.3 een inhoudelijke bespreking van het binnen de Raad van Europa gesloten Verdrag van Straatsburg en de relevante jurisprudentie van het EHRM onder artikel 8 EVRM. Vervolgens wordt in § 3.4 bekeken wat de inhoud is van het huidige regime in de *eerste pijler* van de EU. De schaarse jurisprudentie van het HvJ over bescherming van persoonsgegevens wordt daarbij betrokken. In § 3.4 wordt vervolgens ook beschreven welke regels van toepassing zijn in de *tweede en derde pijler*. Daarbij wordt ingegaan op de belangrijkste verschillen met de bescherming van persoonsgegevens onder de eerste pijler.

---

2 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Verdrag van Straatsburg), Straatsburg 28 januari 1981 (*European Treaty Series*, Nr. 108).

3 Zie richtlijn 95/46 van het Europees Parlement en de Raad van 24 oktober 1995 (*Pb. EG* 1995, L 281/31).

4 Zie verordening 45/2001 van het Europees Parlement en de Raad van 18 december 2000 (*Pb. EG* 2001, L 8/1).

3.2 HISTORISCH OVERZICHT[5]

In Europa hebben drie organisaties een belangrijke rol gespeeld bij de ontwikkeling van de regels over bescherming van persoonsgegevens: de Raad van Europa, de OESO en de E(E)G/EU. Alledrie wilden zij een uniforme toepassing van het recht op bescherming van persoonsgegevens garanderen. Uiteraard om de burger te beschermen, maar ook om een onbelemmerd grensoverschrijdend verkeer van persoonsgegevens mogelijk te maken. Het streven naar een vrij verkeer van gegevens heeft per organisatie een verschillende achtergrond die correspondeert met de algemene grondslagen van deze drie organisaties. Binnen de Raad van Europa werd het vrij verkeer van informatie/persoonsgegevens als beginsel afgeleid uit artikel 10 EVRM, terwijl binnen de OESO dit vrij verkeer meer als instrument diende om economische en sociale ontwikkeling te stimuleren.[6] Binnen de E(E)G en de EU, tenslotte, maakte het vrij verkeer van persoonsgegevens onderdeel uit van het streven naar een interne markt en later ook van het streven naar een ruimte van vrijheid, veiligheid en rechtvaardigheid.

3.2.1 De Raad van Europa en de OESO

De allereerste internationale stappen op het gebied van de gegevensbescherming werden gezet binnen de Raad van Europa. In 1968 verzocht de Parlementaire Vergadering het Comité van Ministers te onderzoeken of het EVRM, vooral artikel 8, en de wetgeving van de verdragsstaten het privé-leven voldoende bescherming boden ten opzichte van de moderne wetenschap en

---

5 Zie voor een uitgebreider historisch overzicht A.C.M. Nugter, *Transborder flow of personal data within the EC*, Deventer 1990, Kluwer (diss. Utrecht); L.F.M. Verhey, 'Europese integratie en privacy-bescherming', in M.C. Burkens & H.R.B.M. Kummeling (eds), *EG en Grondrechten*, Zwolle 1993, W.E.J. Tjeenk Willink, p. 219-258; I. Harden, 'Citizenship and Information', *EPL* 2001, p. 165-193; P. de Hert, 'European Data Protection and E-Commerce: Trust Enhancing?', in J.E.J. Prins e.a. (eds), *Trust in Electronic Commerce, The Role of Trust from a Legal, an Organizational and a Technical Point of View*, Den Haag 2002, Kluwer Law International, p. 171-229 en F.A.M. van de Klaauw-Koops & J.E.J. Prins, 'Internationale privacyregulering: belangen, problemen en mogelijkheden', in J.E.J. Prins & J.M.A. Bervkens (eds), *Privacyregulering in theorie en praktijk*, Deventer 2002, Kluwer, p. 485-510. Zie ook D. Korff, *Data Protection Laws in the European Union*, New York 2005, Federation of European Direct Marketing & Direct Marketing Association.

6 Zie respectievelijk paragraaf 19 van het *Explanatory Report* bij het Verdrag van Straatsburg (*European Treaty Series*, Nr. 108, te vinden op http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm) en de *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* van 23 september 1980 (te vinden via http://www.oecd.org). Op de verhouding tussen artikel 8 en artikel 10 EVRM wordt in § 4.3.7 nader ingegaan.

technologie.[7] Dit leidde in 1973 en 1974 tot twee resoluties van het CvM; één voor de private sector en één voor de publieke sector.[8] Deze (niet bindende) resoluties dienden als leidraad voor de nationale regels over gegevensbescherming. Binnen de Raad van Europa werd al snel geconstateerd dat een dwingend uniform beschermingsniveau een praktische noodzakelijkheid was. Verschil in nationale wetgeving stond het beginsel van 'free international flow of information' in de weg.[9] Dit beginsel werd afgeleid uit artikel 10 EVRM. In 1976 werd door het CvM een Comité van Experts op het gebied van informatieverwerking samengesteld met als opdracht het voorbereiden van een tekst voor een verdrag over de bescherming van persoonsgegevens. Dit Comité moest nauw samenwerken met de OESO. Deze organisatie, die ook een aantal niet-Europese landen tot zijn leden kan rekenen, was inmiddels namelijk ook actief op het gebied van de informatieverwerking. Aan de ene kant onderschreef de OESO de nationale inspanningen om schendingen van een fundamenteel mensenrecht te voorkomen, aan de andere kant voorzag (ook) zij een potentiële belemmering van het vrije grensoverschrijdende verkeer van persoonsgegevens.[10] Parallel en samenwerkend leidde deze inspanningen binnen de Raad van Europa tot het eerder genoemde Verdrag van Straatsburg (1981) en binnen de OESO tot een aanbeveling (1980).[11] Het Verdrag van Straatsburg trad na de vijfde ratificatie (van Duitsland) op 1 oktober 1985 inwerking en is inmiddels ondertekend en geratificeerd door 38 landen, waaronder alle lidstaten van de EU.[12] Ook staten die geen lid waren van de Raad van Europa konden partij worden bij het Verdrag. In 1999 werd dit met een amendement ook mogelijk gemaakt voor de EG.[13]

---

7 Informatie in deze alinea is deels afkomstig uit het *Explanatory Report* bij het Verdrag van Straatsburg.

8 Resolutie (73)22 van het Comité van Ministers van 26 september 1973 en resolutie (74)29 van het Comité van Ministers van 20 september 1974 (beide te vinden via http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/).

9 Paragraaf 9 van het *Explanatory Report* bij het Verdrag van Straatsburg.

10 Informatie afkomstig uit het voorwoord bij de *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* van 23 september 1980 (te vinden via http://www.oecd.org). De OESO bestond in 1980 uit 24 landen: Australië, België, Canada, Denemarken, Duitsland, Engeland, Finland, Frankrijk, Griekenland, IJsland, Ierland, Italië, Japan, Luxemburg, Nederland, Nieuw Zeeland, Noorwegen, Oostenrijk, Portugal, Spanje, Turkije, Verenigde Staten, Zweden en Zwitserland. Later zijn nog zes landen toegetreden: Hongarije, Korea, Mexico, Polen, Slowakije en Tsjechië.

11 De in de vorige voetnoot genoemde *Guidelines* vormden de aanbeveling van de OESO.

12 Zie http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=&CL=ENG voor een ratificatieoverzicht.

13 Zie respectievelijk artikel 23 van het Verdrag van Straatsburg en het amendement van 15 juni 1999 (te vinden via http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents). Overigens zijn op het moment van schrijven enkel leden van de Raad van Europa tot het Verdrag toegetreden en heeft de EG nog geen gebruik gemaakt van de toetredingsmogelijkheid.

Na het vaststellen van de Verdragstekst in 1981, verschenen er dertien relevante aanbevelingen van het CvM. Naast de algemene beginselen uit het Verdrag van Straatsburg vond het CvM het naderhand noodzakelijk om ten aanzien van specifieke sectoren aanbevelingen uit te vaardigen. Zo verschenen er aanbevelingen over de bescherming van persoonsgegevens met het oog op de sociale zekerheid, het gebruik van persoonsgegevens door de politie, de doorgifte van persoonsgegevens door publieke instanties aan derden, de bescherming van persoonsgegevens op het gebied van de telecommunicatie en de bescherming van privacy op het Internet.[14]

In november 2001 werd een protocol bij het Verdrag van Straatsburg opengesteld voor ondertekening. Het protocol droeg de verdragsstaten op om autoriteiten in het leven te roepen die zouden toezien op de naleving van de bepalingen uit het Verdrag van Straatsburg.[15] Ook waren in dit protocol regels opgenomen over de doorgifte van persoonsgegevens aan derde landen.

Ook binnen de OESO werd nog een aantal documenten over bescherming van persoonsgegevens aangenomen. Zo verscheen in 1985 een extra verklaring over de bescherming van persoonsgegevens en het grensoverschrijdende gegevensverkeer, werd in 1998 een verklaring aangenomen over de bescherming van privacy in relatie tot mondiale netwerken en verschenen in 2002 (nieuwe) richtlijnen voor de *Security of Information Systems and Networks*.[16]

Sinds de vraag van de Parlementaire Vergadering aan het CvM in 1968 heeft artikel 8 EVRM via de jurisprudentie van het EHRM (en de voormalige ECRM) voor de bescherming van persoonsgegevens aan belang gewonnen. Dit wordt in § 3.3.2 besproken.

---

14 Zie respectievelijk aanbeveling R(86)1 van het Comité van Ministers van 23 januari 1986, aanbeveling R(87)15 van het Comité van Ministers van 17 september 1987, aanbeveling R(91)10 van het Comité van Ministers van 9 september 1991, aanbeveling R(95)4 van het Comité van Ministers van 7 februari 1995 en aanbeveling R(99)5 van het Comité van Ministers van 23 februari 1999 (alle te vinden via http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents). Aanbeveling R(91)10 komt in hoofdstuk 9 nog ter sprake.

15 *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows*, Straatsburg 8 november 2001 (*European Treaty Series*, Nr. 181). Dit protocol trad na de vijfde ratificatie in werking op 1 juli 2004. Momenteel hebben zestien landen, waaronder dertien lidstaten van de EU, het protocol geratificeerd. Zie http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG voor een ratificatieoverzicht.

16 Zie respectievelijk *Declaration on Transborder Data Flows* van 11 april 1985, *Declaration on the Protection of Privacy on Global Networks*, aangenomen door de ministers tijdens een congres in Ottawa, 7-9 oktober 1998 en *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, aangenomen als aanbeveling van de Raad op 25 juli 2002 (alle te vinden via http://www.oecd.org).

3.2.2 De E(E)G

Bij de werkzaamheden van het Comité van Experts die leidden tot het Verdrag van Straatsburg was ook een vertegenwoordiger van de EEG betrokken. Toen de tekst van het Verdrag van Straatsburg werd vastgesteld, riep de Europese Commissie de lidstaten van de EEG op het Verdrag te ratificeren.[17] De Commissie meende dat een apart initiatief in het kader van de EG niet nodig was, maar behield zich – voor het geval de lidstaten niet tot ratificatie binnen een redelijke termijn overgingen – het recht voor om op basis van het EEG-Verdrag eigen regelgeving op te stellen. Toen bleek dat sommige lidstaten weinig haast maakten met het ratificeren van het Verdrag van Straatsburg, kwam de Commissie in 1990 met een voorstel voor een richtlijn over het vrij verkeer van persoonsgegevens.[18] Deze richtlijn was gebaseerd op de bevoegdheid van de EG zoals neergelegd in artikel 100A EEG-Verdrag (nu artikel 95 EG-Verdrag) om regels te stellen om de instelling en de werking van de interne markt te verwezenlijken. Na veel discussie werd pas op 24 oktober 1995 richtlijn 95/46 aangenomen.[19] Binnen drie jaar moesten de lidstaten de bepalingen in nationale wetgeving hebben omgezet.[20] Dit lukte alleen Griekenland, Italië en Zweden.[21]

De richtlijn stelde niet alleen inhoudelijk eisen aan de nationale wetgeving, lidstaten moesten ook een nationale toezichthoudende instantie in het leven roepen.[22] Daarnaast werd op grond van artikel 29 van de richtlijn op Europees niveau een werkgroep opgericht voor de bescherming van personen in verband met de verwerking van persoonsgegevens.[23] Deze groep, ook wel de 'Artikel 29 Groep', zou bestaan uit vertegenwoordigers van de nationale toezichthoudende autoriteiten. De Artikel 29 Groep was een adviesorgaan voor de Commissie, maar kon ook uit eigen beweging aanbevelingen doen.[24] Naast

17 Aanbeveling 81/679/EEG van de Europese Commissie van 29 juli 1981 (*Pb. EG* 1981, L 246/31).

18 Voorstel voor een richtlijn van de Raad van 13 september 1990 (COM(90)314 def., *Pb. EG* 1990, C 277/3).

19 Zie hierover Van de Klaauw-Koops & Prins 2002, p. 499. Zie over de voorstellen voor de richtlijn ook B.J. Boswinkel, 'De privacyrichtlijn begrensd', *SEW* 1993, p. 550- 592.

20 Zie artikel 32 lid 1 Richtlijn 95/46.

21 Zie http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm voor een overzicht. Op 11 januari 2000 leidde de Commissie op basis van artikel 226 EG-Verdrag voor het HvJ inbreukprocedures in tegen Frankrijk, Luxemburg, Nederland, Duitsland en Ierland. In oktober 2001 werd Luxemburg door het HvJ veroordeeld wegens niet-omzetting van richtlijn 95/46. Zie HvJ EG 4 oktober 2001, *Commissie tegen Luxemburg*, C-450/00, *Jur.* 2001, p. I-7069. De procedures tegen de overige landen werden na bepaalde toezeggingen beëindigd.

22 Zie artikel 28 Richtlijn 95/46.

23 Zie artikel 29 Richtlijn 95/46.

24 Zie artikel 30 Richtlijn 95/46 voor de taken van de Artikel 29 Groep. Zie voor een overzicht van de activiteiten http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

deze Artikel 29 Groep werd er een Comité opgericht samengesteld uit vertegenwoordigers van de lidstaten, dat op verzoek de Commissie advies kon geven.[25]

Richtlijn 95/46 beoogde harmonisatie van nationale wetgeving. Het besef dat ook instellingen van de EG gebonden moesten zijn aan regels over bescherming van persoonsgegevens werd geformaliseerd door de opname van artikel 286 in het EG-Verdrag, na het inwerkingtreden van het Verdrag van Amsterdam.[26] In dit artikel worden met ingang van 1 januari 1999 de besluiten van de Gemeenschap over de bescherming van persoonsgegevens van toepassing verklaard op de instellingen en organen die op grond van het EG-Verdrag waren opgericht. Met 'besluiten' werd gedoeld op richtlijn 95/46 en richtlijn 97/66 over de verwerking van persoonsgegevens in de telecommunicatiesector.[27] In het tweede lid van artikel 286 is bepaald dat vóór 1 januari 1999 door de Raad via de co-decisie procedure een onafhankelijk controleorgaan zou moeten zijn ingesteld voor toezicht op naleving van de regels door de instellingen en organen van de Gemeenschap.

De communautaire instellingen zelf bleken ook moeite te hebben met de gestelde deadline: pas op 18 december 2000 werd verordening 45/2001 aangenomen. In deze verordening werden in de eerste plaats de bepalingen van (met name) richtlijn 95/46 overgezet om ze van toepassing te laten zijn op de Europese instanties. In de tweede plaats werd een onafhankelijke toezichthoudende autoriteit ingesteld: de Europese toezichthouder voor gegevensbescherming (EDPS).[28] Het statuut van deze toezichthouder moest echter nog per apart besluit van het Europees Parlement, de Raad en de Commissie worden vastgesteld. Dat gebeurde op 1 juli 2002.[29] Bijna anderhalf jaar na die datum, op 22 december 2003, werd officieel de toenmalige voorzitter van het Nederlandse College Bescherming Persoonsgegevens – Peter Hustinx – benoemd tot de eerste Europese toezichthouder.[30] In januari 2004 startte hij zijn werkzaamheden.[31]

Ten aanzien van de verwerking van persoonsgegevens in de telecommunicatiesfeer werd op 15 december 1997 de genoemde richtlijn 97/66 aangenomen.

---

25 Zie artikel 31 Richtlijn 95/46.

26 Bij de vaststelling van richtlijn 95/46 verbonden de Commissie en de Raad zich ertoe de regels van de richtlijn in acht te nemen. Ook riepen zij de overige EG-instanties op hetzelfde te doen. Zie hierover het advies van het ECOSOC over het voorstel voor verordening 45/2001 (*Pb. EG* 2000, C 51/48), para. 1.3.

27 Dit blijkt uit considerans nr. 5 van verordening 45/2001. Zie richtlijn 97/66 van het Europees Parlement en de Raad van 15 december 1997 (*Pb. EG* 1998, L 24/1).

