Persoonsregistraties als grensbewaking:

Europese ontwikkelingen inzake het gebruik van informatiesystemen en de toepassing van biometrie

Mr. E.R. Brouwer

Evelien Brouwer is onderzoeker bij het Centrum voor Migratierecht van de Katholieke Universiteit Nijmegen. Dit artikel is gebaseerd op een commentaar dat Brouwer in november 2003 schreef voor de Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht. Met dank aan Karin Alfenaar, Kees Groenendijk, Peter Rodrigues en Ashley Terlouw voor de door hen eerder gemaakte opmerkingen bij dit commentaar.

Trefwoorden: *grensbewaking, biometrie, SIS, VIS*

Met het oog op grensbewaking zullen de Europese regeringen in 2004 enkele besluiten nemen over de opslag en het gebruik van persoonsgegevens, inclusief het koppelen van databestanden. In Europese databestanden zullen biometrische gegevens worden opgeslagen, die ook zullen worden opgenomen in reis- en identiteitsdocumenten. Dit artikel formuleert enkele belangrijke uitgangspunten die ten grondslag moeten liggen aan de rechtmatige verwerking van persoonsgegevens in het kader van grensbewaking.

1 Inleiding

Naar verwachting zullen de Europese regeringen in 2004 besluiten nemen over verschillende voorstellen inzake het gebruik en de opslag van persoonsgegevens als middel voor grensbewaking. Deze voorstellen betreffen niet alleen de instelling van nieuwe databestanden, maar ook het verbinden van deze systemen, de uitbreiding van gebruikers van de bestaande systemen en de opname van nieuwe categorieën gegevens daarin. De lidstaten willen niet alleen een biometrisch gegeven (in de vorm van vingerafdruk, gezichtsherkenning of irisscan) aan de Europese informatiebestanden toevoegen, maar deze ook opnemen in de verplichte reis- of identiteitsdocumenten. Hierdoor kunnen onmiddellijk gegevens worden opgevraagd bij iedere grenspassage van een burger. Zoals bekend, verplicht de Amerikaanse overheid nu al de Europese luchtvaartmaatschappijen om passagiersgegevens aan Amerikaanse grensautoriteiten te verstrekken.[1] Echter ook op Europees niveau wordt een voorstel besproken voor een richtlijn die de luchtvaartmaatschappijen verplicht passagiersgegevens te verstrekken aan de Europese grensautoriteiten.[2]

Het is duidelijk dat deze ontwikkelingen met betrekking tot het gebruik en verwerking van persoonsgegevens gevolgen hebben voor de bescherming van individuele rechten. Personen, EU- en niet-EU-onderdanen, dreigen steeds vaker te worden geconfronteerd met beslissingen waarop zij weinig tot geen controle kunnen uitoefenen. Beslissingen die zijn gebaseerd op het gebruik van informatiebronnen waarvan de betrouwbaarheid en objectiviteit zullen afnemen naarmate er meer staten, instanties of particuliere ondernemingen bij zijn betrokken. In dit artikel worden enkele belangrijke uitgangspunten geformuleerd die in ieder geval ten grondslag moeten liggen aan de toekomstige regelingen inzake de voorgestelde informatiesystemen en het gebruik van biometrie. Omdat tot nu toe een duidelijk overzicht van de huidige ontwikkelingen ontbreekt, geef ik eerst een korte samenvatting van de belangrijkste bestaande systemen en van de voorgestelde maatregelen.

2 Huidige ontwikkelingen en voorstellen

2.1 *Operationele informatiesystemen in Europa*

In het kader van de Europese grensoverschrijdende samenwerking worden op dit moment door middel van verschillende systemen persoonsgegevens opgeslagen en uitgewisseld. Het op dit moment grootste Europese informatiebestand is het Schengen Informatie Systeem (SIS).[3] Deze databank bevat, behalve gegevens over voorwerpen, ook informatie over op te sporen personen, zoals getuigen en verdachten en personen die aan de grens moeten worden geweigerd.[4] Een andere grote database is het in 2003 operationeel geworden Eurodac. Dit bestand, dat vingerafdrukken bevat van asielzoekers, dient ter vaststelling van de voor de behandeling van een

1 *Zie de bijdragen van H. Kranenborg in NTER 2003, p. 162 e.v. en E.R. Brouwer in NJB 2003, p. 1548 e.v.*

2 *Zie Raadsdocument 11406/03 van 11 juli 2003. Een eerdere versie van dit Spaanse voorstel is gepubliceerd in PbEG 2003, C-82/23.*

3 *Dit systeem is geregeld in de Schengen Uitvoeringsovereenkomst van 19 juni 1990, Trb. 1990, 145.*

4 *Op dit moment bevat het SIS meer dan 10 miljoen signaleringen, waarvan één miljoen signaleringen over personen. 90% van die persoonsgegevens betreft derdelanders aan wie de toegang moet worden geweigerd.*

asielverzoek verantwoordelijke Europese staat, op basis van de zogenaamde Dublin II-verordening.[5] In het kader van de strafrechtelijke en justitiële samenwerking zijn er voorts de bestanden van de Europese organisaties Europol en Eurojust.

