GROEP GEGEVENSBESCHERMING ARTIKEL 29

12168/02/NL
WP 80

Werkdocument over biometrie

Goedgekeurd op 1 augustus 2003

De Groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Zij is het onafhankelijke EU-adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer. De taken van de Groep zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 14 van Richtlijn 97/66/EG. Het secretariaat wordt verzorgd door:

Directoraat E (Diensten, intellectuele en industriële eigendom, media en gegevensbescherming) van directoraat-generaal Interne markt van de Europese Commissie, B-1049 Brussel, België, kamer C 100-6/136.

Website: www.europa.eu.int/comm/privacy

DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS

Opgericht bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995[1],

Gelet op artikel 29 en artikel 30, lid 1, onder a), en lid 3, van deze richtlijn,

Gelet op haar reglement, en met name op de artikelen 12 en 14,

heeft het volgende werkdocument goedgekeurd

1. INLEIDING

De snelle ontwikkeling van de biometrietechnologie en de toenemende toepassingen ervan in de laatste jaren maken het vanuit het oogpunt van de gegevensbescherming noodzakelijk deze technologie nader te bestuderen[2]. Een ruim en ongecontroleerd gebruik van biometrie doet vragen rijzen in verband met de bescherming van fundamentele rechten en vrijheden van personen. Dit soort gegevens is heel specifiek omdat ze te maken hebben met de gedragskenmerken en fysiologische kenmerken van een persoon en de unieke identificatie van deze persoon mogelijk maken[3].

Biometrische gegevens worden thans vaak gebruikt bij geautomatiseerde authenticatie/verificatie- en identificatieprocedures, met name voor de controle van de toegang tot zowel fysieke als virtuele omgevingen (toegang tot elektronische systemen of diensten).

Vroeger bleef het gebruik van biometrie hoofdzakelijk beperkt tot DNA en vingerafdrukken. Het verzamelen van vingerafdrukken was vooral bedoeld voor rechtshandhaving (bv. het opsporen van misdadigers). Een samenleving die de ontwikkeling van gegevensbanken met vingerafdrukken of andere biometrische gegevens voor nog meer routinematige toepassingen stimuleert, kan hiermee het gevaar vergroten dat de gegevens door derde partijen worden hergebruikt als element van vergelijking en onderzoek voor eigen doeleinden, zonder dat een dergelijke doelstelling oorspronkelijk werd nagestreefd; die derde partijen kunnen ook rechtshandhavingsautoriteiten zijn.

Een typisch probleem met biometrische gegevens is dat door het toenemend gebruik van deze gegevens het publiek onverschillig kan worden voor het effect van de verwerking

---

[1] PB L 281 van 23.11.1995, blz. 31, beschikbaar op: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.

[2] Sinds 11 september 2001 wordt biometrie vaak voorgesteld als een goed middel om de veiligheid te verbeteren. In de Europese Unie wordt momenteel gepraat over het opnemen van biometrische gegevens op identiteitskaarten, paspoorten, reisdocumenten en visa. De VS zullen binnenkort biometrische identificatiegegevens eisen voor buitenlanders die het land willen binnenkomen en verlaten. In 2003 werd de ILO-conventie nr. 108 gewijzigd om de verplichte biometrie voor zeevarenden te kunnen invoeren. Er zijn ook discussies aan de gang in andere internationale fora zoals de G8, de OESO, enz..

[3] De unieke identificatie hangt echter af van verschillende factoren zoals de omvang van de gegevensbank en het soort biometrische gegevens dat wordt gebruikt.

ervan op het dagelijkse leven. Bijvoorbeeld, het gebruik van biometrie in schoolbibliotheken kan ertoe leiden dat kinderen zich minder bewust worden van de risico's voor de gegevensbescherming waarmee zij in hun latere leven kunnen worden geconfronteerd.

Met dit document wil de Groep ertoe bijdragen dat de nationale bepalingen betreffende gegevensbescherming, die in overeenstemming met Richtlijn 95/46/EG zijn goedgekeurd, op een efficiënte en uniforme manier op biometrische systemen worden toegepast. Behandeld worden hoofdzakelijk biometrische toepassingen voor authenticatie- en verificatiedoeleinden. De Groep zou graag zien dat er uniforme Europese richtsnoeren komen, met name voor de bedrijven die biometrische systemen vervaardigen en voor de gebruikers van dergelijke technologieën.

2. BESCHRIJVING VAN BIOMETRISCHE SYSTEMEN

Biometrische systemen zijn toepassingen van biometrische technologieën voor de automatische identificatie, en/of authenticatie/verificatie van een persoon[4]. Authenticatie/verificatie toepassingen worden vaak voor verschillende taken op totaal uiteenlopende gebieden en onder de verantwoordelijkheid van talrijke verschillende organisaties gebruikt.