28 Zie artikel 41-48 Verordening 45/2001. Zie over de EDPS uitgebreid H. Hijmans, 'The European data protection supervisor: the institutions of the EC controlled by an independent authority', *CMLRev.* 2006, p. 1313-1342.

29 Besluit 1247/2002 van het Europees Parlement, de Raad en de Commissie (*Pb. EG* 2002, L 183/1).

30 Besluit 2004/55 van het Europees Parlement en de Raad (*Pb. EG* 2004, L12/47).

31 De EDPS is gevestigd in Brussel. De website is te vinden op http://www.edps.europa.eu.

Deze werd, gezien de technologische ontwikkelingen in de elektronische communicatie, op 12 juli 2002 vervangen door richtlijn 2002/58.[32]

In het Grondrechtenhandvest uit 2000 werd naast een artikel over de bescherming van privacy (artikel 7), onder het kopje 'vrijheden' een apart artikel toegevoegd over de bescherming van persoonsgegevens (artikel 8):

> 1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
> 2. Deze 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. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
> 3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.[33]

Net als bij het recht op toegang tot documenten, was in de Europese Grondwet een sterkere verankering van het recht op bescherming van persoonsgegevens in het primaire recht voorzien. Niet alleen kreeg het recht een prominentere plek, ook het recht op bescherming van persoonsgegevens kwam door de opname van het Grondrechtenhandvest twee maal voor in de tekst van de Grondwet.[34] Overigens zou met de Grondwet door het opheffen van de drie pijler structuur een uniformer kader voor de bescherming van persoonsgegevens voor de gehele EU zijn gecreëerd. Zover is het echter nog niet.

Hieronder volgt een paragraaf over de gegevensbeschermingsregels in de ruimte van vrijheid, veiligheid en rechtvaardigheid, waarvan de rechtsgrondslag zowel in de eerste als de derde pijler ligt.

3.2.3 De EU: de ontwikkeling van een ruimte van vrijheid, veiligheid en rechtvaardigheid[35]

In het Verdrag van Amsterdam is het streven naar een ruimte van vrijheid, veiligheid en rechtvaardigheid toegevoegd aan de doelstellingen van de Unie.[36] Het tot stand brengen van deze ruimte impliceerde gemeenschappelijke regels voor immigratie en asiel en verbeterde politiële en justitiële samenwerking. Het gebruik van persoonsgegevens speelde daarbij in toenemende mate een rol. Dit ging zelfs zover dat het zwaartepunt van de interesse voor de verwerking van persoonsgegevens verschoof van de totstandbrenging van

---

32 Richtlijn 2002/58 van het Europees Parlement en de Raad (*Pb. EG* 2002, L 201/37).

33 In hoofdstuk 4 wordt uitgebreid ingegaan op de verhouding tussen privacybescherming en bescherming van persoonsgegevens.

34 Zie over het recht op bescherming van persoonsgegevens in de Europese Grondwet uitgebreid § 6.3.2.

35 Zie over de ruimte van vrijheid, veiligheid en rechtsvaardigheid ook R. Barents, 'De denationalisering van het strafrecht', *SEW* 2006, p. 358-374.

36 Zie artikel 2 vierde streepje EU-Verdrag.

de interne markt, zoals in de vorige subparagraaf beschreven, naar het streven naar de ruimte van vrijheid, veiligheid en rechtvaardigheid. Dit kwam onder andere tot uiting in de verplaatsing in maart 2005 van de verantwoordelijkheid voor deze bescherming van de Commissaris voor de Interne Markt, naar de Commissaris voor vrijheid, veiligheid en rechtvaardigheid.[37]

De bevoegdheid om voor de ruimte van vrijheid, veiligheid en rechtvaardigheid regels te stellen is verdeeld over de eerste en de derde pijler van de Unie. Deze constructie levert voor de bescherming van persoonsgegevens soms gecompliceerde situaties op. Deze gecompliceerde constructie volgt uit de oorsprong van de regels. Deze lag namelijk buiten het institutionele kader van de toenmalige EEG.

Op 14 juni 1985 besloten België, Duitsland, Frankrijk, Luxemburg en Nederland een ruimte zonder binnengrenzen te creëren. Deze overeenkomst stond bekend als het 'akkoord van Schengen'.[38] De ruimte zonder binnengrenzen hield een nauwe samenwerking in ten aanzien van de controle van de buitengrenzen. Door het wegvallen van de binnengrenzen ontstond een ruimte van vrijheid, waardoor kansen werden gecreëerd die tot economische verbetering moesten leiden. Maar een ruimte zonder binnengrenzen zou ook ongewenste consequenties kunnen hebben, vooral met betrekking tot criminaliteit. Om die reden gingen de voorstellen voor afschaffing van de binnengrenzen gepaard met regels over samenwerking op politieel en justitieel gebied. In 1990 werd het akkoord van Schengen door middel van de Schengen-uitvoeringsovereenkomst (SUO) geïmplementeerd.[39] Bij de inwerkingtreding van deze overeenkomst in 1995 was het aantal deelnemende landen inmiddels uitgegroeid tot tien. In 1996 waren, met uitzondering van Denemarken, Ierland en het Verenigd Koninkrijk, alle landen van de EU partij bij de overeenkomst. Een van de belangrijkste instrumenten om het Schengen-gebied tot stand te brengen, was het instellen van een Schengen Informatie Systeem (SIS) waarmee op gemakkelijke wijze informatie (persoonlijke gegevens) kon worden uitgewis-

37 Zie hierover een nieuwsbericht van de Commissie van 16 maart 2005 (te vinden via http://ec.europa.eu/justice_home/news/intro/news_intro_en.htm). Overigens werd buiten het kader van de EU op 27 mei 2005 het Verdrag van Prüm gesloten tussen België, Duitsland, Frankrijk, Luxemburg, Nederland, Oostenrijk en Spanje. In dit Verdrag, dat ook wel Schengen III wordt genoemd, werden afspraken gemaakt voor samenwerking in de strijd tegen grensoverschrijdende criminaliteit. Tijdens de JBZ-Raad van 12 en 13 juni 2007 werd besloten essentiële delen uit het Verdrag van Prüm in EU recht om te zetten. Zie hierover http://euobserver.com/9/24244/?rk=1. Zie over het Verdrag van Prüm http://www.euractiv.com/Article?tcmuri=tcm:29-152252-16&type=Analysis en M.G.W. den Boer, 'Schengen III: the show must go on', *SEW* 2006, p. 316-322.

38 De tekst van het akkoord van Schengen van 14 juni 1985 is te vinden in *Pb. EG* 2000, L 239/13.

39 De tekst van de Schengen-uitvoeringsovereenkomst van 19 juni 1990 is te vinden in *Pb. EG* 2000, L 239/19. Zie over de privacyimplicaties van de Schengenovereenkomst L.F.M. Verhey, 'Privacy aspects of the Convention Applying the Schengen Agreement', in H. Meijers e.a. (eds), *Schengen*, Leiden 1992, St. NJCM-Boekerij, p. 110-134.

seld. Dit informatiesysteem moest zowel de uniforme controle van de buitengrenzen dienen, als de samenwerking op politieel en justitieel terrein. Het systeem bestond uit nationale systemen, de zogenaamde N-SIS, en een centraal systeem, het C-SIS.

Via een speciaal protocol bij het Verdrag van Amsterdam werd het omvangrijke Schengen-acquis uiteindelijk geïncorporeerd in het EG en EU-Verdrag.[40] Het verdrag van Amsterdam formuleerde zoals gezegd een nieuwe doelstelling voor de EU: het handhaven en ontwikkelen van een ruimte van vrijheid, veiligheid en rechtvaardigheid. Een globale scheiding tussen vrijheid enerzijds en veiligheid en rechtvaardigheid anderzijds werd gemaakt door een splitsing van de rechtsgrondslag van de verschillende regels. De regels over vrijheid, meer in het bijzonder visa, asiel en immigratie, kregen de voornaamste basis in het EG-Verdrag (titel IV). De regels over veiligheid en rechtvaardigheid vormden de derde pijler van de Unie, de politiële en justitiële samenwerking (titel VI van het EU-Verdrag).[41] De politiële en justitiële samenwerking leidde tot twee specifieke derde pijler organen: Europol en Eurojust.[42] In het EU-Verdrag wordt de bescherming van persoonsgegevens expliciet genoemd in de bepalingen over de politiële samenwerking. Volgens artikel 30 lid 1 sub b EU-Verdrag omvat het gezamenlijk optreden op het gebied van politiële samenwerking de verzameling, opslag, verwerking, analyse en uitwisseling van relevante informatie, met name via Europol, onder voorbehoud van passende bepalingen inzake de bescherming van persoonsgegevens.

Dat de scheiding tussen de eerste en de derde pijler niet altijd even helder was aan te brengen, bleek uit een apart besluit van de Raad waarin van het gehele Schengen-acquis per bepaling de rechtsgrondslag werd bepaald.[43] Ten aanzien van bijvoorbeeld het SIS, dat beide rechtsgebieden moest ondersteunen, kon geen rechtsbasis worden vastgesteld.[44] Uit artikel 2 lid 1 van het protocol bij het Verdrag van Amsterdam volgt dat in afwezigheid van een andersluidend besluit titel VI EU-Verdrag als rechtsbasis van de regeling moet worden beschouwd.[45]

---

40 Het protocol is te vinden in *Pb. EG* 1997, C 340. Het gehele Schengenacquis is gepubliceerd in *Pb. EG* 2000, L 239.

41 Zie over de bescherming van persoonsgegevens in de derde pijler uitgebreid H. Hijmans, 'De derde pijler in de praktijk: leven met gebreken. Over de uitwisseling van informatie tussen de lidstaten.', *SEW* 2006, p. 375-391.

42 Zie over Europol en Eurojust uitgebreid § 3.4.4.

43 Besluit 1999/436 van de Raad van 20 mei 1999 (*Pb. EG* 1999, L 176/17).

44 Bij rechtsbasis staat 'P.M.'.

45 Met het oog op de aanstaande uitbreiding met tien nieuwe lidstaten werd in 2001 de discussie gestart over een vernieuwd informatiesysteem, het SIS II. De basis voor dit nieuwe systeem werd zowel in het EG-Verdrag als in het EU-Verdrag gevonden. Zie besluit 2001/886/JBZ van de Raad van 6 december 2001 (*Pb. EG* 2001, L 328/1) en verordening 2424/2001 van de Raad van 6 december 2001 (*Pb. EG* 2001, L 328/4, verlengd door verordening 1988/2006 van de Raad van 21 december 2006, *Pb. EU* 2007, L 27/3). Zie hierover de mededeling van de Commissie aan de Raad en het Europees Parlement van 18 december 2001

Op de Schengen-initiatieven is sinds de introductie van de ruimte van vrijheid, veiligheid en rechtvaardigheid vlijtig voortgebouwd. In 1999 werd in het Finse Tampere door de Europese Raad een programma opgesteld om het gemeenschappelijke asiel- en immigratiebeleid verder te ontwikkelen en de politiële en justitiële samenwerking te verbeteren (Tampere-programma).[46] De aandacht voor de bescherming van persoonsgegevens in het Tampere-programma was nagenoeg afwezig. Alleen bij de aanpak van het witwassen van geld werd vereist dat dit 'with due regard to data protection' diende plaats te vinden.[47] Dit was anders in de opvolger van het Tampere-programma: het Haags Programma van 2004.[48] Dit programma was doorspekt met verwijzingen naar de bescherming van persoonsgegevens. Door de tussenliggende aanslagen in New York, Madrid en Londen werd de nadruk sterk gelegd op het veiligheidsaspect. Een belangrijk middel om terrorisme (en grensoverschrijdende criminaliteit) te bestrijden, werd gevonden in het vergemakkelijken van grensoverschrijdende uitwisseling van informatie die relevant is voor wetshandhaving. Het zogenaamde *beginsel van beschikbaarheid* moest daarbij het uitgangspunt zijn.[49] Dit beginsel hield in dat een nationale wethandhavingsfunctionaris in alle andere landen van de Unie relevante informatie moest kunnen verkrijgen en voor hetzelfde doel zelf informatie ter beschikking moest stellen. Dat hierbij sprake zou zijn van het verwerken van persoonsgegevens was duidelijk. In het Haags Programma werd daarom benadrukt dat het beginsel van beschikbaarheid gepaard diende te gaan met een strikte toepassing van de grondbeginselen van bescherming van persoonsgegevens.[50]

Ook de doelstellingen ten aanzien van asiel en immigratie stonden in het Haags Programma in het licht van veiligheid: een verbetering van de grenscontroles werd beoogd door effectiever gebruik en koppeling (interoperabiliteit) van bestaande informatiebestanden, zoals het SIS (en later SIS II), het Visa

(COM(2001)720 def., te vinden op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0720:FIN:NL:PDF). In mei 2005 resulteerde dit in een voorstel van de Commissie voor een Raadsbesluit onder de derde pijler en twee voorstellen voor verordeningen onder de eerste pijler. Voorstel voor een besluit van de Raad van 31 mei 2005 (COM(2005) 230 def.), voorstel voor een verordening van het Europees Parlement en de Raad van 31 mei 2005 (COM(2005)236 def.) en voorstel voor een verordening van het Europees Parlement en de Raad van 31 mei 2005 (COM(2005)237 def.). Zie over deze voorstellen uitgebreid het advies van de EDPS van 19 oktober 2005 (*Pb. EU* 2006, C 91/38). De verordeningen werden op 20 december 2006 door de Raad en het Europees Parlement aangenomen. Zie verordening 1986/2006 en verordening 1987/2006 (*Pb. EU* 2006, L 381/1 en L 381/4).

46 Conclusies van de Europese Raad van 15 en 16 oktober 1999 (te vinden via http://europa.eu/european_council/conclusions/index_nl.htm).

47 Tampere-programma, punt 54.

48 Zie annex I bij de conclusies van de Europese Raad van 4 en 5 november 2004 (te vinden via http://europa.eu/european_council/conclusions/index_nl.htm).

49 Zie p. 27 van het Haags Programma.

50 Zie p. 27-28 van het Haags Programma.

Informatie Systeem (VIS) en Eurodac.[51] De Europese Raad moedigde de Commissie aan daarbij meer gebruik te maken van biometrische gegevens, zoals vingerafdrukken en gezichtskenmerken. Bij dit alles moest een juist evenwicht worden gevonden tussen de belangen van de wetshandhaving en de bescherming van de grondrechten van het individu.[52] In 2005 werden de eerste Commissievoorstellen naar aanleiding van het Haags Programma gelanceerd.[53]

Het creëren, gebruiken en koppelen van informatiesystemen binnen de ruimte van vrijheid, veiligheid en rechtvaardigheid vroeg om duidelijke regels over de bescherming van persoonsgegevens. De verschillende rechtsgrondslagen voor het stellen van regels voor het tot stand brengen van deze ruimte leidde echter ten aanzien van de bescherming van persoonsgegevens tot een gefragmenteerde aanpak. Alleen immigratie en asiel vielen binnen de reikwijdte van richtlijn 95/46 of verordening 45/2001. Er bestond ten aanzien van het gebruik van informatiesystemen behoefte aan nadere regelgeving. Ten aanzien van de politiële en justitiële samenwerking is de bescherming van persoonsgegevens momenteel per activiteit geregeld. Daardoor is het terrein van gegevensbescherming in de derde pijler lastig te overzien. De roep om een uniform

51 Zie p. 25 van het Haags Programma. Het VIS is een geautomatiseerd systeem voor de uitwisseling van visumgegevens tussen de lidstaten. Op 19 februari 2004 nam de Raad conclusies aan over de ontwikkeling van het VIS (document 6535/04 VISA 33 COMIX 111 van de Raad). Met beschikking 2004/512/EG van de Raad van 8 juni 2004 werd de mogelijkheid gecreëerd om voorbereidende handelingen te verrichten (*Pb. EU* 2004, L 213/5) en op 28 december 2004 presenteerde de Commissie het voorstel voor de oprichting van het VIS (COM(2004)835 def.). Zie over dit voorstel uitgebreid het advies van de EDPS van 23 maart 2005 (*Pb. EU* 2005, C 181/13). Eurodac is een geautomatiseerde centrale database waarin vingerafdrukgegevens van asielzoekers en illegaal op het grondgebied van een lidstaat binnengekomen derdelanders worden opgeslagen. Zie verordening 2725/2000 van de Raad van 11 december 2000 (*Pb. EG* 2000, L 316/1). Nadere uitvoeringsbepalingen zijn vastgesteld in verordening 407/2002 van de Raad van 28 februari 2002 (*Pb. EG* 2002, L 62/1). Het systeem is sinds 15 januari 2003 actief, zie http://europa.eu/scadplus/leg/en/lvb/l33081.htm.