Het recht op bescherming van persoonsgegevens is in verschillende Europese instrumenten neergelegd. In de eerste plaats is er het Verdrag van de Raad van Europa inzake gegevensbescherming van 28 januari 1981.[6] Dit verdrag is zowel van toepassing op de gegevensverzameling van Europol en Eurojust als op het SIS. De Europese Richtlijn inzake de bescherming van persoonsgegevens van 24 oktober 1995[7] is van toepassing op gegevensverwerking in communautair verband. Onder de reikwijdte van deze richtlijn valt bijvoorbeeld Eurodac. Belangrijk voor de erkenning van het recht op gegevensbescherming als een zelfstandig grondrecht is de recente opname van het recht op gegevensbescherming in art. 8 van het EU Grondrechten Handvest. Ten slotte biedt ook de jurisprudentie van het Europees Hof voor de rechten van de mens in het kader van art. 8 EVRM, inzake het recht op privé-leven, belangrijke aanknopingspunten voor de noodzakelijke waarborgen bij de omgang met persoonsgegevens door de overheid. Genoemd kunnen worden het beginsel van proportionaliteit en subsidiariteit, de vereiste aanwezigheid van een onafhankelijk toezichtmechanisme en het legaliteitsbeginsel.[8]

2.2 Uitbreiding huidig SIS

Met betrekking tot de uitbreiding van het huidige SIS zijn in 2003 enkele concrete voorstellen voor akkoord bij de Raad ingediend. Deze voorstellen beogen slechts aanpassingen van het huidige systeem. In de eerste plaats is er het Spaanse voorstel voor een verordening en een besluit voor de uitbreiding van de functionaliteiten van SIS ten behoeve van terrorismebestrijding.[9] Dit voorstel voorziet in de (beperkte) toegang tot het SIS voor Europol en Eurojust, de regeling van een juridische basis van Sirene (organisatie die additionele informatie aan de nationale autoriteiten verstrekt bij de bovengenoemde SIS-signaleringen) en de regeling van de bewaartermijnen van de Sirenegegevens. Op grond van dit voorstel zullen ook enkele aanvullend op te nemen persoonsgegevens (bijvoorbeeld of iemand ontsnapt of gewapend is) in het SIS worden opgenomen. In de tweede plaats heeft de Commissie in augustus 2003 een voorstel ingediend voor een verordening op grond waarvan nationale organisaties belast met de afgifte van kentekenbewijzen toegang kunnen krijgen tot bepaalde categorieën gegevens (gestolen voertuigen en documenten) in het SIS.[10]

2.3 SIS II

Algemene en meer ingrijpende veranderingen vinden echter plaats in het kader van de besluitvorming over 'de ontwikkeling van het SIS van de tweede generatie', of kortweg 'SIS II'. De besluitvorming rond SIS II is oorspronkelijk bedoeld om het SIS technisch gebruiksklaar te maken voor een groter aantal landen. Deze wijziging is nodig met het oog op de toetreding van nieuwe EU-landen vanaf 2004. Deze praktische reden om SIS te wijzigen is echter ook aangegrepen om te onderhandelen over nieuwe doeleinden van het SIS, over nieuwe categorieën op te nemen gegevens en over nieuwe gebruikers van het SIS.[11] De lidstaten willen SIS II eind 2006 gereed hebben voor gebruik voor alle EU-lidstaten. Om deze datum te halen, zouden eind 2003 de besluiten moeten worden genomen over de voorgestelde functionele wijzigingen van het SIS. De belangrijkste voorstellen die op dit moment in de onderhandelingen over SIS II spelen zijn:

- Het verlaten van het huidige zogenaamde 'hit-no-hit'-systeem. Op dit moment wordt bij het aantreffen van een bepaald object of persoon in het SIS, een welomschreven actie van een bepaalde autoriteit gevraagd. De huidige voorstellen lijken van SIS een meer proactief informatiesysteem te maken. In plaats van alleen een meldingssysteem, zal het SIS een meldings- èn onderzoekssysteem worden.[12] Zo wordt voorgesteld om niet alleen gegevens op te nemen over personen die voor concrete doeleinden of acties worden gezocht, maar ook informatie over personen die mogelijk strafbare feiten zullen plegen, of mogelijk een gevaar voor de openbare orde of nationale veiligheid inhouden.
- De wijziging van de huidige architectuur: het huidige systeem bestaat uit een centraal systeem (CSIS), met in alle landen exacte kopieën van dat centrale systeem. Deze nationale SIS-bestanden (NSIS) zijn gebonden aan de algemene Schengenregels inzake gegevensbescherming die zijn neergelegd in de Schengen Uitvoeringsovereenkomst (hierna SUO). Het huidige recht verbiedt Schengenstaten om SIS-gegevens die door andere staten zijn ingebracht te kopiëren naar overige nationale bestanden. De Commissie stelt nu voor om één centrale database in te richten, waartoe nationale gebruikers via zogenaamde 'interfaces' direct toegang krijgen.[13] Het opslaan van de SIS-gegevens in nationale bestanden zou dan, volgens de Commissie, onder de eigen verantwoordelijkheid van die staten vallen.
- Koppeling van verschillende gegevensverzamelingen. Hierboven zagen we reeds dat de autoriteiten van de Europese organisaties Europol en Eurojust binnenkort rechtstreeks toegang krijgen tot bepaalde categorieën SIS-gegevens. In het kader van SIS II wordt echter ook de mogelijkheid besproken om SIS direct met andere Europese systemen te verbinden, zoals met de gegevensverzameling van Sirene,[14] met Eurodac of met het toekomstige Visum Informatie Systeem. In sommige Europese stukken wordt zelfs gesproken van de mogelijkheid om de verschillende systemen te integreren in één Europees Informatie Systeem.[15]
- Voorstel om zogenaamde interlinking van signalerin-

5 Verordening 343/2003, PbEG 2003, L 50/1.

6 ETS nr. 108.

7 95/46/EC, OJ 1995, L 281/31.

8 Zie onder andere het Leander-arrest, EHRM 26 maart 1987, Series A, no. 116; Amann vs. Switzerland, 16 februari 2000, Report of Judgements and Decisions 2000-II; ECtHR 7 juli 1989, Series A, no. 160; en Rotaru vs. Romania, 4 mei 2000, ECtHR 2000-V.

9 OJ 2002, C 160.

10 COM (2003) 510.

11 Zie onder meer de mededeling over SIS II van de Commissie, COM (2001) 720.

12 Zie de Commissie, die reeds in 2001 ervoor waarschuwde dat de opzet van het SIS fundamenteel zou wijzigen. COM (2001) 720, p. 8.