52 Zie p. 25 van het Haags Programma. Zie over het gebruik van metrische gegevens ook verordening 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten (*Pb. EU* 2004, L 385/1). Zie over biometrische gegevens uitgebreid het rapport van de Joint Research Centre van de Europese Commissie: *Biometrics at the Frontiers: Assessing the Impact on Society*, 2005, te vinden op http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf.

53 Zie bijv. het voorstel van de Commissie voor een kaderbesluit van de Raad betreffende de uitwisseling van informatie volgens het beschikbaarheidsbeginsel van 12 oktober 2005 (COM(2005)490 def., te vinden op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0490:FIN:NL:PDF). Zie voor de verdere uitwerking van het Haags Programma in het algemeen het Actieplan van de Raad en de Commissie ter uitvoering van het Haags Programma voor de versterking van de ruimte van vrijheid, veiligheid en recht in de Europese Unie (*Pb. EU* 2005, C 198/1).

rechtskader, zoals in de communautaire pijler, werd dan ook vaak gehoord.[54] Na verschillende initiatieven hiertoe, werd pas in oktober 2005 door de Commissie een voorstel ingediend voor een uniforme regeling ten aanzien van de bescherming van persoonsgegevens in de derde pijler.[55] Al eerder, in oktober 2000, was op initiatief van Portugal de samenwerking verbeterd tussen de verschillende gemeenschappelijke toezichthouders van Europol, Schengen en de douanesamenwerking door de oprichting van een gemeenschappelijk secretariaat.[56]

3.3 De inhoud van het huidige regime binnen de Raad van Europa[57]

3.3.1 Het Verdrag van Straatsburg

Het Verdrag van Straatburg begint in artikel 1 met de volgende doelstelling:

> The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.

Deze omschrijving is meteen de definitie van wat onder 'bescherming van persoonsgegevens' (*data protection*) moet worden verstaan. Uit artikel 2 sub

---

54 Zie bijv. de resolutie van de gezamenlijke nationale toezichthouders tijdens de European Data Protection Conference op 14 september 2004, te vinden op http://www.cbpweb.nl/downloads_int/20040914_resolutie_EDP_conference.pdf en de *Opinion of the Europol, Eurojust, Schengen and Customs Joint Supervisory Authorities* van 28 september 2004 t.b.v. de House of Lords, te vinden op http://www.cbpweb.nl/downloads_int/okt2004_opinies_gcas.pdf ?refer=true&theme=purple.

55 Zie bijv. het werkdocument van de 2514e bijeenkomst van de Raad van 3 juni 2003, te vinden op http://www.europarl.europa.eu/hearings/20031006/libe/council_note_en.pdf. Zie voorts het Commissievoorstel voor een kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken van 4 oktober 2005 (COM(2005)475 def., te vinden op http://eur-lex.europa.eu/LexUriServ/site/nl/com/2005/com2005_0475nl01.pdf). In mei 2005 werd het voorstel met wijzigingen door het Europees Parlement goedgekeurd, zie het verslag van 18 mei 2006 (A6-0192/2006, te vinden via http://www.europarl.europa.eu/activities/expert/reports.do?language=NL), zie over het voorstel ook het advies van de EDPS van 19 december 2005 (*Pb. EU* 2006, C 47/27).

56 Besluit 2000/641/JBZ van de Raad van 17 oktober 2000 (*Pb. EG* 2000, L 271/1).

57 De inhoud van de OESO-aanbeveling blijft in het navolgende onbesproken. De aanbeveling formuleert in algemene bewoordingen een aantal principes die meer in detail zijn terug te vinden in het Verdrag van Straatsburg en de communautaire regelgeving. Zie over de OESO-aanbeveling ook De Hert 2002, p. 172-174. De inhoud van de (niet bindende) sectorspecifieke aanbevelingen die door het Comité van Ministers van de RvE zijn aangenomen blijft hier verder ook onbesproken. Zoals aangegeven zal aanbeveling R(91) 10 in hoofdstuk 9 ter sprake komen.

a volgt dat als 'persoonsgegevens' (*personal data*) wordt aangemerkt elke informatie die betrekking heeft op 'een geïdentificeerd of identificeerbaar persoon' (*data subject*). Van 'geautomatiseerde verwerking' (*automatic processing*) is sprake als geheel of gedeeltelijk via geautomatiseerde middelen de gegevens worden opgeslagen, als de gegevens aan logische en/of rekenkundige handelingen worden onderworpen en als de gegevens worden aangepast, gewist, ontsloten of *verspreid* (artikel 2 sub c). Dit laatste ziet volgens de toelichting zowel op verstrekking van de gegevens aan een of meerdere personen als op het mogelijk maken van inzage in de gegevens.[58] Het verzamelen van persoonsgegevens valt volgens de toelichting niet onder het begrip 'verwerken'.[59] Ten aanzien van het verzamelen van gegevens zijn echter wel regels gesteld.[60] De natuurlijke of rechtspersoon die volgens nationaal recht bevoegd is om te beslissen over het doel van de verzameling van gegevens, over welke gegevens moeten worden opgeslagen en welke handelingen ermee zullen worden verricht, is de *controller of the file* (artikel 2 sub d). De bepalingen van het Verdrag zien zowel op verwerking van persoonsgegevens door de overheid als door particulieren (artikel 3 sub a). De werking van het Verdrag kan onder bepaalde voorwaarden door een verdragspartij worden beperkt en/of uitgebreid. Zo kunnen bepaalde categorieën gegevens van de werking van het Verdrag worden uitgesloten en/of kunnen de regels ook van toepassing worden verklaard op niet-natuurlijke personen en op het niet-geautomatiseerd verwerken van persoonsgegevens (artikel 3 lid 2 sub a, b en c).

In het vervolg van het Verdrag worden drie verschillende onderwerpen behandeld: de inhoudelijke eisen aan bescherming van persoonsgegevens (artikel 5 tot en met 11), het grensoverschrijdende gegevensverkeer (artikel 12) en de mechanismen voor wederzijdse bijstand en consultatie (artikel 13 tot en met 20).

In artikel 5 zijn de voorschriften neergelegd waaraan de automatische verwerking van persoonsgegevens moet voldoen.

> Personal data undergoing automatic processing shall be:
> a. obtained and processed fairly and lawfully;
> b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
> c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
> d. accurate and, where necessary, kept up to date;
> e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

58 Paragraaf 31 van het *Explanatory Report* bij het Verdrag van Straatsburg. Overigens vormt dit *Explanatory Report* niet een bindende interpretatie van de tekst van het Verdrag, zie onder paragraaf II van het *Explanatory Report*.

59 Paragraaf 31 van het *Explanatory Report* bij het Verdrag van Straatsburg.

60 Zie artikel 5 sub a en 12 van het Verdrag.

Artikel 6 verbiedt dat speciale categorieën (gevoelige) gegevens worden verwerkt, tenzij in nationale wetgeving voldoende waarborgen zijn neergelegd. Het gaat om gegevens over iemands raciale afkomst, over zijn politieke opvattingen of over iemands godsdienstige of andere overtuiging. Ook gaat het om gezondheidsgegevens of om gegevens over het seksuele gedrag of strafrechtelijke veroordelingen.

In artikel 8 zijn waarborgen opgenomen voor de persoon van wie de gegevens worden verwerkt:

> Any person shall be enabled:
> a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
> b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
> c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;
> d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

Uitzonderingen op artikel 5, 6 en 8 zijn alleen mogelijk als zij bij wet zijn voorzien en noodzakelijk zijn in een democratische samenleving in het belang van de veiligheid van de staat, de openbare veiligheid, het monetaire belang van de staat of de vervolging van strafbare feiten (artikel 9 lid 2 sub a). Een andere uitzondering kan gemaakt worden voor de bescherming van de persoon wiens gegevens worden verwerkt of voor de bescherming van de rechten en vrijheden van anderen (artikel 9 lid 2 sub b). Volgens de toelichting moet bij dit laatste gedacht worden aan de persvrijheid of de geheimhouding van bedrijfsgegevens.[61] In artikel 10 is bepaald dat de verdragspartijen passende sancties en remedies moeten instellen voor schendingen van de bepalingen uit het Verdrag. Hiermee is benadrukt dat het Verdrag geen *rechtstreeks* werkende bepalingen bevat waarop personen zich zouden kunnen beroepen.[62] Tot slot is in artikel 11 bepaald dat het Verdrag de Verdragspartijen niet verhindert om betrokkenen een verdergaande bescherming te bieden.

In artikel 12 zijn regels neergelegd over het grensoverschrijdende verkeer van persoonsgegevens. Het is een verdragspartij niet toegestaan om, met als enige doel de bescherming van het privé-leven, het grensoverschrijdende

---

61 Paragraaf 58 van het *Explanatory Report* bij het Verdrag van Straatsburg.

62 Meer algemeen wordt in artikel 4 lid 1 van het Verdrag verdragsstaten de plicht opgelegd om alle noodzakelijke maatregelen te nemen om nationale wetgeving in overeenstemming te brengen met de basisbeginselen uit het Verdrag.

verkeer van persoonsgegevens tussen twee verdragsstaten te verhinderen of aan speciale toestemming onderhevig te maken (lid 2). Hierop zijn twee uitzonderingen (lid 3). Ten eerste als een verdragsstaat speciale regels heeft voor bepaalde categorieën gegevens. Deze uitzonderingsmogelijkheid vervalt als het ontvangende verdragsstaat een gelijkwaardige bescherming biedt. Ten tweede is een uitzondering mogelijk als doorgifte van persoonsgegevens naar een ander verdragsstaat duidelijk is bedoeld om de gegevens vervolgens naar een derde land (*i.e.* geen verdragspartij) door te geven. In het eerdergenoemde protocol bij het Verdrag van Straatsburg zijn over de doorgifte van persoonsgegevens aan derde landen nadere regels neergelegd. Deze doorgifte mag alleen plaatsvinden als het derde land een 'passend beschermingsniveau' (*adequate level of protection*) biedt (artikel 2 lid 1). De beoordeling of van een passend beschermingsniveau sprake is, kan van geval tot geval worden gemaakt, of in het algemeen ten aanzien van één land.[63] Hierbij moet rekening worden gehouden met de inhoudelijke eisen uit het Verdrag.

In het Verdrag van Straatsburg wordt tot slot afgesproken dat de verdragspartijen elkaar zullen bijstaan om de implementatie van het Verdrag te bewerkstelligen (artikel 13). Met dat doel roepen de verdragsstaten één of meer autoriteiten in het leven. Deze autoriteiten werden door het additionele protocol bij het Verdrag omgevormd tot toezichthoudende autoriteiten met ruime onderzoeks- en interventiebevoegdheden (artikel 1). In artikel 14 tot en met 17 van het Verdrag zijn regels neergelegd over de bijstand die de verdragspartijen moeten bieden aan elke persoon die zich in het buitenland bevindt en die van de waarborgen uit artikel 8 gebruik wil maken. Artikel 18 regelt de totstandkoming van het Raadplegend Comité, een internationale instantie die voorstellen voor amendering van het Verdrag kan doen en die op verzoek uitleg over het Verdrag kan geven.

3.3.2 Het EVRM

In de jaren 70 werd de bescherming die artikel 8 EVRM aan persoonsgegevens kon bieden kennelijk niet toereikend geacht. De vraag van de Parlementaire Vergadering aan het CvM uit 1968 leidde immers tot een apart Verdrag over de bescherming van persoonsgegevens. Na de totstandkoming van het Verdrag van Straatsburg heeft het EHRM in zijn jurisprudentie echter de bescherming van persoonsgegevens voor een belangrijk deel onder artikel 8 gebracht.[64]

---

63 Paragraaf 26-29 van het *Explanatory Report* bij het *Additional Protocol* (*European Treaty Series*, nr. 181).

64 Zie voor een uitgebreide analyse van de jurisprudentie van het EHRM over bescherming van persoonsgegevens P. de Hert, 'Mensenrechten en de bescherming van persoonsgegevens: overzicht en synthese van de Europese rechtspraak 1955-1997', in Rimanque e.a. (eds), *Mensenrechten Jaarboek 1996/97 van het Interuniversitair centrum mensenrechten*, Antwerpen 1997, Maklu, p. 43-96. Zie ook C. Ovey and R. White, *Jacobs & White, The European Convention*

Ook uit de jurisprudentie van het EHRM is een daarom aantal vereisten voor de bescherming van persoonsgegevens af te leiden. Artikel 8 EVRM luidt:

> 1. Een ieder heeft recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
> 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Het gebruikelijke toetsingsschema dat het EHRM bij dit artikel hanteert, is dat eerst, althans nadat aan de gebruikelijke ontvankelijkheidseisen is voldaan, wordt bekeken of de feiten binnen de *reikwijdte* van het recht van artikel 8 vallen. Vervolgens beoordeelt het EHRM of er sprake is van een *inbreuk* op dit recht. Tot slot toetst het EHRM of deze inmenging *gerechtvaardigd* is op grond van lid 2. Is dat niet het geval, dan is sprake van een schending van het in artikel 8 neergelegde recht.[65] Is er sprake van een positieve verplichting dan is de toetsing anders. De grens tussen het vaststellen van de inbreuk en de rechtvaardiging ervan vervaagt. Het EHRM beoordeelt namelijk na vaststelling van de toepasselijkheid van artikel 8 meteen of er een juiste belangafweging heeft plaatsgevonden.[66]

Hieronder wordt alleen besproken in welke omstandigheden het EHRM bij verwerking van persoonsgegevens een inbreuk op artikel 8 EVRM vaststelde en op welke gronden deze inbreuk al dan niet gerechtvaardigd was. Jurisprudentie over de vraag wanneer gegevensverwerking wel en niet binnen de reikwijdte van het recht op privacy viel, komt in het volgende hoofdstuk uitgebreid aan bod.

3.3.2.1 Persoonsgegevens en de inbreuk op de bescherming van het privé-leven

Het overzicht hieronder geeft een indruk van welk handelen van de overheid ten aanzien van persoonsgegevens door het EHRM als een inbreuk op het privé-leven is beschouwd. In de jurisprudentie van het EHRM is het handelen van de overheid ten aanzien van persoonsgegevens ruwweg onder te verdelen in vier categorieën. Ten eerste de overheid die gegevens van een individu *vastlegt*. Ten tweede de overheid die bestaande persoonsgegevens, uit handen

---

on Human Rights, Oxford 2006, Oxford University Press, p. 286-296. Voor een algemene bespreking van artikel 8 EVRM zie P. van Dijk e.a. (eds), *Theory and Practice of the European Convention on Human Rights*, Antwerpen 2006, Intersentia, p. 663-750.

65 Een voorbeeld van de toepassing van dit toetsingsschema is te vinden in de uitspraak van het EHRM in de zaak *Rotaru*, EHRM 4 mei 2000, *Rotaru t. Roemenië*, r.o. 45-63.

66 Zie bijv. EHRM 24 juni 2004, *Von Hannover t. Duitsland*, r.o. 57.

van derden, *verzamelt*. Ten derde de overheid die persoonsgegevens *bewaart en er vervolghandelingen mee verricht*. En tot slot de overheid die een persoon *toegang tot de bewaarde gegevens weigert*. Aan de hand van deze vierdeling zal hieronder de jurisprudentie van het EHRM kort worden besproken.

Vastleggen van persoonsgegevens

De jurisprudentie van het EHRM over de manier waarop de overheid persoonsgegevens vastlegt, ziet vooral op het afluisteren van gesprekken of telefoongesprekken.[67] Het ging zowel om gesprekken die gevoerd werden in de privé-sfeer als in het publieke domein. Uit de zaak *Halford t. het Verenigd Koninkrijk*, waarin iemands telefoon op de werkplek werd afgeluisterd, volgt dat de redelijke privacyverwachting van de betrokken persoon een belangrijk criterium is om te bepalen of bepaald handelen inbreuk maakt op het recht op bescherming van het privé-leven.[68] In *Halford* overwoog het EHRM dat de klager inderdaad een redelijke privacyverwachting mocht koesteren: het afluisteren van zijn telefoon op de werkplek vormde een inbreuk op het recht op privacybescherming.[69] In *Copland t. het Verenigd Koninkrijk* kwam het EHRM tot dezelfde conclusie ten aanzien van het (onvermeld) controleren van mail- en surfgedrag van werknemers.[70]

Ook het filmen of fotograferen van personen werd een aantal keer als een inbreuk op de bescherming van het privé-leven beschouwd. In de zaak *Murray t. het Verenigd Koninkrijk* werd een aantal personen in eigen huis gearresteerd wegens verdenking van betrokkenheid bij terroristische activiteiten.[71] Eenmaal aangekomen op het politiebureau werd één van hen tegen haar wil gefotografeerd. Uit de beslissing van het EHRM blijkt niet direct of het fotograferen tegen iemands wil op zichzelf een inbreuk maakt op het privé-leven. Het EHRM vond namelijk dat de hele situatie – inclusief de arrestatie in eigen huis – een inmenging met het privé-leven van de klagers betekende.[72] Bij de behandeling van de vraag of de inbreuk gerechtvaardigd was, besteedde het EHRM wel apart aandacht aan het ongewild gefotografeerd worden, zij het in combinatie met het bewaren van de foto's.[73]

---

67 EHRM 6 september 1978, *Klass t. Duitsland*; EHRM 2 augustus 1984, *Malone t. het Verenigd Koninkrijk*; EHRM 24 april 1990, *Kruslin t. Frankrijk*; EHRM 24 april 1990, *Huvig t. Frankrijk*; EHRM 15 juni 1992, *Lüdi t. Zwitserland*; EHRM 25 juni 1997, *Halford t. het Verenigd Koninkrijk;* EHRM 16 februari 2000, *Amann t. Zwitserland;* EHRM 12 mei 2000, *Khan t. het Verenigd Koninkrijk*; EHRM 19 maart 2002, *Greuter t. Nederland* (ontvankelijkheidsbeslissing), EHRM 27 april 2004, *Doerga t. Nederland*; EHRM 29 maart 2005, *Matheron t. Frankrijk* en EHRM 1 maart 2007, *Heglas t. Tsjechië*.

68 EHRM, *Halford*, r.o. 45. Zie over het criterium van de redelijke privacyverwachting uitgebreid § 4.3.4.

69 EHRM, *Halford*, r.o. 48.

70 EHRM 3 april 2007, *Copland t. het Verenigd Koninkrijk*.

71 EHRM 28 oktober 1994, *Murray t. het Verenigd Koninkrijk*.

72 EHRM, *Murray*, r.o. 86.

73 EHRM, *Murray*, r.o. 93.

Verzamelen van persoonsgegevens
Het verzamelen van gegevens ziet op het verkrijgen van persoonlijk informatie door de overheid uit handen van derden (particulieren of private instanties). Door de moderne technieken en communicatiemiddelen worden in de private sector steeds meer persoonsgegevens verzameld en opgeslagen. In Europa is – in navolging van de Verenigde Staten – een trend zichtbaar dat criminaliteit bestreden en voorkomen wordt door zoveel mogelijk gegevens te verzamelen en te koppelen. Deze gegevens worden grotendeels verkregen uit handen van private organisaties, zoals telefoon- en vliegmaatschappijen. Het verzamelen van door derden vastgelegde gegevens zal daarom steeds vaker onderwerp zijn van geschil voor het EHRM.

Tot nu toe heeft het EHRM zich niet vaak over het verzamelen van persoonsgegevens uitgesproken. Dat het verkrijgen van gegevens uit handen van derden wel degelijk een inbreuk kan vormen op het recht uit artikel 8 EVRM blijkt uit *Malone t. het Verenigd Koninkrijk* en *P.G. en J.H. t. het Verenigd Koninkrijk*. In beide zaken vroeg de overheid aan een telecommunicatiebedrijf extra informatie over een afgetapt telefoongesprek, zoals het (toen nog) gedraaide nummer en de duur van het gesprek. Deze informatie was door het telecommunicatiebedrijf vastgelegd om de telefoonrekening op te kunnen maken. Dit vastleggen van belgegevens staat bekend als 'metering'.[74] In *Malone* oordeelde het EHRM dat het (ongevraagd) vrijgeven van deze informatie aan de overheid, en dan vooral de gedraaide telefoonnummers, een inbreuk vormde op de bescherming van het privé-leven.[75] Door deze formulering legde het EHRM de verantwoordelijkheid in eerste instantie bij het telecommunicatiebedrijf. In *P.G. en J.H.* was de formulering anders:

> It is not in dispute that the *obtaining by the police* of information relating to the numbers called on the telephone in B.'s flat interfered with the private lives or correspondence (in the sense of telephone communications) of the applicants who made use of the telephone in the flat or were telephoned from the flat.[76]

Bewaren van persoonsgegevens en het verrichten van vervolghandelingen
Het louter *bewaren* van persoonsgegevens door de overheid leverde volgens het EHRM geen inbreuk op artikel 8 op. Het bewaren moest systematisch zijn, of gecombineerd worden met een bepaald gebruik ervan voordat van een inbreuk sprake was.[77] In *Leander t. Zweden* was het opslaan en gebruik van de informatie *in combinatie met* de onmogelijkheid de informatie te corrigeren

74 EHRM, *Malone*, r.o. 83 en EHRM 25 september 2001, *P.G. en J.H. t. het Verenigd Koninkrijk*, r.o. 42.
75 EHRM, *Malone*, r.o. 84.
76 EHRM, *P.G. en J.H.*, r.o. 42 (eigen cursivering).
77 Zie de eerder besproken arresten EHRM, *Rotaru* en EHRM, *P.G. en J.H.*; Zie ook EHRM 28 januari 2003, *Peck t. het Verenigd Koninkrijk* en EHRM 17 juli 2003, *Perry t. het Verenigd Koninkrijk*. Zie hierover uitgebreid § 4.3.2 en § 4.3.3.

een inbreuk op het recht op privé-leven.[78] In de ontvankelijkheidsbeslissing in *Knauth t. Duitsland* werd het gebruik van een persoonsdossier, ook los van de onmogelijkheid het dossier in te zien, beschouwd als inbreuk op het privéleven.[79]

Met de gegevens werden verschillende vervolghandelingen verricht. Zo leverde het publiekelijk bekend maken van persoonsgegevens een inbreuk op de bescherming van het privé-leven op.[80] En ook het overhandigen van persoonlijke informatie door de overheid aan private instanties werd als een inbreuk beschouwd. Dit was bijvoorbeeld het geval in *M.S. t. Zweden*, waarin een mevrouw tijdens haar werk van een trap viel, waardoor zij wegens rugklachten enige tijd niet kon werken.[81] Toen zij bij een Zweedse sociale verzekeringsinstantie een aanvraag voor compensatie indiende, controleerde deze haar medisch dossier dat afkomstig was van het ziekenhuis (een overheidsinstantie) waarin de vrouw meerdere keren was behandeld. In het dossier werd vermeld dat zij door een bepaalde aandoening al sinds jonge leeftijd rugklachten had. De verzekeringsinstantie concludeerde dat de val op het werk niet de oorzaak was van de rugklachten, en wees haar verzoek om compensatie af. Het EHRM overwoog dat het doorgeven van de medische informatie aan de verzekeringsinstantie een inbreuk vormde op artikel 8 EVRM.[82]

Weigering van toegang tot persoonsgegevens

In hoofdstuk 2 werd aan de hand van zaak *Leander* al besproken dat uit artikel 8 EVRM een recht op toegang tot eigen persoonsgegevens is af te leiden.[83] Toegang tot persoonsgegevens neemt in de jurisprudentie van het EHRM onder artikel 8 verschillende posities in. Soms behandelde het EHRM dit recht als een positieve verplichting onder artikel 8: de overheid had de plicht om toegang tot de gegevens te verlenen. In andere gevallen werd de weigering van toegang in combinatie met ander gebruik van de gegevens beschouwd als een inbreuk op artikel 8 lid 1. Het recht op toegang werd soms ook gezien als een waarborg die onder lid 2 mede de gerechtvaardigheid van de inbreuk kon bepalen.[84]

Bij toegang tot eigen persoonsgegevens zijn er in de jurisprudentie van het EHRM globaal twee situaties te onderscheiden. In de eerste plaats is er de weigering van de overheid om informatie over iemands verleden of identiteit vrij te geven. Deze zaken werden door het EHRM behandeld als een eventuele schending van de positieve verplichting onder artikel 8. Daardoor

78 EHRM 26 maart 1987, *Leander t. Zweden*, r.o. 48.
79 Zie EHRM 22 november 2001, *Knauth t. Duitsland* (ontvankelijkheidsbeslissing).
80 Zie EHRM 25 januari 1997, *Z. t. Finland* en EHRM 11 april 2001, *Kolarides t. Cyprus* (ontvankelijkheidsbeslissing).
81 EHRM 27 augustus 1997, *M.S. t. Zweden*.
82 EHRM, *M.S.*, r.o. 35.
83 Zie § 2.5.2.
84 Zie verder § 3.3.2.2.

kwam de vraag naar de inbreuk op het recht op privé-leven minder duidelijk aan bod. Voorbeelden van dit soort zaken zijn *Gaskin t. het Verenigd Koninkrijk* en *Odièvre t. Frankrijk*.[85] Gaskin wilde toegang hebben tot informatie over de adressen waar hij in zijn jeugd was ondergebracht. In *Odièvre t. Frankrijk* probeerde de klaagster te achterhalen wie haar natuurlijke moeder was. Kort na haar geboorte was zij afgestaan door haar moeder, die verzocht had informatie over haar identiteit geheim te houden. Wat deze laatste zaak bijzonder maakt, is dat de betreffende informatie zowel persoonsgegevens waren van de klager als van haar natuurlijke moeder. Bij de vraag of de Franse overheid zijn positieve plicht onder artikel 8 had geschonden, beoordeelde het EHRM of de Franse overheid een juiste belangenafweging had gemaakt.

In de tweede plaats is er de weigering door de overheid van toegang tot een persoonsdossier op basis waarvan bijvoorbeeld een ontslag of weigering tot indienststelling had plaatsgevonden. Hiervan is *Leander* een voorbeeld. In deze zaak bevatte het dossier 'information relating to the private life of mr. Leander'.[86] Het weigeren van toegang werd niet als een eventuele schending van een positieve verplichting behandeld. Samen met het opslaan van de gegevens was de weigering volgens het EHRM een inbreuk op artikel 8 lid 1 EVRM, waarna aan lid 2 getoetst werd of de inbreuk gerechtvaardigd was.[87] Ook in *Rotaru t. Roemenië* stelde het EHRM een inbreuk vast. Het opslaan en gebruik van de gegevens samen met de 'refusal to allow the applicant an opportunity to refute it' vormden een inbreuk op het recht op bescherming van het privé-leven.[88]

In *Smith t. het Verenigd Koninkrijk* probeerde iemand op grond van artikel 8 EVRM toegang te krijgen tot een zakelijk dossier waarin zich documenten bevonden waar zijn naam in voor kwam als directeur van een bepaalde onderneming.[89] De klacht werd kennelijk ongegrond verklaard omdat de verlangde informatie louter zakelijk was en de verzoeker al op de hoogte was van de inhoud van de gevraagde documenten.[90] Het EHRM overwoog dat het verzoek eerder was ingegeven om bewijs te vergaren en dat het niet een situatie betrof als in *Gaskin* en *Rotaru*.[91]

---

85 EHRM 7 juli 1989, *Gaskin t. het Verenigd Koninkrijk*, r.o. 37 en EHRM 13 februari 2003, *Odièvre t. Frankrijk*. Zie over de zaak *Gaskin* L.F.M. Verhey, 'Het recht op inzage in persoonsdossiers', *NJCM-Bulletin* 1990, p. 206-217. Zie verder ook EHRM 7 februari 2002, *Mikulić t. Kroatië*, r.o. 54.

86 EHRM, *Leander*, r.o. 48.

87 EHRM, *Leander*, r.o. 48.

88 EHRM, *Rotaru*, r.o. 46.

89 EHRM 4 januari 2007, *Smith t. het Verenigd Koninkrijk* (ontvankelijkheidsbeslissing), p. 4.

90 Zie over deze zaak ook § 8.4.6.

91 EHRM, *Smith*, p. 4.

3.3.2.2 Persoonsgegevens en de gerechtvaardigde inbreuk op de bescherming van het privé-leven

Volgens artikel 8 lid 2 EVRM is een inbreuk gerechtvaardigd als deze bij wet is voorzien, een legitiem doel dient, en noodzakelijk is in een democratische samenleving. Het eerste vereiste houdt in dat de inbreukmakende maatregel een basis heeft in nationale wetgeving, en dat deze wetgeving toegankelijk was en voorzienbaar.[92] Wat onder een legitiem doel wordt verstaan, is uitgewerkt in het tweede lid van artikel 8. Bij het derde vereiste wordt beoordeeld of de aangevoerde argumenten relevant en voldoende zijn, en of de maatregel proportioneel was ten opzichte van het beoogde doel.[93] Lidstaten hebben bij het maken van deze belangenafweging een beoordelingsruimte. Het EHRM ziet er op toe dat de grens van deze beoordelingsruimte niet is overschreden. Deze grens is afhankelijk van factoren als de aard en ernst van de betrokken belangen, en de ernst van de inbreuk.[94]

In *Klass t. Duitsland* introduceerde het EHRM het vereiste dat in geval van (geheim) overheidstoezicht op de burger, er adequate en effectieve waarborgen moesten bestaan om misbruik tegen te gaan.[95] Aan dit vereiste is in latere jurisprudentie onder artikel 8 lid 2 vaak getoetst. Het EHRM was daarbij niet altijd even consequent in het moment waarop het dit vereiste naar voren bracht. Zo viel de toets aan dit vereiste in *Rotaru* onder de vraag naar de wettelijke basis van de maatregel,[96] en in *Z. t. Finland* en *M.S. t. Zweden* onder de noodzakelijkheidstoets.[97] Het gevolg was dat in het eerste geval een plicht bestond om aan te tonen dat bij wet was voorzien in bepaalde adequate en effectieve waarborgen. Was daar niet aan voldaan, dan kwam het EHRM niet meer toe aan een toetsing van de door de overheid gemaakte belangenafweging onder de noodzakelijkheidstoets. Kon de staat wél bepaalde wettelijke waarborgen aantonen, dan liet het EHRM deze meewegen in de toetsing van de gemaakte belangenafweging. In het tweede geval, *Z. t. Finland* en *M.S. t. Zweden*, ging het EHRM meteen over tot deze toets. In recente jurisprudentie behandelt het EHRM het vereiste van adequate en effectieve waarborgen alleen nog onder de vraag naar de wettelijke basis.[98]

Uit de jurisprudentie van het EHRM zijn waarborgen af te leiden waarmee gegevensverwerking moet zijn omgeven om van een gerechtvaardigde inbreuk op het privé-leven te kunnen spreken. De hieronder weergegeven lijst is niet uitputtend, en de overheid is niet verplicht het bestaan van al deze elementen

92 Zie bijv. EHRM 25 maart 1998, *Kopp t. Zwitserland*, r.o. 55.
93 Zie bijv. EHRM, *Peck*, r.o. 76.
94 Zie bijv. EHRM, *Peck*, r.o. 77.
95 EHRM, *Klass*, r.o. 50.
96 EHRM, *Rotaru*, r.o. 59.
97 EHRM, *Z.*, r.o. 103 en *M.S.*, r.o. 43.
98 Zie bijv. EHRM 6 juni 2006, *Segerstedt-Wiberg e.a. t. Zweden*, r.o. 76. De ontvankelijkheidsbeslissing van het EHRM in *Greuter* lijkt hier weer een uitzondering op te zijn.

aan te tonen. Uit de jurisprudentie volgt dat het EHRM per geval bekijkt of de waarborgen die zijn aangedragen bij wet waren voorzien en vervolgens of zij voldoende bescherming boden tegen eventueel misbruik.[99]

– *Effectief toezicht door een onafhankelijke en onpartijdige instantie*. In *Klass* wees het EHRM op de *rule of law*.[100] Deze impliceert dat als de uitvoerende macht inbreuk maakt op het recht uit artikel 8, dat dan (uiteindelijk) effectieve controle door de rechterlijke macht *mogelijk* moet zijn. Dit garandeert namelijk een onafhankelijke, onpartijdige en correcte procedure. De rechterlijke controle kan vooraf worden gegaan door toezicht door een onafhankelijke instantie. Dit volgt uit de zaken *Leander* en *Gaskin* waarin voor de rechtvaardiging van de weigering van toegang tot eigen persoonsgegevens belang werd gehecht aan de aan- respectievelijk afwezigheid van een onafhankelijke toezichthoudende instantie.[101]

– *Beperkingen ten aanzien van het vastleggen, verzamelen, bewaren en gebruiken van de gegevens*. Over het vastleggen van gegeven door middel van geheim toezicht overwoog het EHRM dat een individu moet kunnen weten onder welke omstandigheden en voorwaarden de publieke autoriteiten bevoegd waren om gebruik te maken van dergelijke middelen.[102] Een belangrijk vereiste voor het gebruik van persoonsgegevens is verder de zogenaamde *doelbinding*. Gegevens mogen alleen gebruikt worden voor het wettelijk vastgestelde doel waarvoor ze zijn verkregen.[103] Daarnaast moeten de gegevens relevant zijn voor het beoogde doel.[104] Ook hecht het EHRM belang aan het stellen van grenzen aan de *duur* van het bewaren van de gegevens.[105] In *M.S. t. Zweden*, liet het EHRM meewegen dat schending van de geheimhoudingsplicht door

---

99 Zie hierover ook L.F.M. Verhey, 'De EG-richtlijn bescherming persoonsgegevens: uitgangspunten en hoofdlijnen', *NJCM-Bulletin* 1997, p. 242 en I. Harden, 'Citizenship and Information', *EPL* 2001, p. 173-174.