13 Zie de Commission Staff Working Paper inzake de ontwikkeling van SIS II van 18 februari 2003, SEC (2003) 206, opgenomen in het Raadsdocument 6615/03, 28 februari 2003.

14 Zie Raadsdocument 6172/03.

15 In een nota van het EU-voorzitterschap inzake derde pijler informatiesystemen wordt als een mogelijke optie voor de lange termijn genoemd 'het samenbrengen van alle bestaande systemen in één "Unie Informatie Systeem" zodat aan alle toekomstige behoeftes in alle relevante gebieden voldaan kan worden', Raadsdocument 8857/03 van 6 mei 2003. Ook het EP-rapport inzake de tweede generatie Schengen Informatie Systeem van de rapporteur Carlos Coelho, A5-0398/2003, 7 november 2003, noemt de mogelijkheid van één geïntegreerd systeem.

gen in het SIS mogelijk te maken: nu hebben van tevoren vastgestelde autoriteiten slechts toegang tot bepaalde categorieën gegevens. Interlinking zou het mogelijk maken dat een gebruiker die slechts toegang heeft tot een bepaalde categorie gegevens in verband met zijn functie, ook toegang krijgt tot andere aanwezige alerts over de gezochte persoon in het SIS, ook al heeft de gebruiker in verband met zijn functie primair geen toegang tot deze gegevens.
- Landen als de Verenigde Staten, maar ook buurlanden van nieuwe EU-staten hebben al hun belangstelling voor de door de Europese staten opgeslagen persoonsgegevens getoond. Ook over de toegang van deze derdestaten zal een besluit moeten worden genomen.
- Toegang van het Verenigd Koninkrijk en Ierland: ook al participeren deze landen op dit moment niet in de EU-samenwerking op het gebied van asiel en migratie, op grond van het Raadsbesluit 2000/365/EG zullen deze landen wel toegang tot het SIS krijgen voor wat betreft de justitiële en politiële gegevens. Onderhandelingen vinden echter ook plaats over de toegang van deze landen tot gegevens over visa en te weigeren vreemdelingen.[16]
- Beheer en plaats van het SIS: op dit moment is het centrale SIS (CSIS) gesitueerd in Straatsburg en valt het onder beheer van de Raad. Het Europees Parlement en de Commissie stellen voor om SIS door een zelfstandig agentschap te laten beheren.

Op 11 december 2003 publiceerde de Commissie een mededeling over de ontwikkeling van het tweede generatie SIS.[17] Volgens de planning van de Commissie kan het SIS II in de periode 2006-2007 operationeel worden gemaakt. Dan zal echter, volgende de Commissie in deze mededeling, de politieke besluitvorming over de nieuwe functies van het SIS II uiterlijk juni 2004 moeten zijn afgerond. Uit de mededeling blijkt ook dat de Commissie voorstander is van de opname van biometrische gegevens in het SIS en van een zekere mate van technische integratie van het SIS met het toekomstige Visum Informatie Systeem (zie over beide onderwerpen de volgende paragrafen).

2.4 *Visum Informatie Systeem*

Het Visum Informatie Systeem (hierna VIS) betreft het voorstel voor een centrale Europese database waarmee informatie over visa die door de EU-staten zijn verstrekt of geweigerd, kan worden uitgewisseld. Dit systeem zou niet alleen gegevens moeten gaan bevatten over de afgegeven visa, maar ook over iedere visumaanvraag èn visumweigering. In juni 2002 hebben de Ministers van Justitie en Binnenlandse Zaken reeds richtsnoeren aangenomen voor de instelling van een gemeenschappelijk systeem voor de uitwisseling van informatie over visa.[18] Uit de in deze richtsnoeren genoemde doeleinden kan men afleiden dat het toekomstige VIS een multifunctioneel systeem moet worden.[19] Zo worden als doeleinden van het VIS genoemd:
- de vergemakkelijking van fraudebestrijding door middel van betere uitwisseling van informatie inzake visumaanvragen tussen de lidstaten (daarbij is niet aangegeven welke fraude wordt bedoeld);
- betere consulaire samenwerking op lokaal niveau en uitwisseling van gegevens tussen centrale autoriteiten die bevoegd zijn voor consulaire samenwerking;
- de verbetering van de methode om vast te stellen of de bezitter van een visum en de wettige houder ervan één en dezelfde persoon zijn;
- de bestrijding van het zogenaamde 'visumshopping' (wanneer een aanvrager, na weigering door één consulaat, bij een consulaat van een andere lidstaat een visumverzoek indient);
- het vereenvoudigen van identificatie in het kader van de Dublin II-verordening en terugkeerprocedures;
- een beter beheer van een gemeenschappelijk visumbeleid en
- het leveren van een bijdrage aan de interne veiligheid en bestrijding van terrorisme.

De Raad moet, op het moment van schrijven, nog een politiek akkoord bereiken over de basiselementen van VIS, zoals:
- de architectuur: een systeem vergelijkbaar met het huidige SIS (dus een centrale opzet met nationale kopieën in iedere lidstaat), of een systeem dat is geïntegreerd met SIS, of een geheel nieuwe structuur;
- de vaststelling van de definitieve doeleinden;
- een regeling van gebruikers;
- de toegang voor derdestaten en
- de opname (en de keuze) van biometrische gegevens.

Door de Europese Raad wordt, tijdens hun bijeenkomst in Brussel van 12 december 2003, op een spoedige besluitvorming door de Raad inzake de ontwikkeling van het VIS aangedrongen.[20] Inhoudelijke voorstellen hiertoe zijn te vinden in ontwerpconclusies van de Raad van november 2003.[21] Op grond van deze ontwerpconclusies zouden in het VIS niet alleen gegevens worden opgenomen over aangevraagde en afgegeven visa, maar ook over geweigerde, nietig verklaarde, ingetrokken en verlengde visa. Naast identificerende gegevens over de aanvrager zal in het VIS een digitale foto van de aanvrager, informatie over de verzekeringspolis worden opgenomen en op termijn ook biometrische gegevens (zie ook de volgende paragraaf). Ten slotte zal, op grond van dit voorstel, het VIS ook gegevens bevatten over de personen die de visa-aanvrager hebben uitgenodigd en over de personen die instaan voor de kosten van verblijf en levensonderhoud. Volgens het voorstel moeten de volgende autoriteiten toegang tot het VIS krijgen: de grenscontrole- en immigratiediensten, de politieautoriteiten en de diensten die verantwoordelijk zijn voor de binnenlandse veiligheid.