100 EHRM, *Klass*, r.o. 55. Zie ook EHRM, *Rotaru*, r.o. 59.

101 EHRM, *Leander*, r.o. 65 en EHRM, *Gaskin*, r.o. 49. Zie ook EHRM, *Odièvre*, r.o. 49 en EHRM 5 april 2005, *Brinks t. Nederland* (ontvankelijkheidsbeslissing), p. 10. In EHRM 18 mei 2004, *Eccleston t. het Verenigd Koninkrijk* (ontvankelijkheidsbeslissing), speelden de feiten zich af na aanpassing van de Britse wetgeving. Omdat de klager niet alle rechtsmiddelen had uitgeput werd de klacht niet-ontvankelijk verklaard. De zaak *M.G. t. het Verenigd Koninkrijk* van 24 september 2004 speelde zich af zowel voor als na de aanpassing van de Britse wetgeving. Het handelen van de overheid van voor de aanpassing werd als in strijd met artikel 8 beschouwd.

102 EHRM, *Kopp*, r.o. 64. Zie ook EHRM, *Perry*, r.o. 45 en EHRM, *Doerga*, r.o. 45. In de uitspraak van het EHRM van 14 februari 2006, *Turek t. Slowakije*, werd artikel 8 door het EHRM geschonden geacht, omdat de regels waaraan de overheid gebonden was, geheim waren, r.o. 116.

103 EHRM, *Z.*, r.o. 103.

104 EHRM, *Murray*, r.o. 93

105 EHRM, *Rotaru*, r.o. 57. Zie ook EHRM, *Segerstedt-Wiberg e.a. t. Zweden*, r.o. 90.

overheidspersoneel tot civiele of strafrechtelijke aansprakelijkheid kon leiden.[106]

– *Controle over de verwerking van eigen persoonsgegevens*. Een belangrijke waarborg tegen misbruik van gegevens is de mogelijkheid van toegang tot eigen persoonsgegevens.[107] Deze mogelijkheid strekt zich echter niet zo ver uit dat iemand die vanuit zijn professionele hoedanigheid bij naam in bepaalde zakelijke documenten genoemd wordt, toegang tot die documenten moet hebben.[108] Wat ook meeweegt bij de beoordeling of voldoende waarborgen tegen misbruik bestaan is de mogelijkheid voor het individu om correcties aan te brengen.[109] Daarnaast moet de betrokkene zo veel mogelijk op de hoogte worden gesteld van het feit dat persoonlijke informatie in handen van de overheid is.[110]

Bij de belangenafweging spelen naast deze waarborgen ook andere elementen een rol. In *Z. t. Finland* hield het EHRM rekening met de gevoelige aard van de gegevens. Het overwoog dat de HIV-besmetting van de klaagster als medisch gegeven extra vertrouwelijk behandeld diende te worden.[111] Daarnaast kan het gewicht van het nagestreefde doel in de belangenafweging worden betrokken. In *Murray* liet het EHRM bijvoorbeeld de bestrijding van terrorisme als legitiem doel in de belangafweging zwaar meewegen.[112]

Ook de redelijke privacyverwachting van de betrokkene kan een rol spelen in de belangenafweging. Een voorbeeld daarvan is de ontvankelijkheidsbeslissing van het EHRM in de zaak *Wypych t. Polen*.[113] Hierin had een Pools gemeenteraadslid informatie over zijn inkomen en bezittingen openbaar moeten maken. In zijn oordeel liet het EHRM meewegen dat Wypych als politicus bepaalde openbaarheid over zijn persoon kon verwachten. Het concludeerde dat het openbaar maken van de informatie geen ongerechtvaardigde inbreuk op Wypychs recht op privacy inhield.[114] Op de redelijke privacyverwachting wordt in hoofdstuk 4 uitgebreider ingegaan.[115]

106 EHRM, *M.S.*, r.o. 43.
107 EHRM, *Leander*, r.o. 48.
108 EHRM, *Smith*, p. 4.
109 EHRM, *Leander*, 48 en EHRM, *Rotaru*, r.o. 46.
110 EHRM, *Klass*, r.o. 58.
111 EHRM, *Z.*, r.o. 96. Zie ook EHRM, *M.S.*, r.o. 41.
112 EHRM, *Murray*, r.o. 91.
113 EHRM 25 oktober 2005, *Wypych t. Polen* (ontvankelijkheidsbeslissing). Zie over deze zaak ook § 4.3.4 en § 9.5.3.3.
114 EHRM, *Wypych*, p. 11. Deze beslissing komt nader ter sprake in § 4.3.4 en § 9.5.3.3.
115 Zie § 4.3.4.

3.4 De inhoud van het huidige regime in de EU

3.4.1 Vooraf

In deze paragraaf wordt vooral de regelgeving besproken die op de *instellingen en organen* van de Unie van toepassing is. Voor activiteiten binnen de eerste pijler is de toepasselijke regelgeving duidelijk: verordening 45/2001 is verreweg het belangrijkste instrument voor de Europese instellingen. Daarnaast zijn meer specifieke regelingen relevant. In § 3.4.2 zullen de regels voor de bescherming van persoonsgegevens in de eerste pijler worden besproken.

In de tweede en derde pijler is het minder duidelijk aan welke regels de instellingen gebonden zijn. Verordening 45/2001 is niet van toepassing op de verwerking van persoonsgegevens in de tweede en derde pijler. Er bestaat, zoals eerder aangegeven, momenteel noch voor de lidstaten noch voor de EU-instellingen overkoepelende wetgeving.[116] In de tweede en derde pijler is de bescherming van persoonsgegevens fragmentarisch geregeld en daarbij is de aanwezige regelgeving ook nog eens hoofdzakelijk gericht tot de lidstaten. De vraag aan welke regels de Europese instellingen zijn gebonden als zij persoonsgegevens verwerken in het kader van de tweede of derde pijler is daarom niet eenvoudig te beantwoorden. Voor de instellingen die al bestaan op basis van de eerste pijler moet worden teruggevallen op artikel 8 EVRM en het Verdrag van Straatsburg. Hierop wordt in § 3.4.3 ingegaan. In § 3.4.4 worden de gegevensbeschermingsregels besproken die gelden voor twee organen die specifiek zijn opgericht in het kader van de derde pijler: Eurojust en Europol.

3.4.2 Bescherming van persoonsgegevens in de eerste pijler

3.4.2.1 Verordening 45/2001

In artikel 286 EG-Verdrag worden richtlijn 95/46 en richtlijn 97/66 van toepassing verklaard op de Europese instellingen en organen.[117] In artikel 286 EG-Verdrag is *geen* directe verplichting opgenomen om de bepalingen van deze richtlijnen in een aparte verordening om te zetten. Dat dit in verordening 45/2001 toch is gebeurd, heeft twee redenen. Ten eerste was er een verordening nodig om aan natuurlijke personen wettelijk afdwingbare rechten toe te kennen ten opzichte van de Europese instellingen. Ten tweede wilde men de verplichtingen vaststellen die zouden gaan rusten op de voor de verwerking verant-

116 Een kaderbesluit voor de bescherming van persoonsgegevens in de derde pijler wordt, zoals gezegd, op het moment van schrijven bediscussieerd, *supra* noot 55.

117 Zie ook § 3.2.2.

woordelijken.[118] Het HvJ heeft zich nog niet over verordening 45/2001 uitgesproken. Over de inhoud van richtlijn 95/46 deed het HvJ pas drie maal uitspraak.[119]

Hieronder wordt de inhoud van verordening 45/2001 besproken. In vergelijking met het Verdrag van Straatsburg is de verordening breder opgezet en gedetailleerder. In grote lijnen lopen beide documenten gelijk op. Eventuele opmerkelijke inhoudelijke verschillen met het Verdrag van Straatsburg worden aangestipt. De bepalingen van verordening 45/2001 die voor dit onderzoek bijzonder relevant zijn, worden in hoofdstuk 7 meer in detail besproken.[120]

Het doel van de verordening

Het doel van verordening 45/2001 is volgens de considerans het zorgdragen voor een doeltreffende naleving van enerzijds de regels over de bescherming van fundamentele rechten en vrijheden van natuurlijke personen en anderzijds de regels over het vrij verkeer van persoonsgegevens tussen de instellingen onderling en de instellingen en de lidstaten.[121]

De reikwijdte van de verordening[122]

Volgens artikel 3 zijn de bepalingen van de verordening van toepassing op de verwerking van persoonsgegevens door alle communautaire instellingen of organen, wanneer zij geheel of gedeeltelijk handelen in het kader van de eerste pijler.[123] De verordening ziet in beginsel op geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. In tegenstelling tot het Verdrag van Straatsburg kan de verordening ook van toepassing zijn op niet-geautomatiseerde verwerking van persoonsgegevens. Daarvan is sprake als de betreffende gegevens in een bestand zijn opgenomen of voor opname daarin bestemd zijn.[124] Het begrip 'persoonsgegeven' ziet op iedere informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[125] 'Identificeerbaar' betekent dat de persoon direct of indirect kan worden geïdentificeerd aan de hand van met name een identificatienummer of van één of meer specifieke elementen die voor zijn fysieke, fysiologische, psychische, economische, culturele of sociale identiteit kenmerkend zijn. Onder 'verwerken' wordt

118 Zie considerans nr. 5 van verordening 45/2001.

119 HvJ EG 20 mei 2003, *Österreichischer Rundfunk*, C-465/00, C-138/01 en C-139/01, *Jur*. 2003, p. I-4989, HvJ EG 6 november 2003, *Lindqvist*, C-101/01, *Jur*. 2003, p. I-12971 en HvJ EG 30 mei 2006, *Parlement t. Raad en Commissie*, C-317/04 en C-318/04, *Jur*. 2006, p. I-4721.

120 Zie § 7.3 en § 7.4.

121 Considerans 13 verordening 45/2001.

122 In het kader van de afbakening van het raakvlak tussen toegang tot documenten en bescherming van persoonsgegevens wordt in hoofdstuk 5 gedetailleerder ingegaan op de reikwijdte van verordening 45/2001.

123 Artikel 3 lid 1 verordening 45/2001. Bij deze bepaling wordt uitgebreider stilgestaan in § 3.4.3.1.

124 Artikel 3 lid 2 verordening 45/2001. Zie hierover uitgebreid § 5.2.2.

125 Artikel 2 sub a verordening 45/2001.

verstaan het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorgifte, verspreiden of op enige ander wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, evenals het afschermen, wissen of vernietigen van gegevens.[126] De omschrijving is gedetailleerder dan die onder het Verdrag van Straatsburg, bovendien valt het verzamelen van gegevens in verordening 45/2001 wél onder het begrip 'verwerken'.[127] Er moet sprake zijn van verwerking onder de verantwoordelijkheid van één van de communautaire instellingen of organen. De regels gelden daarom ook voor natuurlijke of rechtspersonen die voor rekening van een Europese instantie gegevens verwerken.[128]

Algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens

De algemene voorwaarden vormen als hoofdstuk II het meest substantiële deel van de verordening. Er zijn onder meer regels opgenomen over de kwaliteit van de gegevens, de toelaatbaarheid van de gegevensverwerking en de mogelijke uitzonderingen en beperkingen daarop, over bijzondere categorieën van gegevens, over de rechten van betrokkenen en over de vertrouwelijkheid en beveiliging van de verwerking.

- Ten aanzien van de *kwaliteit* van de gegevens bepaalt artikel 4 dat de persoonsgegevens eerlijk en rechtmatig moeten worden verwerkt. Het eerder onder artikel 8 EVRM besproken doelbindingsprincipe en de daaruit door het EHRM afgeleide vereisten zijn ook in artikel 4 terug te vinden.[129] De gegevens moeten zijn verkregen en worden verwerkt voor welbepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Daaraan wordt toegevoegd dat die gegevens vervolgens niet op een met die doeleinden onverenigbare wijze mogen worden verwerkt.[130] De gegevens moeten relevant zijn voor het beoogde doel en nauwkeurig. Daarnaast mogen de gegeven niet langer worden bewaard dan noodzakelijk. Onder bepaalde voorwaarden en in een beperkt aantal gevallen mag het doel van de verwerking worden gewijzigd.[131]
- Over de *verwerking* van persoonsgegevens wordt in artikel 5 bepaald dat deze alleen mag plaatsvinden als aan bepaalde voorwaarden is voldaan. Verwerking is toegestaan als dit noodzakelijk is voor de vervulling van een taak van algemeen belang of voor de uitvoer van het openbaar gezag.

126 Artikel 2 sub c verordening 45/2001.
127 Zie § 3.3.1.
128 Artikel 2 sub e verordening 45/2001.
129 Zie § 3.3.2.2.
130 Zie over deze toevoeging uitgebreid § 7.3.3.
131 Artikel 6 verordening 45/2001.

Daarnaast is verwerking toegestaan als dit noodzakelijk is om een wettelijke verplichting na te komen of voor de uitvoering van een overeenkomst. Ook is verwerking toegestaan als de betrokkene ondubbelzinnig toestemming heeft verleend of als het noodzakelijk is ter bescherming van een vitaal belang van de betrokkene.

- Voor *doorgifte van gegevens aan lidstaten of derden* die onder de werking van artikel 95/46 vallen, geldt dat dit enkel mag geschieden als de ontvanger aantoont dat de gegevens nodig zijn voor de uitvoering van een taak die wordt verricht in het algemeen belang of ter uitoefening van het openbaar gezag. Deze doorgifte is ook toegestaan als de ontvanger de noodzaak ervan aantoont en er geen reden bestaat om aan te nemen dat de belangen van de betrokkene worden geschaad.[132] Voor doorgifte van persoonsgegevens aan ontvangers die buiten de werking van richtlijn 95/46 vallen, bijvoorbeeld personen in derde landen, geldt dat deze doorgifte alleen is toegestaan als in het land van de ontvanger een 'passend beschermingsniveau' wordt gewaarborgd.[133] Bij twijfel is het aan de Commissie om te beoordelen of van een passend beschermingsniveau sprake is. Als de Commissie concludeert dat daarvan geen sprake is, dan is zij bevoegd in onderhandeling te treden met het derde land om tot een oplossing te komen.[134] Een voorbeeld van deze procedure, op basis van richtlijn 95/46, is de omstreden overeenkomst die in 2004 werd gesloten met de VS over de doorgifte van passagiersgegevens aan de Amerikaanse douaneautoriteiten. De overeenkomst werd uiteindelijk door het HvJ vernietigd.[135] Onder bepaalde omstandigheden, die vergelijkbaar zijn met de eerder genoemde voorwaarden voor verwerking, is doorgifte ondanks het ontbreken van een passend beschermingsniveau wel mogelijk.
- Voor een aantal *bijzondere categorieën gegevens* gelden strengere regels. Het gaat om gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, en voor gegevens die de gezondheid of het seksueel gedrag betreffen.[136] In beginsel is de verwerking van deze gegevens verboden. Uitzonderingen hierop zijn mogelijk onder andere als de betrokkene uitdrukkelijk heeft toegestemd, als de verwerking noodzakelijk is voor de bescherming van vitale belangen van de betrokken of voor de verdediging van een recht in rechte.[137] Ook is het verbod niet van toepassing als deze gegevens duidelijk door de betrokkene openbaar zijn gemaakt. Verwerking van strafrechtelijke gegevens is alleen toegestaan

132 Artikel 8 sub a en b verordening 45/2001.
133 Artikel 9 verordening 45/2001.
134 Artikel 9 verordening 45/2001 verwijst naar de regels van richtlijn 95/46, m.n. artikel 25.
135 Zie hierover uitgebreider § 8.2.2.1.
136 Artikel 10 verordening 45/2001.
137 De uitzonderingen zijn te vinden in artikel 10 lid 2-4 verordening 45/2001.

als dat door het EG-Verdrag is voorzien, of door een regeling op basis van het EG-Verdrag.[138]