16 *Zie de nota van het Verenigd Koninkrijk van 25 maart 2003, Raadsdocument 7786/03.*

17 *COM (2003) 771, 11 december 2003. Doordat dit rapport op het moment van afronding van mijn bijdrage is verschenen, was ik niet meer in de gelegenheid om hierop uitgebreid in te gaan.*

18 *Zie Raadsdocument 9615/02 van 5 juni 2002.*

19 *Zie ook de mededeling van de Commissie over een gemeenschappelijk beleid inzake illegale immigratie, mensenhandel en mensensmokkel, COM (2003) 323, juni 2003.*

20 *Conclusies van het voorzitterschap, 12 december 2003, Brussel.*

21 *Zie Raadsdocument 14776/03, 13 november 2003.*

Voorzover de autoriteiten hiertoe bevoegd zijn, mogen VIS-gebruikers de gegevens in het hierboven genoemde SIS raadplegen en vice versa.[22]

2.5 Opname biometrische gegevens

Op nationaal niveau bereiden verschillende Europese lidstaten reeds wetgeving voor ter opname van biometrische gegevens in alle identiteitsdocumenten, ook in die van EU-onderdanen. Deze wetgeving vloeit onder meer voort uit een maatregel die de Amerikaanse overheid heeft ingevoerd na de gebeurtenissen van 11 september 2001. Op basis van deze maatregel dienen alle landen waarvan de onderdanen van een visum zijn vrijgesteld, de reisdocumenten van hun onderdanen van biometrische gegevens te voorzien. Gebeurt dit niet, dan vervalt voor dat land de visumvrijstelling op basis van het zogenaamde Amerikaanse Visa Waiver Program. Er wordt echter ook Europese wetgeving voorbereid inzake het gebruik van biometrie. In september 2003 heeft de Commissie voorstellen ingediend die het mogelijk maken om biometrische gegevens op te nemen in zowel de visa, als de verblijfsdocumenten van derdelanders.[23] In deze voorstellen geeft de Commissie de voorkeur aan de opname van (twee) vingerafdrukken en een digitale fotoafdruk. Eerder heeft de Europese Commissie aangekondigd dat zij ook voorstellen zal indienen voor de opname van veiligheidskenmerken, waaronder biometrische gegevens, in de paspoorten van EU-onderdanen.[24]

Daarnaast onderhandelen de lidstaten, zoals we hierboven al zagen, ook over de opname van biometrische gegevens in zowel het SIS II als het VIS.[25] Bij deze discussie gaat het niet meer over de vraag òf deze gegevens wel in een centraal informatiebestand mogen worden opgenomen, maar over de vorm van biometrische gegevens die zal worden gekozen.[26]

3 Algemene kritiekpunten

3.1 Gebrek aan democratische en inhoudelijke legitimatie

Een goede besluitvorming vereist een openbare afweging van nut en effectiviteit van voorgestelde systemen enerzijds, tegenover de financiële kosten en de bescherming van individuele rechten anderzijds. De Europese bewindslieden geven aan dat de politieke besluitvorming over de bovenbeschreven onderwerpen eind 2003-begin 2004 moet zijn afgerond. De EU-lidstaten lijken echter al over de principiële punten, zoals de invoering van het VIS, de uitbreiding van de taken van het huidige SIS en het gebruik van biometrie, hun besluiten te hebben genomen, zonder dat hier enig parlementair debat aan vooraf is gegaan. Een structureel en publiek debat over concrete voorstellen ontbreekt: mondjesmaat worden door hetzij de Commissie, hetzij de verschillende lidstaten, voorstellen gedaan over mogelijke doelen, categorieën op te nemen gegevens of gebruikers van de toekomstige systemen. De haalbaarheidstudie inzake het VIS die de Commissie in mei 2003 aan de Raad heeft gestuurd, is tot nu toe niet publiek gemaakt. Hierdoor blijft het onhelder of, en zo ja welke afweging er is gemaakt tussen enerzijds de verwachte voordelen van het VIS, en anderzijds de betrokken rechten en belangen van individuen. Er dreigt een legitimatie achteraf plaats te vinden van een materie die niet alleen zeer ingewikkeld is, maar ook ingrijpende gevolgen kan hebben voor de rechten en vrijheden van Europese burgers en derdelanders.

De besluitvorming over het opzetten van nieuwe informatiesystemen of het uitbreiden van de huidige systemen vereist bovendien een voorafgaande evaluatie van de bestaande instrumenten.

Lidstaten zullen moeten aangeven wat het effect van de bestaande instrumenten is en waar deze instrumenten met het oog op de gestelde doelen falen. Pas na zo'n evaluatie kan, in een democratisch kader en in nauw overleg met de nationale en internationale toezichtorganen inzake de gegevensbescherming, een afgewogen besluit worden genomen over nieuwe maatregelen. Wat betreft het gebruik van het huidige SIS, wordt meermalen verwezen naar het nut van dit systeem, onder meer gezien het groot aantal hits (dat wil zeggen dat een gebruiker een bepaald persoon aantreft in het systeem). Cijfers over de bijdrage die deze hits daadwerkelijk leveren aan de bestrijding van criminaliteit of aan andere met het SIS gestelde doeleinden, zijn er niet, althans zijn niet publiek bekend gemaakt. Een belangrijk probleem ten aanzien van het huidige SIS is het ontbreken van openbare rapporten over het functioneren van dit systeem. De jaarverslagen van het bij het SIS ingestelde toezichtorgaan, de GCA, geven wel enig inzicht in het gebruik van het SIS, maar bestrijken slechts een deelaspect van het gebruik van SIS, namelijk de gegevensbescherming.

Ook wat betreft de voorgestelde opname van biometrische gegevens is onvoldoende onderbouwd wat het precieze doel en meerwaarde is van deze opname. De lidstaten geven niet aan wat de gevolgen van het gebruik van biometrie zijn, noch in hoeverre de betrouwbaarheid van deze gegevens kan worden gegarandeerd. In dit kader is het veelzeggend dat de Groep Gegevensbescherming Artikel 29, een Europees adviesorgaan op het gebied van gegevensbescherming, recent kanttekeningen heeft geplaatst bij het opslaan van biometrische gegevens.[27] In een advies van augustus 2003 geeft de werkgroep expliciet aan dat ieder besluit over gebruik van biometrie aan het proportionaliteitsvereiste moet voldoen. De werkgroep adviseert om biometrische gegevens niet in een centraal databestand op te nemen. Bovendien verwijst de werkgroep naar de kritische opstelling van verschillende nationale autoriteiten voor de gegevensbescherming inzake het gebruik van biometrie.

22 Zoals hierboven aangegeven, gaat de Commissie in haar recente mededeling, COM (2003) 771, van 11 december 2003 ook in op de mogelijke integratie van het VIS met SIS II.

23 Voorstel van 25 september 2003, COM (2003) 558. Tijdens de Raad van Ministers van Justitie en Binnenlandse Zaken van 27-28 november 2003 is algemene instemming bereikt over dit voorstel, Raadsdocument 14995/03 (Presse 334).

24 COM (2003) 323, 3 juni 2003, p. 6.

25 Zie bijvoorbeeld Raadsdocument 10857/03.

26 Zie ten aanzien van het VIS, de conclusies van de Raad van Justitie en Binnenlandse Zaken op 27-28 november 2003, Raadsdocument 14995/03 (Presse 334). Zie ten aanzien van het SIS, de recente mededeling van de Commissie COM (2003) 771.

27 Werkdocument over biometrie, aangenomen op 1 augustus 2003, 12168/02/NL WP 80. De Groep Gegevensbescherming Artikel 29 is op basis van art. 29 van Richtlijn nr. 95/46/EG ingesteld.

3.2 *Gebrek aan transparantie van huidige regelgeving inzake gegevensbescherming*

Richtlijn nr. 95/46/EG inzake gegevensbescherming is niet van toepassing op het SIS, omdat de rechtsgrondslag van het SIS berust op de huidige derde pijler van het EU-Verdrag en de genoemde richtlijn alleen van toepassing is op communautaire gegevensverwerking. Van de zijde van de Commissie is aangegeven dat, met het oog op de opheffing van het verschil tussen de drie pijlers in het kader van het ontwerp Constitutioneel Verdrag, het SIS II in de toekomst één rechtsbasis, met ook één regeling voor de gegevensbescherming dient te krijgen. Zolang echter de besluitvorming rond het Constitutioneel Verdrag niet is afgerond, zal de Commissie de wetgevingsvoorstellen inzake SIS II nog op twee rechtsgrondslagen baseren.[28]

Zoals we hierboven zagen is de EG-richtlijn wel van toepassing op Eurodac en zal deze, gezien de communautaire rechtsgrondslag daarvan, ook van toepassing zijn op het toekomstige VIS. De EG-richtlijn is echter niet van toepassing op de persoonsbestanden van Europol, Eurojust, en tot nu toe, het SIS. Hierdoor ontstaat een vreemde tweedeling tussen de normen van het Dataprotectieverdrag van de Raad van Europa en de daarop gebaseerde aanbevelingen enerzijds en de communautaire regels inzake gegevensbescherming anderzijds. Bovendien hebben systemen als SIS, Europol en Eurodac ook nog eens hun eigen regelingen inzake gegevensbescherming met een afzonderlijk toezichtmechanisme. Dit naast elkaar bestaan van verschillende dataprotectieregimes komt de transparantie van het toepasselijke recht niet ten goede. De opname van het recht op gegevensbescherming in art. 8 van het EU Charter is een belangrijke stap naar de erkenning van een pijleroverschrijdend individueel grondrecht op een adequate gegevensbescherming. Art. 50 van de ontwerp Constitutioneel Verdrag bevat bovendien de opdracht aan de EU-wetgever om één EU-regeling inzake gegevensbescherming op te stellen en één autoriteit te belasten met de gegevensbescherming. Een voorstel om eenvormige regels voor de derde pijler te ontwikkelen is tijdens de Raad van juni 2003 door de Griekse delegatie aan de Raad voorgelegd. Tot nu toe lijkt de Raad echter weinig gevolg aan dit voorstel te geven.[29]

Ten behoeve van de transparantie voor de burgers zou het de aanbeveling verdienen wanneer gegevensverwerking en informatiesystemen onder één gemeenschappelijk kader van gegevensbescherming komen. Deze algemene regels zouden dan per sector of onderwerp kunnen worden uitgewerkt in meer specifieke regels. Deze specifieke regels mogen dan echter geen afbreuk doen aan de basisbeginselen.