- Worden de gegevens bij de betrokkene zelf verzameld, dan moet de communautaire instantie onder andere aan de betrokkene meedelen, wie de ontvangers zijn van gegevens, wat het doel is van de verwerking, wat de duur is van de bewaring en welke rechten de betrokkene heeft.[139] Nagenoeg dezelfde *informatieplicht* geldt als de gegevens bij een ander worden verzameld. Het tijdstip waarop deze informatie moet worden meegedeeld, is het tijdstip van registratie of het moment waarop verstrekking van de gegevens aan een derde wordt overwogen.[140]
- Met *rechten van de betrokkene* is bedoeld het recht op toegang tot de gegevens, de mogelijkheid direct rectificatie van onnauwkeurige of onvolledige persoonsgegevens te verlangen of de afscherming van de gegevens.[141] Ook kan het data subject in geval van onwettige verwerking het wissen van de gegevens verlangen.[142] De betrokkene kan verder verlangen dat de communautaire instantie de derde aan wie de gegevens zijn verstrekt van de bovengenoemde handelingen op de hoogte brengt.[143] Daarnaast heeft de betrokkene het recht om te worden ingelicht als de gegevens voor de eerste keer aan derden worden verstrekt voor *direct marketing*.[144] Tot slot heeft de betrokkene het recht om bij de betreffende instantie bezwaar te maken tegen de verwerking van zijn gegevens.[145] Als een data subject van mening is dat zijn rechten zijn geschonden dan kan hij naar het HvJ of naar de EDPS stappen.[146] Een beslissing van de EDPS is vatbaar voor beroep bij het Gerecht.[147]
- In artikel 20 is voor de communautaire instanties de mogelijkheid neergelegd om de toepassing van artikel 4 en de artikelen die de rechten van de betrokkene vastleggen, te *beperken*. Dit kan onder andere in het kader van preventie, onderzoek, opsporing en vervolging van strafbare feiten of voor de bescherming van de betrokkene of van de rechten en vrijheden van anderen.
- Instanties hebben de plicht om er voor te zorgen dat gegevens voldoende zijn *beveiligd*.[148] Personen die in dienst zijn van de instellingen en organen mogen alleen persoonsgegevens verwerken volgens de instructies van de

138 Artikel 10 lid 5 verordening 45/2001.
139 Artikel 11 verordening 45/2001.
140 Artikel 12 verordening 45/2001.
141 Artikel 13-15 verordening 45/2001.
142 Artikel 16 verordening 45/2001.
143 Artikel 17 verordening 45/2001.
144 Artikel 18 sub b verordening 45/2001.
145 Artikel 18 sub a verordening 45/2001.
146 Artikel 32 verordening 45/2001.
147 Artikel 32 lid 3 verordening 45/2001. Zie hierover Hijmans 2006-II, p. 1339-1341.
148 Artikel 22 verordening 45/2001.

eindverantwoordelijke voor de verwerking.[149] Elke communautaire instelling en elk communautair orgaan moet een *functionaris voor gegevensbescherming* instellen.[150] Schendt een personeelslid één van zijn verplichtingen onder de verordening, dan kan hij aan een tuchtmaatregel worden onderworpen.[151]

Toezicht op de naleving

Sinds januari 2004 is, zoals aangegeven, de EDPS actief.[152] Deze toezichthouder heeft als taak er voor te zorgen dat de fundamentele rechten en vrijheden van natuurlijke personen, en dan vooral het recht op persoonlijke levenssfeer, bij de verwerking van persoonsgegevens door de communautaire instellingen en organen in acht worden genomen.[153] Hij ziet toe op de naleving van verordening 45/2001 en andere communautaire besluiten over persoonsgegevens. De EDPS heeft daartoe verschillende bevoegdheden.[154] Deze bestaan uit de mogelijkheid om door particulieren gemelde schendingen voor te leggen aan de betrokken instantie, en voorstellen te doen om de schending te beëindigen; de mogelijkheid om waarschuwingen of berispingen uit te vaardigen, rectificatie of vernietiging te gelasten; een tijdelijk of definitief verwerkingsverbod op te leggen; de kwestie te rapporteren aan het Europees Parlement, de Raad of de Commissie; het HvJ te adiëren of te interveniëren in een aanhangig geding.[155] Ook kan de EDPS al dan niet op eigen initiatief adviezen uitvaardigen.[156]

Naast de mogelijkheid om een klacht in te dienen bij de EDPS kan een data subject ook de normale beroepswegen voor het Gerecht bewandelen.[157] Dan moet wel aan de gebruikelijke eisen voor ontvankelijkheid zijn voldaan. Als de betrokkene het niet eens is met de beslissing van de EDPS staat ook

149 Artikel 21 verordening 45/2001.
150 Artikel 24 verordening 45/2001.
151 Artikel 49 verordening 45/2001.
152 Zie § 3.2.2.
153 Artikel 41 verordening 45/2001. Zie hierover uitgebreid Hijmans 2006-II. Overigens is elke communautaire instelling en elk communautair orgaan verplicht een functionaris voor gegevensbescherming in te stellen. Deze draagt op onafhankelijke wijze zorg voor de interne toepassing van de bepalingen van verordening 45/2001 en is een aanspreekpunt voor de EDPS. Zie artikel 24-25 verordening 45/2001.
154 Artikel 47 verordening 45/2001.
155 Van de mogelijkheid om te interveniëren werd voor het eerst gebruik gemaakt in de eerdergenoemde zaak over de doorgifte van passagiersgegevens aan Amerikaans douaneautoriteiten. Het verzoek om interventie werd door het HvJ toegestaan. Zie de beschikkingen van het HvJ EG van 17 maart 2005, *Europees Parlement t. Raad*, C-317/04, *Jur*. 2005, p. I-2457 en *Europees Parlement t. Commissie*, C-318/04, *Jur*. 2005, p. I-2467. Zie over deze zaak verder § 8.2.2.1.
156 Artikel 46 sub d verordening 45/2001.
157 Zie de artikelen 230, 232 en 235 juncto 288 EG-Verdrag. Deze bepalingen komen hieronder in § 3.4.3 uitgebreider ter sprake.

de weg naar het Gerecht open.[158] Tot slot is een klacht tegen het gewraakte handelen van de Europese instellingen mogelijk bij de Europese Ombudsman.[159]

3.4.2.2 Specifieke regelgeving

Specifieke regelgeving is opgesteld omdat door bepaalde ontwikkelingen een vertaalslag van de algemene regels nodig was. Dit was vooral zo ten aanzien van elektronische communicatie die na het van kracht worden van richtlijn 95/46 een zeer snelle ontwikkeling doormaakte. Ook bestond er behoefte aan nadere regelgeving voor bepaalde sectoren.

Elektronische communicatie
In 2001 vaardigde de Commissie een mededeling uit met de titel '*e*Europe 2002'.[160] Deze mededeling paste in het streven om van de EU tegen 2010 de meest dynamische en meest concurrerende kenniseconomie ter wereld te maken.[161] Het doel van de mededeling was om het algehele gebruik van Internet te bevorderen, wat gepaard moest gaan met een gedegen bescherming van persoonsgegevens. De regelgeving over elektronische communicatie wordt met *eEurope 2002* in verband gebracht. Vijf richtlijnen vormen samen het gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten.[162] De meest relevante daarvan is richtlijn 2002/58, de opvolger van de eerder genoemde richtlijn 97/66. Richtlijn 2002/58 ziet specifiek op elektronische communicatie en bescherming van persoonsgegevens. Uit artikel 2 volgt dat de bepalingen van de richtlijn een specificatie van en een aanvulling op richtlijn 95/46 vormen.

Uiteraard is richtlijn 2002/58, net als richtlijn 95/46, gericht tot de lidstaten. Zoals aangegeven, zijn de bepalingen van richtlijn 95/46 en van richtlijn 97/66, de voorloper van richtlijn 2002/58, voor de communautaire instellingen en organen omgezet in verordening 45/2001. In deze verordening zijn dan ook regels opgenomen over de beveiliging van de telecommunicatienetwerken en het vertrouwelijke karakter van het communicatieverkeer.[163] Verder wordt bepaald wat er mag gebeuren met de verkeers- en rekeningsgegevens, en met

158 Artikel 32 lid 3 verordening 45/2001.
159 Artikel 21 en 195 lid 1 EG-Verdrag.
160 Mededeling van de Commissie van 13 maart 2001 (COM(2001)140 def., te vinden op http://europa.eu/scadplus/leg/en/lvb/l24226a.htm).
161 De zogenaamde strategie van Lissabon, deze is vervat in de conclusies van de Europese Raad van 23 en 24 maart 2000 (te vinden via http://europa.eu/european_council/conclusions/index_nl.htm).
162 Zie de richtlijnen 2002/19-22 van het Europees Parlement en de Raad van 7 maart 2002 (*Pb. EG* 2002, L 108/7) en de eerder genoemde richtlijn 2002/58.
163 Artikel 35 en 36 verordening 45/2001.

de gebruikerslijsten.[164] Tot slot is een bepaling gewijd aan de mogelijkheid van nummerherkenning.[165]

Het plan *e*Europe 2002 werd opgevolgd door *e*Europe 2005.[166] Dit was een tweede mededeling van de Commissie waarin op verzoek van de Europese Raad van Barcelona een actieplan werd geformuleerd om onder andere de kwaliteit en de toegankelijkheid van Internet te verbeteren. In februari 2003 nam de Raad een resolutie aan waarin het de doelstellingen van zowel *e*Europe 2002 als *e*Europe 2005 onderschreef.[167] In maart 2004 werd in navolging van *e*Europe 2005 een speciaal Europees Agentschap voor netwerk- en informatiebeveiliging opgericht (ENISA).[168] *e*Europe 2005 werd opgevolgd door iEurope 2010.[169]

Statistische gegevens en wetenschap

Al in de beginjaren van de EEG werd het voor een goede besluitvorming nodig geacht een dienst in te stellen die zich bezig zou houden met het verzamelen van statistische gegevens. In 1958 werd het Statistisch Bureau voor de Gemeenschappen opgericht, een bureau dat tegenwoordig bekend staat onder de naam Eurostat.[170] Eurostat hield en houdt zich bezig met het verzamelen van allerlei soorten gegevens, waaronder ook persoonsgegevens. Het huidige regelgevende kader voor de productie van communautaire statistieken wordt gevormd door verordening 322/97.[171] Ten aanzien van de bescherming van persoonsgegevens valt Eurostat in beginsel onder de werking van verordening 45/2001. Al in verordening 322/97 waren echter specifieke normen vastgelegd waaraan Eurostat zich diende te houden. Deze zien vooral op de communicatie tussen nationale statistische instanties en Eurostat. Kunnen de gegevens direct of indirect geïdentificeerd worden, dan moeten zij als vertrouwelijk worden beschouwd en geldt daarvoor een geheimhoudingsplicht. Zijn deze gegevens uit een nationale openbare bron afkomstig dan vervalt de vertrouwelijk-

164 Artikel 37 en 38 verordening 45/2001

165 Artikel 39 verordening 45/2001.

166 Mededeling van de Commissie van 28 mei 2002 (COM(2002)263 def., te vinden op http://ec.europa.eu/information_society/eeurope/2002/news_library/documents/eeurope2005/eeurope2005_nl.pdf).

167 Resolutie van de Raad van 18 februari 2003 (*Pb. EU* 2003, C 48/2).

168 Verordening 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 (*Pb. EU* 2004, L 77/1). Het Verenigd Koninkrijk heeft tegen deze verordening een vernietigingsactie ingesteld bij het HvJ omdat het meent dat een onjuiste rechtsbasis is gekozen. Zie de bevestigende conclusie van Advocaat-generaal Kokott van 22 september 2005, *Verenigd Koninkrijk t. Europees Parlement en Raad*, C-217/04, *Jur.* 2005, p. I-3771.

169 Zie hiervoor http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm.

170 De website van Eurostat is te vinden op http://epp.eurostat.ec.europa.eu, een uitgebreid historisch overzicht over het verzamelen van statistische gegevens in de E(E)G is via deze pagina te vinden.

171 Verordening 322/97 van de Raad van 17 februari 1997 (*Pb. EG* 1997, L 52/1).

heid.[172] Vertrouwelijke gegevens die niet tot *directe* identificatie kunnen leiden mogen tussen de nationale instanties en Eurostat worden overgedragen.[173]

Het doelbindingsbeginsel is ook terug te vinden in verordening 322/97. In artikel 15 wordt bepaald dat de persoonlijke gegevens uitsluitend voor statistische doeleinden gebruikt dienen te worden, tenzij de betrokkene expliciet toestemming heeft verleend voor verwerking met een ander doel. Nationale instanties en communautaire instanties kunnen gebruik maken van gegevens uit administratieve bestanden van hun eigen openbaar bestuur als dit noodzakelijk is voor de communautaire statistiek.[174] Dit lijkt in strijd met de doelbinding van de *oorspronkelijke* vergaring van de gegevens, maar in verordening 45/2001 is voor de verwerking van persoonsgegevens voor statistische doeleinden een uitzondering opgenomen.[175]

De enige mogelijkheid voor derden om toegang te verkrijgen tot vertrouwelijke gegevens uit handen van Eurostat is als dit een wetenschappelijk doel dient.[176] Deze toegang is aan voorwaarden onderhevig, die nader zijn uitgewerkt in verordening 831/2002.[177] De derde moet verbonden zijn aan een erkende universiteit of andere instelling voor hoger onderwijs, of aan een erkende wetenschappelijke onderzoeksinstantie.[178] Op de derde rust een geheimhoudingsplicht, die contractueel moet worden vastgelegd.[179] De derde krijgt de gegevens niet, maar kan ze alleen ter plaatse inzien.[180]

Persoonsgegevens van Euroambtenaren

De regels ten aanzien van Euroambtenaren zijn neergelegd in het zogenaamde Ambtenarenstatuut.[181] Hierin wordt niet expliciet verwezen naar verordening 45/2001. Het Ambtenarenstatuut kent wel een aantal specifieke bepalingen waarin over persoonsgegevens wordt gesproken. Zo stelt artikel 26 eisen aan de inhoud van het persoonsdossier en de toegang daartoe. Ook is in dit artikel bepaald dat het persoonsdossier voor derden geheim is en alleen geconsulteerd mag worden in de kantoorruimte van de administratie of via een veilig elektronisch medium.[182] In artikel 26a wordt de personeelsleden het recht toegekend op toegang tot hun medische gegevens.

In verordening 45/2001 zelf is een apart artikel gewijd aan de mogelijkheid voor '[e]enieder die in dienst is van een communautaire instelling of van een

172 Artikel 13 verordening 322/97.
173 Artikel 14 verordening 322/97.
174 Artikel 16 verordening 322/97.
175 Zie respectievelijk artikel 13 lid 2 richtlijn 95/46 en artikel 1 sub b verordening 45/2001.
176 Artikel 17 verordening 322/97.
177 Verordening 831/2002 van de Commissie van 17 mei 2002 (*Pb. EG* 2002, L 133/7).
178 Artikel 3 lid 1 verordening 831/2002.
179 Artikel 4 sub c verordening 831/2002.
180 Artikel 4 lid 2 en 5 verordening 831/2002.
181 Deze is te vinden op http://ec.europa.eu/civil_service/docs/toc100_en.pdf.
182 Zie over de verhouding van deze en andere bepalingen van het Ambtenarenstatuut tot de Eurowob § 2.4.9.

communautair orgaan' om rechtstreeks een klacht in te dienen bij de EDPS wegens een vermeende schending van een van de bepalingen uit de verordening.[183] Dat ook bij het verwerken van gegevens van Euroambtenaren de bepalingen van verordening 45/2001 van toepassing zijn, werd bevestigd door het Gerecht in de zaak *Voigt*.[184]

3.4.3 Bescherming van persoonsgegevens in de tweede en derde pijler: communautaire instellingen en organen[185]

3.4.3.1 De betekenis van artikel 3 lid 1 verordening 45/2001

In artikel 3 wordt over de reikwijdte van de verordening het volgende bepaald:

> De bepalingen van deze verordening zijn van toepassing op de verwerking van persoonsgegevens door alle communautaire instellingen of organen, voorzover die verwerking plaatsvindt ten behoeve van de uitvoering van werkzaamheden die geheel of gedeeltelijk onder het toepassingsgebied van het Gemeenschapsrecht vallen.

In dit artikel wordt een duidelijke keuze gemaakt: ook het grijze gebied tussen werkzaamheden in de eerste en de twee andere pijlers wordt binnen de reikwijdte van de verordening gebracht. Alleen het verwerken van persoonsgegevens in de uitvoering van werkzaamheden die *in het geheel buiten* het toepassingsgebied van het Gemeenschapsrecht vallen, wordt niet gedekt door verordening 45/2001.