4 Concrete aanbevelingen

4.1 *Doelbindingsbeginsel*

Eén van de belangrijkste uitgangspunten van gegevensbescherming is het doelbindingsbeginsel. Dit houdt in de eerste plaats in dat de EU-lidstaten alleen gegevens mogen verwerken voor een specifiek, expliciet en legitiem doel. De lidstaten moeten bij ieder besluit op het gebied van de verwerking van persoonsgegevens expliciet aangeven wat het doel van deze gegevensverwerking is. Het legitimiteitvereiste houdt echter ook in dat lidstaten moeten aangeven waarom het gekozen instrument tot het beoogde doel bijdraagt. Deze motiveringsplicht vloeit ook voort uit de beginselen van noodzakelijkheid en proportionaliteit, zoals die zijn geformuleerd door het Europees Hof voor de rechten van de mens in jurisprudentie rond art. 8 EVRM.[30]

Het doelbindingsbeginsel houdt in dat opgeslagen of verzamelde persoonsgegevens niet voor andere doeleinden mogen worden gebruikt. Naleving van dit beginsel zal moeilijker te garanderen zijn, naarmate het informatiesysteem grootschaliger is en naarmate er meer staten en autoriteiten gebruik van maken. Tot nu toe lijken de lidstaten bij de besluitvorming over toekomstige systemen dit aspect niet expliciet mee te wegen.

4.2 *Op te nemen gegevens*

Op grond van het genoemde doelbindingsbeginsel dienen de te verwerken gegevens adequaat, relevant en niet excessief in het licht van het beoogde doel te zijn.[31] Dit betekent dat de lidstaten voor iedere categorie gegevens die zij in Europese databanken willen opnemen, de relevantie en proportionaliteit moeten vaststellen, in het licht van het doel waarvoor deze gegevens zullen worden gebruikt. Daarbij is het soort gegevens dat mag worden opgenomen, afhankelijk van de aard en reikwijdte van het beoogde gebruik van deze gegevens. Hoe ruimer het gebruik en hoe meer autoriteiten toegang hebben tot het systeem, des te strenger de eisen met betrekking tot de adequaatheid en juistheid van de gegevens zullen moeten zijn.

In het kader van SIS II, maar eventueel ook van het VIS, moet een principiële keuze worden gemaakt tussen een systeem van wederzijdse erkenning van nationale beslissingen om iemand in een systeem op te nemen, of een systeem waarbij de criteria voor de opname van een persoon (of object) in een systeem volledig zijn geharmoniseerd. Op dit moment kent het SIS een gemengd systeem. De regeling van het SIS, de Schengen Uitvoeringsovereenkomst, beschrijft welke personen (of objecten) voor welke doeleinden in het SIS mogen worden opgenomen. Deze criteria zijn echter vaag en laten ruimte voor verschillen in invulling door de Schengenstaten. Daarnaast is de regeling van het SIS gebaseerd op het beginsel van wederzijdse erkenning.

28 *Aldus Commissaris Vitorino in zijn speech tijdens een seminar over SIS II dat plaatsvond in het Europees Parlement op 6 oktober 2003.*

29 *Zie het verslag van de Raad van Ministers van Justitie en Binnenlandse Zaken van 5-6 juni 2003, Raadsdocument 9845/03.*

30 *Bijvoorbeeld in de bekende uitspraken in het Klass-arrest, 6 september 1978, Series A 28 en het Leander-arrest, 26 maart 1987, Series A 116.*

31 *Zie bijvoorbeeld art. 6 (c) Richtlijn nr. 95/46/EG.*

Bijvoorbeeld wanneer één staat een vreemdeling op nationale gronden toegang tot het grondgebied wil weigeren en deze persoon daartoe in het SIS opneemt, dan zal deze persoon ook de toegang tot alle andere Schengenstaten worden geweigerd.

De nationale verschillen in de uitvoering en het gebruik van het SIS bemoeilijken de controle door toezichtorganen of rechter. Daarnaast kleeft aan het systeem van wederzijdse erkenning het nadeel van ondoorzichtigheid en een mate van willekeur tegenover de persoon die in het systeem wordt opgenomen. Duidelijke, nauwkeurig omschreven criteria voor opname van gegevens in een Europees informatiesysteem verdienen daarom de voorkeur boven een systeem van wederzijdse erkenning van nationale besluiten.

Met name in de nasleep van de gebeurtenissen van 11 september 2001, zijn in het kader van de discussie rond SIS II door de afzonderlijke lidstaten verschillende voorstellen gedaan ter opname van nieuwe categorieën gegevens. De voorgestelde categorieën variëren van 'gewelddadige ordeverstoorders', 'potentieel gevaarlijke personen die van bepaalde evenementen moeten worden uitgesloten', en 'personen ten aanzien van wie moet worden voorkomen dat ze het Schengengebied verlaten'.[32]

Maar zoals reeds aangegeven, bevat ook de huidige regeling van het SIS vage criteria, zoals bijvoorbeeld 'vreemdelingen die een gevaar voor de openbare orde en veiligheid of de nationale veiligheid kunnen opleveren' in art. 96 SUO. Dergelijke omschrijvingen laten toe dat personen in het SIS worden opgenomen, louter en alleen op basis van een vermoeden, zonder dat hiervoor aan nadere criteria moet zijn voldaan.

Het is van groot belang dat grootschalige, multifunctionele informatiesystemen enkel zogenaamde 'harde gegevens' bevatten, dat wil zeggen informatie waarvan vooraf is getoetst dat die een werkelijke situatie of eigenschap weergeeft en die niet is gebaseerd op vermoedens of op het gebruik van zogenaamde profielen. Zogenaamde 'zachte' informatie, die opsporings- of veiligheidsdiensten nodig hebben bij hun taken, horen thuis in aparte (analyse-)bestanden, waarvan de gebruiker van tevoren weet dat deze informatie nader moet worden getoetst. Deze informatie mag alleen worden gebruikt voor verder onderzoek en niet voor vervolging of weigering aan de grens.

4.3 Gebruikers – toegang aan derden

In de huidige onderhandelingen over SIS II worden voorstellen gedaan ter uitbreiding van gebruikers van het SIS: zowel van nationale autoriteiten als van derdestaten. Het huidige SIS is gebaseerd op het principe dat van tevoren vastgestelde gebruikers slechts toegang hebben tot bepaalde categorieën van gegevens, waarvan van tevoren is vastgesteld dat zij die voor de uitvoering van hun taak nodig hebben. Dit beginsel dient ook het uitgangspunt te blijven bij het toekomstige SIS, maar ook bij andere toekomstige informatiesystemen. Voor een transparante regeling is het ook noodzakelijk dat wanneer besluiten zijn genomen over de gebruikers, de lidstaten de lijsten met deze gebruikers aan het nationale en het Europees parlement overleggen of anderszins openbaar maken.