Dit is een belangrijke keuze omdat in veel situaties niet altijd een onderscheid tussen werkzaamheden in de verschillende pijlers kan worden gemaakt. Een voorbeeld is de verwerking van persoonsgegevens van iemand die in dienst is bij de Commissie, maar expliciet is aangesteld om zich met derde pijler aangelegenheden bezig te houden. Deze verwerking valt, gedeeltelijk of zelfs helemaal, binnen het kader van de eerste pijler. Het zou een onwenselijke situatie opleveren als in die zin per werknemer een onderscheid gemaakt zou moeten worden. Het is dan ook zeer goed verdedigbaar dat op de verwerking van persoonsgegevens van álle werknemers van de communautaire instellingen of organen de regels van verordening 45/2001 van toepassing zijn. Het eerder aangehaalde artikel 33 uit verordening 45/2001, waarin de mogelijkheid voor een directe klacht bij de EDPS wordt gecreëerd, spreekt van '[*e*]*en-*

183 Artikel 33 verordening 45/2001.

184 GvEA EG 19 juni 2003, *Voigt t. ECB*, T-78/02, *Jur.* 2003, FP-IA-165, p. II-839, r.o. 71.

185 Zie over bescherming van persoonsgegevens in de derde pijler B. de Schutter, 'The processing of data in the police and judicial area and the protection of privacy', congresbijdrage februari 2003 (te vinden op http://www.era.int/web/en/resources/5_2341_645_file_en.716.pdf) en Hijmans 2006-I.

ieder die in dienst is van een communautaire instelling of van een communautair orgaan'.[186] Maar er zijn nog meer situaties die lastig los te zien zijn van de communautaire institutionele inbedding. Naast verwerking van de gegevens van personeelsleden zijn er meer administratieve handelingen van de instellingen en organen waarbij verwerking van persoonsgegevens plaatsvindt. Of die handelingen ten dienste staan van een activiteit verricht in de eerste pijler of in een van de twee andere pijlers is meestal niet duidelijk. Om die reden zijn ook op dit administratief handelen van de communautaire instellingen en organen de bepalingen van verordening 45/2001 van toepassing.

Voor het onderhavige onderzoek is ook de volgende situatie van belang. Tijdens een vergadering van de Raad komen dikwijls veel verschillende onderwerpen verspreid over de verschillende pijlers aan bod. Gesteld dat tijdens een vergadering genotuleerd wordt en in deze notulen bepaalde persoonsgegevens terug te vinden zijn, geldt dan voor het gehele document de werking van verordening 45/2001 of alleen ten aanzien van die delen waarin er over de eerste pijler werd gesproken? Voor het regime van toegang tot documenten is het in de praktijk in elk geval bijzonder lastig om een onderscheid te maken. De vraag of tegenover de Eurowob één normatief kader staat, namelijk verordening 45/2001, of meerdere, wordt in hoofdstuk 5 besproken.

Alleen de verwerking van persoonsgegevens door communautaire instellingen en organen die onderdeel is van de inhoudelijke werkzaamheden in de tweede en derde pijler, de echte veiligheidssamenwerking of politiële en justitiële samenwerking, valt buiten de reikwijdte van de verordening. In de tweede pijler is dat bijvoorbeeld het geval bij het opstellen van zogenaamde zwarte lijsten waarop personen vermeld staan die in verband worden gebracht met terroristische activiteiten en waarvan de financiële tegoeden moeten worden bevroren.[187] In de derde pijler worden persoonsgegevens voornamelijk door de lidstaten verwerkt. De verantwoordelijkheid voor de gegevensbescherming wordt in de wetgeving die van kracht is in de derde pijler ook nadrukkelijk bij de lidstaten gelegd. Zelfs als er bijvoorbeeld een gemeenschappelijke database in het leven wordt geroepen, blijven de lidstaten verantwoordelijk voor de gegevens. Dit is anders als er een speciale Europese instantie in het leven is geroepen, zoals Europol en Eurojust, die zelf bepaalde handelingen met de gegevens verricht.[188] Dan is alleen geen sprake van een communautaire instelling (zie hieronder in § 3.4.4).

---

186 Eigen cursivering. Zie § 3.4.2.1.

187 Zie over dit sanctieregime M.K. Bulterman, 'Oh, Baby, baby, it's a wide world: over terrorismebestrijding, financiële sancties en rechtsbescherming', *NJCM-Bulletin* 2005, p. 1069-1084.

188 Bij het SIS II, waar de Commissie een belangrijke rol in zal spelen, is dit anders, omdat dit informatiesysteem, zoals gezegd, zijn basis zal hebben in zowel het EG-Verdrag als het EU-Verdrag. In de voorstellen voor het SIS II is bepaald dat de bepalingen van verordening 45/2001 van toepassing zijn op de Commissie bij alle verwerking van persoonsgegevens in het kader van het SIS II. Considerans 15 van het SIS II voorstel, *supra* noot 45.

3.4.3.2 Artikel 8 EVRM en het Verdrag van Straatsburg

Voor het geval de communautaire instellingen toch persoonsgegevens verwerken in het kader van de tweede of derde pijler, wordt er in considerans 15 van verordening 45/2001 op gewezen dat dan de bescherming van de fundamentele rechten en vrijheden van personen dient te worden gewaarborgd met inachtneming van artikel 6 EU-Verdrag.[189] In dit Verdragsartikel is vastgelegd dat de Unie de grondrechten zoals onder andere neergelegd in het EVRM als algemene beginselen van Gemeenschapsrecht eerbiedigt.[190] Artikel 8 EVRM is één van die fundamentele rechten en via de jurisprudentie van het EHRM krijgt zo ook het Verdrag van Straatburg gelding.[191]

Hierbij dient een kanttekening te worden geplaatst. Deze gaat over de mogelijkheid van een individu om de eerbiediging van de grondrechten in rechte af te dwingen. Er is binnen de EU geen speciale rechtsweg naar het Hof van Justitie als een burger van mening is dat één van zijn fundamentele rechten is geschonden.[192] Hij zal gebruik moeten maken van de reguliere rechtsmiddelen en in de daaropvolgende procedure de schending van het mensenrecht als argument naar voren moeten brengen. In het kader van de eerste pijler is dit veelvuldig gebeurd bij een verzoek om nietigverklaring op grond van artikel 230 EG-Verdrag of in prejudiciële procedures op grond van artikel 234 EG-Verdrag.[193] Hoewel het HvJ al in een vroeg stadium aangaf de schending van een fundamenteel recht als een grond voor vernietiging te aanvaarden, vernietigde het pas in 1998 puur op basis van een schending van een fundamenteel recht een rechtshandeling van een Europese instelling.[194] Naast artikel 230 EG bestaat de mogelijkheid om op grond van artikel 235 juncto 288 EG-Verdrag een schadevergoedingsactie te starten wegens niet-contractuele aansprakelijkheid van de EG. Deze actie kan ook worden ingesteld

189 Considerans 15 verordening 45/2001.

190 Zie ook § 1.8. Zie over de EG en de relatie met het EVRM: R.A. Lawson, *Het EVRM en de Europese Gemeenschappen – Bouwstenen voor het optreden van internationale organisaties*, Deventer 1999, Kluwer (diss).

191 Zie daarover § 4.3.2.

192 Zie hierover ook H.R. Kranenborg & R.A. Lawson, 'Grondrechten in de ontwerp-Grondwet van de Europese Unie: een mooi resultaat met curieuze trekjes', *NJCM-Bulletin* 2003, p. 751-764, m.n. p. 760-763 en W. van Gerven, 'Remedies for Infringements of Fundamental Rights', *EPL* 2004, p. 261-284.

193 Zie bijv. HvJ EG 17 december 1970, *Internationale Handelsgesellschaft*, 11/70, *Jur*. 1970, p. 1125 en HvJ EG 14 mei 1974, *Nold t. Commissie*, 4/73, *Jur*. 1973, p. 491.

194 Het HvJ vernietigde een deel van de uitspraak van het Gerecht wegens schending van het recht op een eerlijk proces (artikel 6 EVRM), zie HvJ EG 17 december 1998, *Baustahlgewebe t. Commissie*, C-185/95 P, *Jur*. 1998, p. I-8417. De mogelijkheid hiertoe werd al eerder benoemd door het HvJ in *Nold t. Commissie*.

als de schade het gevolg is van een schending van een mensenrecht.[195] Een indirecte manier om een uitspraak van het HvJ te ontlokken over de conformiteit van Europese regelgeving met fundamentele rechten is via de prejudiciële procedure. Dan moet er wel een mogelijkheid zijn om een zaak op nationaal niveau aanhangig te maken.

De rechtsmiddelen die de burger ten dienste staan in de eerste pijler zijn niet dezelfde als in de tweede en derde pijler. Ten aanzien van de bepalingen die het gemeenschappelijk buitenlands en veiligheidsbeleid betreffen heeft het HvJ geen enkele bevoegdheid.[196] Over de politiële en justitiële samenwerking kan het HvJ zich wel uitspreken, zij het onder de voorwaarden die zijn neergelegd in artikel 35 EU-Verdrag. Hieruit blijkt dat een beroep tot nietigverklaring alleen kan worden ingesteld tegen besluiten en kaderbesluiten genomen door *de Raad* in het kader van de derde pijler.[197] Dit rechtsmiddel is verder alleen weggelegd voor de Commissie en de lidstaten. Een individu kan dus geen beroep tot nietigverklaring instellen. Ook is er in het EU-Verdrag niet voorzien in een mogelijkheid tot een verzoek om schadevergoeding zoals onder de eerste pijler. Het gevolg is dat de burger geen enkele directe beroepsmogelijkheid heeft. Wel is er voorzien in een prejudiciële procedure.[198] Maar deze mogelijkheid bestaat alleen als de betreffende lidstaat het HvJ hiertoe bevoegd

195 Zie bijv. GvEA EG 24 april 2002, *Elliniki Viomichania Opion AE t. Raad en Commissie*, T-220/96, *Jur*. 2002, p. II-2265, r.o. 27 en GvEA EG 10 april 2003, *Travelex t. Commissie*, T-195/00, *Jur*. 2003, p. II-1677, r.o. 150, waarin een verzoek om schadevergoeding mede gebaseerd werd op een beweerdelijke schending van het recht op eigendom zoals dat is neergelegd in artikel 1 protocol 1 van het EVRM. In beide zaken wees het Gerecht de verzoeken af. Zie ook GvEA EG 4 oktober 2006, *Tillack t. Commissie*, T-193/04, n.n.g., waarin om een schadevergoeding werd gevraagd vanwege een vermeende schending van de bescherming van het privé-leven en de woning, de persvrijheid, het beginsel van vermoeden van onschuld en het recht op een eerlijk proces. Omdat de beweerdelijke schendingen hoe dan ook niet de Europese instantie in kwestie (OLAF) kon worden verweten, slaagde het beroep niet.

196 Zie artikel 46 EU-Verdrag.

197 Artikel 35 lid 6 EU-Verdrag. Zie hierover uitgebreid D.M. Curtin & R.H. van Ooik, 'Een Hof van Justitie van de Europese *Unie*?', *SEW* 1999, p. 24-38. Zie ook L.A. Geelhoed & H. Hijmans, 'Het rechterlijk toezicht op de uitvoering van het gemeenschapsrecht in een Europabrede Unie', *SEW* 2002, p. 407-417.

198 Artikel 35 lid 1 EU-Verdrag. Zie voor een prejudiciële vraag over de verenigbaarheid van een kaderbesluit met grondrechten de conclusie van Advocaat-generaal Ruiz-Jarabo Colomer van 12 september 2006, *Advocaten voor de Wereld VZW t. Leden van de Ministerraad*, C-303/05, n.n.g. en de uitspraak van het HvJ EG van 3 mei 2007, *Advocaten voor de Wereld*, C-303/05, n.n.g.

heeft verklaard.[199] Daarbij kan de mogelijkheid om vragen te stellen beperkt worden tot de rechter in laatste instantie.[200]

Komt een zaak uiteindelijk voor het HvJ terecht dan is het wel expliciet bevoegd verklaard om artikel 6 lid 2 EU-Verdrag toe te passen.[201] Dat de bevoegdheid van het HvJ om over conformiteit met grondrechten te oordelen, beperkt wordt door de schaarse rechtsmiddelen in de tweede en derde pijler wordt bevestigd in de beschikking in de zaak *Segi*.[202] Segi was een Baskische organisatie die genoemd werd in een Annex bij gemeenschappelijk standpunt 2001/931 van de Raad dat was aangenomen onder de tweede en derde pijler in de strijd tegen het terrorisme.[203] Het handelen van de organisatie werd door de Spaanse rechter illegaal verklaard, en enkele leiders werden tot gevangenisstraffen veroordeeld. Toen Segi en twee van zijn leiders tegen de vermelding in de Annex in beroep wilden gaan en een schadevergoeding wilden claimen, bleek dat dat voor hen niet mogelijk was. Zij vonden dat deze onmogelijkheid om de zaak voor een rechter te brengen in strijd was met artikel 6 lid 1 en artikel 13 EVRM. Het Gerecht overwoog het volgende:

> Ook dient te worden opgemerkt dat de waarborg van de eerbiediging van de grondrechten krachtens artikel 6, lid 2, EU in casu irrelevant is, nu artikel 46, sub d, EU het Hof geen enkele bijkomende bevoegdheid verleent.[204]

Het Gerecht erkende vervolgens dat 'moet worden vastgesteld dat verzoekers waarschijnlijk niet over een effectief rechtsmiddel bij de Gemeenschapsrechter of de nationale rechter beschikken tegen de plaatsing van Segi op de lijst'.[205] De eventuele mogelijkheid om een prejudiciële vraag te stellen, strekt zich

199 Artikel 35 lid 2 EU-Verdrag. Zie over artikel 35 EU-Verdrag en de prejudiciële procedure HvJ EG 16 juni 2005, *Pupino*, C-105/03, *Jur*. 2005, p. I-5285. Van de 27 lidstaten hebben veertien een verklaring afgelegd in de zin van artikel 35 lid 2 en 3 EU-Verdrag (zie *Pb. EG* 1999, L 114/56; *Pb. EG* 1999, C 120/24; *Pb. EU* 2003, L 236/980 en *Pb. EU* 2005, L 327/19).

200 Artikel 35 lid 3 EU-Verdrag. Twee van de veertien landen beperken de mogelijkheid om prejudiciële vragen te stellen tot de nationale rechter in hoogste instantie.

201 Artikel 46 sub d EU-Verdrag.

202 GvEA EG 7 juni 2004, *Segi e.a. t. Raad* (beschikking), T-338/02, *Jur*. 2004, p. II-1647.

203 Gemeenschappelijk standpunt 2001/931/GBVB van de Raad van 27 december 2001 (*Pb. EG* 2001, L 344/93). Dit standpunt geeft uitvoer aan resolutie 1373(2001) van de VN Veiligheidsraad van 28 september 2001, te vinden op http://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf. Zie over financiële sanctie en het gebrek aan rechtsbescherming ook GvEA EG 21 september 2005, *Ahmed Ali Yusuf en Al Barakaar International Foundation t. Raad en Commissie*, T-306/01, *Jur*. 2005, p. II-3533 en GvEA EG 21 september 2005, *Yassin Abdullah Kadi t. Raad en Commissie*, T-315/01, *Jur*. 2005, p. II-3649. Zie ook H. Labayle, 'Architecte ou spectatrice? La Cour de Justice de l'Union dans l'Espace de liberté, sécurité et justice', *RTDE* 2006, p. 1-46, m.n. § III en over het sanctieregime Bulterman 2005.

204 GvEA, *Segi e.a.*, r.o. 37. Zie ook GvEA EG 12 december 2006, *Organisatie van Volksmujahedeen van Iran t. Raad*, T-228/02, n.n.g.

205 GvEA, *Segi e.a.*, r.o. 38.

namelijk niet uit tot de geldigheid en interpretatie van *gemeenschappelijke standpunten*.[206] Segi werd in zijn klacht niet-ontvankelijk verklaard.

Segi trof vervolgens een hogere voorziening bij het HvJ. In oktober 2006 verscheen de conclusie van Mengozzi, de Advocaat-generaal in deze zaak.[207] Hij voerde aan dat er wél een effectief rechtsmiddel bestaat, namelijk de gang naar de nationale rechter.[208] Gezien de verplichting om in een effectief rechtsmiddel te voorzien, is de nationale rechter volgens Mengozzi verplicht de geldigheid van de EU-lijst na te gaan.[209] Hiermee wijkt de AG af van de geldende leer in de *eerste* pijler, dat alleen het HvJ bevoegd is zich over de geldigheid van het Gemeenschapsrecht uit te spreken. Volgens Mengozzi is dit gerechtvaardigd omdat, in tegenstelling tot de eerste pijler, in de tweede en derde pijler geen sprake is van een volledig stelsel van rechtsmiddelen.[210] Dat er een risico is dat het Europese recht niet uniform wordt geïnterpreteerd, woog volgens Mengozzi niet op tegen het probleem dat er geen effectieve rechtsbescherming voor het individu is.[211] Het betoog van de AG werd uiteindelijk door het HvJ niet overgenomen.[212] Het HvJ overwoog dat er wél een indirecte rechtsgang mogelijk was, namelijk de prejudiciële procedure. Als een gemeenschappelijk standpunt, in tegenstelling tot het beoogde karakter, toch rechtsgevolgen blijk te hebben, dan moet het volgens het HvJ mogelijk zijn om een prejudiciële vraag te stellen over de rechtmatigheid ervan ook al wordt dit rechtsinstrument in artikel 35 EU-Verdrag niet genoemd.[213] Dat niet elke lidstaat de rechtsmacht van het HvJ voor de beantwoording van prejudiciële vragen heeft aanvaard, liet het HvJ verder onbesproken.[214]

De conclusie is dat artikel 8 EVRM en het Verdrag van Straatburg bij handelingen binnen de tweede en derde pijler conform artikel 6 EU-Verdrag weliswaar moeten worden geëerbiedigd, maar dat de juridische afdwingbaarheid ervan voor de Europese rechter voor de burger momenteel afwezig is of bijzonder mager. Dit staat in schril contrast met de eerste pijler, waarin naast het algemene (volledige) stelsel van rechtsbescherming in verordening 45/2001 voor de bescherming van persoonsgegevens ook nog eens extra toezicht door de EDPS inroepbaar is.