Wanneer SIS II, en eventueel VIS, onder een zelfstandig agentschap wordt gebracht, zoals is voorgesteld door het Europese Parlement en de Commissie, is het tevens van belang dat een dergelijk agentschap niet de bevoegdheid krijgt om zelfstandig toestemming te verlenen voor doorgifte van de SIS-gegevens aan derdestaten of instanties. Gegevensverstrekking aan derden mag uitsluitend geschieden op basis van duidelijke, wettelijk geregelde criteria aan bepaalde vooraf vastgestelde instanties. De besluitvorming hierover moet in een democratisch kader en in overleg met toezichtorganen voor de gegevensbescherming plaatsvinden. Dit voorkomt dat het gebruik van het SIS of het VIS volkomen ondoorzichtig wordt door discretionaire bevoegdheden te verlenen aan hetzij een agentschap, hetzij de nationale overheden.

Het uitgangspunt van Europese samenwerking op het gebied van gegevensuitwisseling is steeds geweest dat de andere Europese staten waaraan de gegevens worden uitgewisseld, een gelijk of in ieder geval een, van tevoren afgesproken, minimumniveau van gegevensbescherming bieden. Met betrekking tot de gegevensverstrekking aan derde-, niet Europese staten, vereist de Europese richtlijn inzake gegevensbescherming dat deze staten over een adequaat gegevensbeschermingsniveau beschikken. Ook aan toekomstige gegevensverstrekking aan derdestaten moeten strenge eisen worden gesteld, zoals: gegevensuitwisseling mag enkel plaatsvinden op basis van een concreet verzoek met toetsing door een toezichthoudend orgaan; de ontvangende staat moet de garantie bieden dat de gegevens voor een beperkt en concreet doel worden gebruikt; en het individu dient te worden geïnformeerd over de gegevensverstrekking aan derdestaten of instanties. En meer dan nu, moeten dergelijke afspraken over gegevensverstrekking aan derdestaten uitsluitend op basis van wederkerigheid worden gemaakt.

4.4 Bewaartermijnen

Voor het huidige SIS geldt dat gegevens over personen drie jaar mogen worden bewaard, met uitzondering van personen die voor onopvallende of gerichte controle zijn opgenomen: daarvoor geldt een termijn van één jaar. Echter wanneer de nationale overheid langere bewaring noodzakelijk acht, kan zij de termijn steeds verlengen. Opvallend is dat in een bijeenkomst van 20 juni 2002, de Raad nog oordeelde dat verlenging van bewaartermijnen niet nodig zou zijn omdat de huidige SIS-regeling aan de bestaande behoeften voldoet.[33] Een jaar later echter stelt de Raad, in een andere samenstelling, vast dat bij de beslissingen over nieuwe functies van het SIS, óók een

32 Zie onder meer de volgende Raadsdocumenten: 6164/1/01, 14790/01 en 5968/02. Zie ook de conclusies in Raadsdocument 9808/03 die tijdens de Raad van Ministers van Justitie en Binnenlandse Zaken van 5-6 juni 2003 zijn goedgekeurd.

33 Zie de notulen van de Ecofin Raad, Raadsdocument 10089/02 (Press 181) en ook een eerdere nota van het EU-voorzitterschap, Raadsdocument 13269/01, 31 oktober 2001.

nr. 1 - februari 2004

besluit moet worden genomen over wijziging van de bewaartermijnen.[34] Concrete voorstellen zijn, voorzover bekend, nog niet gepubliceerd. Ten aanzien van het VIS wordt, in de hierboven genoemde ontwerpconclusies van de Raad, als bewaartermijn vijf jaar voorgesteld.[35] Na deze termijn worden de gegevens naar een centraal archief overgebracht, dat 'off-line' nog eens voor vijf jaar raadpleegbaar zal zijn. Bovendien kunnen nationale overheden, aldus dit voorstel, besluiten om de gegevens naar nationale archieven over te brengen.

Om het gebruik van verouderde, onbruikbare gegevens te voorkomen, zal per categorie gegevens en per doel waarvoor die gegevens worden opgeslagen, een passende bewaringstermijn moeten worden vastgesteld. De vaststelling van deze bewaartermijnen moet in overleg met de onafhankelijke toezichtorganen geschieden.

Verlenging van deze termijn mag niet automatisch gebeuren, maar dient per concreet geval te worden gemotiveerd. Naleving van de bewaartermijnen dient periodiek getoetst te worden door het onafhankelijk toezichtorgaan, op Europees of op nationaal niveau.

4.5 Individuele rechten

De burger heeft het recht op informatie over het gebruik van zijn of haar persoonlijke gegevens. Dit vergroot niet alleen het draagvlak voor de voorgestelde systemen bij de burgers, maar ook de efficiency en juistheid van de gebruikte systemen. Door de uitoefening van dit recht kunnen immers ook foute en onterecht opgenomen gegevens worden opgespoord en gecorrigeerd. In de huidige regeling van het SIS, maar ook Eurodac en Europol zijn dergelijke rechten opgenomen. Ongetwijfeld zal de EU-wetgever ook in de toekomstige instrumenten bepalingen over individuele rechten opnemen.

Het zou echter aanbeveling verdienen wanneer de toekomstige regelingen er in voorzien dat autoriteiten, anders dan op grond van de huidige regelingen, de burger zoveel mogelijk vooraf informeren over het gebruik van zijn of haar persoonsgegevens. De verstrekte informatie moet duidelijkheid bieden over het voorgenomen doel van de gegevensopslag, wie de gebruikers zijn van die informatie, wat de bewaartermijnen zijn en ten slotte welke rechten en rechtsmiddelen de betreffende persoon heeft. Deze informatie moet bij voorkeur worden verstrekt op het moment van afname van de betreffende gegevens of op het moment wanneer deze gegevens in een informatiesysteem worden opgenomen. Bij de afname van biometrische gegevens zal de betreffende persoon in ieder geval op het moment van afname over het doel en het gebruik moeten worden geïnformeerd.

Wanneer bij een grensovergang of anderszins, gezichts- of irisherkenning wordt gebruikt als biometrisch identificatiemiddel, dan moeten de autoriteiten de aldus gecontroleerde personen steeds inlichten over het moment en de wijze waarop zij worden gecontroleerd.

4.6 Effectieve rechtsmiddelen

Aan de in de Europese informatiesystemen opgenomen persoon moeten effectieve rechtsmiddelen openstaan. Dit kan hetzij door eenvoudige toegang te bieden tot een nationaal of Europees toezichtorgaan, onder voorwaarde dat dit orgaan over bindende bevoegdheden beschikt, hetzij door toegang te bieden tot een nationale rechter. Bij toegang tot een nationale rechter verdient het de voorkeur het systeem van het huidige SIS te kiezen, waarbij een individu zelf kan kiezen op welk grondgebied het een procedure wil starten. Het rechtsmiddel moet openstaan ten aanzien van zowel het besluit om iemand in een informatiesysteem op te nemen, als ten aanzien van het besluit dat op basis van een in een systeem opgenomen informatie is genomen. Een besluit met rechtsgevolgen voor de betrokkene moet dus mede op de juistheid van die gegevens kunnen worden getoetst.

Op grond van de huidige regeling van het SIS, de Schengen Uitvoeringsovereenkomst, moet iedere uitspraak van een nationale rechter of toezichtinstantie in verband met de rechtmatigheid van gegevensverwerking worden nageleefd door de nationale autoriteiten van alle andere lidstaten. Het verdient aanbeveling om voor een vergelijkbare regeling te kiezen bij SIS II en het VIS.

4.7 Internationaal toezichtorgaan

Op dit moment bestaan er op Europees niveau verschillende toezichtmechanismen. In de eerste plaats wordt toezicht op nationaal niveau uitgevoerd: bijvoorbeeld bij het SIS houden nationale dataprotectieautoriteiten toezicht op gebruik van de nationale SIS-systemen. De wijze waarop dit toezicht wordt uitgeoefend kan verschillen, omdat dit nationaal verschillend is geregeld. Daarnaast hebben SIS, Europol en Eurodac ieder hun eigen gemeenschappelijke toezichthoudende autoriteit. Wel is voor deze autoriteiten met een besluit van oktober 2000 een gemeenschappelijk secretariaat gecreëerd.[36] Op korte termijn zal een Europees toezichthoudend orgaan worden aangesteld. Dit orgaan is echter alleen belast met het toezicht op de uitvoering van het Europese recht inzake gegevensbescherming door de Europese instanties en lichamen zelf. Hoewel het bestaan van deze Europese autoriteiten is toe te juichen, biedt het geheel van deze verschillende toezichtmechanismen, een versnipperd en ondoorzichtig beeld.

Het lijkt raadzaam om op Europees niveau één orgaan in te stellen dat toezicht houdt op de persoonsinformatiesystemen die op basis van Europees recht zijn ingesteld en die door de nationale autoriteiten van de EU-lidstaten worden gebruikt. Eventueel kan dit Europees toezichtorgaan worden toegerust met gespecialiseerde 'kamers' of afdelingen voor de afzonderlijke Europese informatiesystemen. Het toezichtorgaan dient in ieder geval voldoende financiële middelen te krijgen om haar taken naar behoren uit te voeren. Ook moet ze worden toegerust

34 *Zie eerdergenoemd Raadsdocument 9808/03.*

35 *Raadsdocument 14776/03, 13 november 2003. Zie ook Raadsdocument 9615/02 van 5 juni 2002.*

36 *Raadsbesluit van 17 oktober 2000, OJ 2000, L 271.*

met bindende instrumenten, zoals bijvoorbeeld de mogelijkheid een instantie te verplichten tot verwijdering of correctie van gegevens; de bevoegdheid boetes op te leggen; en te bevelen dat gegevensverwerking bij ernstige schending van de regelgeving wordt stopgezet.

4.8 Opname evaluatieplicht

Ten slotte dient de wetgever in de wettelijke regeling van ieder toekomstig informatiesysteem een evaluatieplicht op te nemen. Deze evaluatie moet de effecten wat betreft gebruik, behaalde doelen, rechtsbescherming en kosten bestrijken. De evaluatie dient te worden uitgevoerd binnen een bepaalde termijn (bijvoorbeeld twee jaar) na het operationeel worden van het informatiesysteem.

5 Conclusie

De noodzaak van de opheffing van de interne grenscontroles werd in 1985 door de Europese Commissie in haar Witboek over de interne markt nog gemotiveerd met de overweging: 'Grenscontrole komt op de burger over als de veruitwendiging (sic) van een willekeurige administratieve macht die boven de individuen staat'.[37] Inmiddels, anno 2003, is de vraag gerechtvaardigd of de maatregelen die op het gebied van het gebruik van persoonsinformatie ten behoeve van de grenscontrole worden voorgesteld, niet veel meer als een willekeurige administratieve macht zullen worden ervaren.

Bij de komende besluitvorming zullen de lidstaten met name de beginselen van proportionaliteit en subsidiariteit in het oog moeten houden. Inachtneming van de hierboven genoemde minimumvoorwaarden draagt niet alleen bij aan het vertrouwen van de burger in de (Europese) overheid, maar ook aan een effectieve en transparante uitvoering van de door die overheid gestelde taken.

37 *COM 1985 (310), juni 1985, r.o. 48, p. 14.*