---

206 Zie artikel 35 lid 1 EU-Verdrag.
207 Conclusie van Advocaat-generaal Mengozzi van 26 oktober 2006, *Segi. e.a. t. Raad*, C-354/04 P en C-355/04 P, n.n.g.
208 Conclusie AG Mengozzi, *Segi e.a.*, para. 99.
209 Conclusie AG Mengozzi, *Segi e.a.*, para. 102.
210 Conclusie AG Mengozzi, *Segi e.a.*, para. 123.
211 Conclusie AG Mengozzi, *Segi e.a.*, para. 130.
212 HvJ EG 27 februari 2007, *Segi e.a. t. Raad*, C-355/04 P, n.n.g.
213 HvJ, *Segi e.a.*, r.o. 52-55.
214 Zie boven, voetnoot 199.

3.4.4 Bescherming van persoonsgegevens in de tweede en derde pijler: niet-communautaire instellingen en organen

3.4.4.1 Niet-communautaire instellingen en organen

Het aantal specifieke tweede en derde pijler organen is vrij beperkt. Onder de tweede pijler waren op het moment van afronding van dit onderzoek drie instanties opgericht: het instituut voor veiligheidsstudies van de Europese Unie, het satellietcentrum en het Europese defensie agentschap.[215] In de oprichtingsbesluiten is over de bescherming van persoonsgegevens niets bepaald. Er moet worden teruggevallen op artikel 8 EVRM en het Verdrag van Straatsburg. Onder de derde pijler zijn twee instanties opgericht: Europol en Eurojust. Zij kennen eigen regels over bescherming van persoonsgegevens.

3.4.4.2 Europol en het Europol-informatie systeem (politiële samenwerking)

Al in de eerder genoemde Schengen-uitvoeringsovereenkomst waren afspraken gemaakt tussen de betrokken landen over politiële samenwerking en de uitwisseling van informatie.[216] In 1995 werd op basis van het oude artikel K.3 van het EU-Verdrag de Europol-Overeenkomst gesloten.[217] De op te richten Europese Politiedienst (Europol) moest de samenwerking op het gebied van grensoverschrijdende criminaliteitsbestrijding ondersteunen, waarbij het verzamelen, analyseren en vergemakkelijken van het uitwisselen van informatie één van de primaire taken was.[218] Voor de vervulling van zijn taken werd Europol opgedragen een informatiesysteem aan te leggen en te beheren.[219] Nationale verbindingsofficieren moesten rechtstreeks informatie in dit systeem invoeren, en Europol zelf moest informatie invoegen die afkomstig was van derde staten of van de analyse van de aanwezige informatie. In november 2002 kreeg Europol meer operationele bevoegdheden toegekend.[220] Een gevoelig onderwerp was de mogelijke toegang van Europol tot het Schengen Informatie Systeem.[221] Na een lange discussie kreeg Europol in februari 2005

---

215 Gemeenschappelijk optreden 2001/554/GBVB van de Raad van 20 juli 2001 (*Pb. EG* 2001, L 200/1), Gemeenschappelijk optreden 2001/555/GBVB van de Raad van 20 juli 2001 (*Pb. EG* 2001, L 200/5) en Gemeenschappelijk optreden 2004/551/GBVB van de Raad van 12 juli 2004 (*Pb. EU* 2004, L 245/17).

216 Zie hierover C. Fijnaut, 'Police Co-operation and the Area of Freedom, Security and Justice', in N. Walker (ed.) *Europe's Area of Freedom, Security and Justice*, Oxford 2004, Oxford University Press, p. 249. Zie § 3.2.3.

217 Europol-overeenkomst (*Pb. EG* 1995, C 316/2). Artikel K.3 is gedeeltelijk terug te vinden in het huidige art. 30 EU-Verdrag.

218 Artikel 3 Europol-overeenkomst.

219 Artikel 7 Europol-overeenkomst.

220 Akte van de Raad van 28 november 2002 (*Pb. EG* 2002, C 312/1).

221 Zie § 3.2.3. Zie hierover Statewatch op http://www.statewatch.org/news/2002/mar/15europol.htm.

onder bepaalde voorwaarden het recht toegekend om het SIS te raadplegen.[222] Zo mocht Europol alleen zoeken naar gegevens die nodig waren voor het uitoefenen van zijn functies, was het gebruik van gevonden informatie onderworpen aan goedkeuring van de lidstaat vanwaar de gegevens afkomstig waren en moest Europol regelen dat alleen speciaal geautoriseerd personeel toegang tot het SIS had.[223]

Regels over de bescherming van persoonsgegevens zijn terug te vinden in de Europol-overeenkomst en in op deze overeenkomst gebaseerde specifieke regelingen.[224] Voor de Europol-overeenkomst was het Verdrag van Straatsburg de inspiratiebron. In de overeenkomst wordt Europol expliciet opgedragen rekening te houden met het Verdrag van Straatsburg en de aanbeveling van het CvM over het gebruik van persoonsgegevens op politieel gebied.[225] De beginselen van het Verdrag van Straatsburg zijn terug te vinden in de artikelen 17 tot 24 van de Europol-overeenkomst en in sommige gevallen zijn ze nader uitgewerkt in aparte besluiten van de Raad.[226] De wisselwerking tussen nationale instanties en Europol leidde tot een gecompliceerde regeling voor de bescherming van persoonsgegevens. Zo rust de verantwoordelijkheid voor de bescherming van bij Europol opgeslagen gegevens, vooral voor de rechtmatigheid van het verzamelen en de verstrekking aan Europol, alsook het invoeren, de juistheid en de actualiteit van de gegevens en het toezicht op de bewaartermijnen, in beginsel op de lidstaten.[227] Alleen als Europol gegevens van derden heeft verkregen of als gegevens het resultaat zijn van de analysewerkzaamheden van Europol zelf, is Europol verantwoordelijk voor de bescherming van deze gegevens.[228]

De afdwingbaarheid van de rechten van het data subject wijkt ook ten opzichte van Europol sterk af van de afdwingbaarheid in de eerste pijler. Het data subject krijgt wél een speciale buitengerechtelijke beroepsmogelijkheid toegekend. Artikel 24 van de Europol-overeenkomst is de rechtsgrondslag voor de oprichting van een gemeenschappelijk controle orgaan. Hetzelfde artikel geeft ieder individu het recht om een verzoek tot deze autoriteit te richten om te onderzoeken of Europol bij de verwerking van persoonsgegevens op de juiste wijze tewerk is gegaan.[229] De bevoegdheden van het controleorgaan

---

222 De SUO werd geamendeerd door het besluit 2005/211/JBZ van de Raad van 24 februari 2005 (*Pb. EU* 2005, L 68/44).

223 Deze en andere voorwaarden zijn te vinden in het nieuwe artikel 101A van de SUO.

224 Op het moment dat dit onderzoek werd afgerond, werd een nieuwe rechtsgrond voor Europol besproken. Op 20 december 2006 verscheen een voorstel van de Commissie voor een besluit van de Raad tot oprichting van de Europese Politiedienst (Europol) (COM(2006) 817 def.).

225 Artikel 14 lid 3 Europol-overeenkomst. Zie ook § 3.2.1.

226 Zie bijv. het besluit van de Raad van 12 maart 1999 over de vaststelling van regels over de verstrekking van persoonsgegevens aan derde staten en instanties (*Pb. EG* 1999, C 88/1).

227 Artikel 15 lid 1 sub 1 Europol-overeenkomst.

228 Artikel 15 lid 1 sub 3 Europol-overeenkomst.

229 Artikel 24 lid 4 Europol-overeenkomst.

gaan daarbij niet veel verder dan de mogelijkheid om de directeur van Europol te sommeren op zijn opmerkingen te antwoorden.[230]

Op de verwerking van persoonlijke gegevens van personeelsleden van Europol zijn aparte regels van toepassing. In het speciale statuut voor personeelsleden is een bepaling opgenomen over het personeelsdossier.[231] Deze bepaling is verder uitgewerkt in een apart besluit van de Raad van Bestuur van Europol.[232] In de considerans van dit besluit wordt direct verwezen naar het Verdrag van Straatburg en richtlijn 95/46. Een klacht van een van de personeelsleden over de bescherming van zijn persoonsgegevens kan uiteindelijk voor het HvJ worden gebracht.[233]

3.4.4.3 Eurojust (justitiële samenwerking)

In februari 2002 werd op basis van artikel 31 van het EU-Verdrag met een besluit van de Raad onder de derde pijler Eurojust formeel opgericht. Eurojust is een orgaan van de Unie met rechtspersoonlijkheid.[234] Eurojust bestaat uit officieren van justitie en rechters of politieambtenaren met een gelijkwaardige bevoegdheid. Het doel van Eurojust is om de bestrijding van ernstige vormen van criminaliteit te versterken.[235] In de considerans van het oprichtingsbesluit is aangegeven dat om deze doelstelling te bereiken, Eurojust persoonsgegevens zal verwerken.[236] In de regels over de verwerking van persoonsgegevens wordt een onderscheid gemaakt tussen verwerking van personeelsgegevens en gegevensverwerking in de inhoudelijke taakuitoefening van Eurojust. In artikel 30 van het Eurojust-besluit worden de Gemeenschapsregels ten aanzien van ambtenaren en andere personeelsleden van de EG op de personeelsleden van Eurojust van toepassing verklaard. Dit heeft tot gevolg dat ook de Gemeenschapsrechtelijke rechten die de personeelsleden van de communautaire instellingen en organen ontlenen aan verordening 45/2001 tot hun beschikking staan.

Een belangrijk deel van het Eurojust-besluit is gewijd aan de bescherming van persoonsgegevens. In tegenstelling tot Europol vindt veel van de verwerking van de persoonsgegevens wél onder de verantwoordelijkheid van Eurojust plaats. Net als in de Europol-overeenkomst dient het Verdrag van Straatburg als bron van inspiratie. De gestelde normen blijken ook ongeveer in lijn te zijn met verordening 45/2001. Als onderdeel van de interne regels van Eurojust is sinds 2005 een apart reglement van kracht dat ziet op de bescherming van

230 Artikel 24 lid 5 Europol-overeenkomst.
231 Artikel 23 besluit van de Raad van 3 december 1998 (*Pb. EG* 1999, C 26/23).
232 Besluit van de Raad van bestuur van Europol van 27 september 1999 (*Pb. EG* 2001, C 65/1).
233 Artikel 16 van het besluit van de Raad van bestuur van Europol.
234 Besluit 2002/187/JBZ van de Raad van 28 februari 2002 (Eurojust-besluit) (*Pb. EG* 2002, L 63/1), zie artikel 1.
235 Zie de eerste considerans en artikel 3 Eurojust-besluit.
236 Considerans 9 Eurojust-besluit.

persoonsgegevens. Dit reglement is in lijn met het Eurojust-besluit en kiest een structuur die zeer sterk lijkt op die van richtlijn 95/46 en verordening 45/2001.[237]

Weer is het belangrijkste verschil met de bescherming van persoonsgegevens onder de eerste pijler de juridische afdwingbaarheid van de rechten. Eurojust kent net als Europol een gemeenschappelijk controleorgaan. Dit orgaan heeft sterkere bevoegdheden dan het controleorgaan van Europol. Expliciet is bepaald dat de besluiten van het gemeenschappelijke controleorgaan definitief en bindend zijn.[238] Data subjecten kunnen zich tot dit controle orgaan wenden als zij van mening zijn dat één van hun rechten uit het Eurojust-besluit is geschonden.[239]

3.4.4.4 Kunnen handelingen van Europol en Eurojust door het HvJ worden vernietigd?

Als moet worden teruggevallen op de algemene rechtsbescherming onder de tweede en derde pijler, dan komt het data subject er niet al te best vanaf.[240] Ten aanzien van handelingen van Eurojust en Europol geldt bovendien een extra verschil dat leidt tot (nog) minder mogelijke rechterlijke controle. De eerder besproken vernietigingsactie uit artikel 35 EU-Verdrag is immers niet van toepassing op besluiten van één van beide instanties. De vernietigingsactie ziet namelijk alleen op besluiten en kaderbesluiten van de Raad. In december 2004 probeerde Advocaat-generaal Maduro in een door Spanje aangespannen zaak voor het HvJ tegen Eurojust hier verandering in aan te brengen.[241] In lijn met jurisprudentie van het HvJ ten aanzien van de vernietigingsactie uit artikel 230,[242] bepleitte hij uitvoerig dat het HvJ zou erkennen dat ook bindende besluiten van Eurojust ter vernietiging aan het HvJ voorgelegd moesten kunnen worden (door een lidstaat of de Commissie). Uiteindelijk wees het HvJ het beroep van de Spaanse regering af, omdat deze zijn actie helemaal niet op artikel 35 EU had gebaseerd maar, vreemd genoeg, alleen op artikel 230 EG-Verdrag.[243] Het pleidooi van AG Maduro is daarmee inhoudelijk niet verworpen. Het wachten is op een nieuwe zaak waarin dit onderwerp weer aan de orde komt.

---

237 Beschikkingen van het interne reglement betreffende de verwerking en bescherming van persoonsgegevens bij Eurojust (*Pb. EU* 2005, C 68/1).

238 Artikel 23 lid 8 Eurojust-besluit. Het reglement van orde van het Gemeenschappelijk controleorgaan is gepubliceerd in het publicatieblad van de EU 2004, C 86/1.

239 Zie artikel 19 lid 8 en artikel 20 lid 2 Eurojust-besluit.

240 Zie § 3.4.3.2.

241 Conclusie van Advocaat-generaal Maduro van 16 december 2004, *Spanje t. Eurojust*, C-160/03, *Jur*. 2005, p. I-2077.

242 Zie met name HvJ EG 23 april 1986, *Les Verts t. Europees Parlement*, 294/83, *Jur*. 1986, p. 1339.

243 HvJ EG 15 maart 2005, *Spanje t. Eurojust*, C-160/03, *Jur*. 2005, p. I-2077.

3.5 Conclusie

De bescherming van persoonsgegevens heeft in Europa een indrukwekkende ontwikkeling doorgemaakt. De eerste internationale samenwerking op dit gebied ontstond een kleine dertig jaar geleden binnen de Raad van Europa en de OESO. Later werden ook binnen de EEG en de EU regels over de bescherming van persoonsgegevens uitgewerkt. De laatste jaren is het (beoogde) gebruik van persoonsgegevens binnen de ruimte van vrijheid, veiligheid en rechtvaardigheid explosief toegenomen. Een belangrijke impuls hiervoor is de strijd tegen het terrorisme. Volgens het Haags Programma uit 2005 moet het toenemende gebruik van gegevens gepaard gaan met initiatieven om de bescherming van persoonsgegevens te versterken.

Binnen de EU als geheel is de bescherming van persoonsgegevens op dit moment niet uniform geregeld. Op de instellingen en organen van de Unie is binnen de eerste pijler verordening 45/2001 van toepassing. Voor verwerking van persoonsgegevens die (geheel) buiten de eerste pijler plaatsvindt, bestaat vooralsnog geen algemene regelgeving. In de derde pijler zijn wel bijzondere regelingen van kracht. In situaties waarin specifieke regelgeving ontbreekt, vormen artikel 8 EVRM en het Verdrag van Straatsburg het vangnet. Hoewel de normatieve verschillen tussen de regels in de eerste pijler en de tweede en derde pijler niet erg groot zijn, is er voor het individu wel een belangrijk verschil in de juridische afdwingbaarheid van de toegekende rechten voor de Europese rechter. Deze is momenteel namelijk nagenoeg afwezig in de tweede en derde pijler.

In dit hoofdstuk is de inhoud van het Verdrag van Straatsburg en van verordening 45/2001 besproken. Verordening 45/2001 is geïnspireerd op het Verdrag van Straatsburg, waardoor beide instrumenten in grote lijnen overeenkomen. Verordening 45/2001 is verder uitgewerkt en daardoor gedetailleerder. Daarnaast heeft verordening 45/2001 een bredere reikwijdte omdat zij onder bepaalde voorwaarden ook ziet op niet-geautomatiseerde verwerking. In dit hoofdstuk zijn ook de vereisten ten aanzien van de bescherming van persoonsgegevens onder artikel 8 EVRM weergegeven. Belangrijke elementen voor de rechtmatige verwerking van persoonsgegevens blijken te zijn: de rechtmatigheid van en binding aan het doel van de verwerking, de kwaliteit van de gegevens en de controlerechten van de betrokkene.