Elk biometrisch gegeven, of het nu gebruikt wordt voor authenticatie/verificatie of identificatie, heeft, in meerdere of mindere mate de volgende eigenschappen:
- **universeel :** alle mensen hebben het[5];
- **uniek** : er bestaan geen twee personen met precies hetzelfde kenmerk;
- en **permanent**: het kenmerk mag niet veranderen of te veranderen zijn.

Biometrische technieken kunnen worden ingedeeld in twee hoofdcategorieën, afhankelijk van het feit of stabiele gegevens of dynamische gedragsgegevens worden gebruikt[6].

Er zijn de op fysieke en **fysiologische** kenmerken gebaseerde technieken zoals vingerafdrukcontrole, vingerbeeldanalyse, irisherkenning, netvliesanalyse, gezichtsherkenning, handpalmpatroonschets, oorvormherkenning, lichaamsgeurdetectie, stemherkenning, DNA-patroonanalyse[7] en zweetporiënanalyse, enz.

---

[4] Het verschil tussen authenticatie (verificatie) en identificatie is belangrijk. Authenticatie geeft een antwoord op de vraag Ben ik degene die ik beweer te zijn? Het systeem verifieert de identiteit van de persoon door de verwerking van biometrische gegevens die betrekking hebben op de vraagsteller en neemt een ja/nee besluit (1:1 vergelijking). Identificatie geeft een antwoord op de vraag Wie ben ik? Het systeem erkent de vraagsteller door hem te onderscheiden van andere personen van wie de biometrische gegevens eveneens zijn opgeslagen. In dit geval neemt het systeem een 1-n besluit en antwoordt dat de vraagsteller X is.

[5] Wat dit betreft zijn niet alle biometrische gegevens gelijkwaardig en als middel om onderscheid te maken tussen personen van zeer uiteenlopend nut, afhankelijk van de gebruikte biometrische kenmerken. De meest onderscheidende biometische elementen lijken, DNA, netvlies en vingerafdruk te zijn.

[6] Sommige technieken kunnen zowel fysiologisch zijn als het gedrag betreffen.

[7] Over het gebruik van DNA voor biometrische identificatie is heel wat te zeggen; deze onderwerpen komen in dit stuk echter niet aan bod. Het onmiddellijk opstellen van een DNA-profiel bij een controle lijkt momenteel als authenticatiemiddel niet mogelijk.

En er zijn de op **gedragskenmerken** gebaseerde technieken zoals controle van handtekeningen, toetsaanslaganalyse, loopanalyse, enz.

Door de snelle technische ontwikkeling en de toenemende bezorgdheid om veiligheid werken talrijke biometrische systemen met een combinatie van verschillende biometrische kenmerken van de gebruiker en andere identificatie- of authenticatietechnologieën. Sommige systemen bv. hebben gezichts- en stemherkenning. Voor authenticatie kunnen drie verschillende methoden gezamenlijk worden gebruikt, gebaseerd op iets wat een persoon weet (wachtwoord, PIN, enz.), iets wat een persoon heeft (token, CAD-sleutel, smartcard, enz.) en iets wat een persoon kenmerkt (een biometrisch kenmerk). Met een computer kan men bv. een smartcard inbrengen, een wachtwoord invoeren en vingerafdrukken tonen.

De biometrische gegevens (bv. vingerafdrukbeeld, foto van de iris of het netvlies, opname van de stem) worden verzameld tijdens de zogenaamde “registratie”-fase met gebruik van een voor elk type biometrisch gegeven specifieke sensor. Uit de biometrische gegevens haalt het biometrische systemen gebruikersspecifieke kenmerken om een biometrische "template" te maken. De template is een gestructureerde reductie van een biometrisch beeld: de geregistreerde biometrische meting van een persoon. Opgeslagen wordt de template, in gedigitaliseerde vorm, en niet het biometrische element zelf. Daarnaast kunnen biometrische gegevens als ruwe gegevens (een beeld) worden verwerkt, afhankelijk van de werking van het gebruikte biometrische systeem[8].

De registratiefase speelt een belangrijke rol aangezien het de enige fase is waarin ruwe gegevens, extractie en beschermingsalgoritmen (cryptografie, hashing, enz.) en templates gelijktijdig aanwezig zijn. In dit verband zij erop gewezen dat indien de ruwe gegevens informatie geven die als gevoelig kan worden beschouwd in de zin van artikel 8 van Richtlijn 96/46/EG, de registratie van dergelijke gegevens volgens deze bepaling moet gebeuren (zie punt 3.7).

Een ander belangrijk punt uit het oogpunt van de gegevensbescherming is de vorm waarin de templates van de gebruikers worden opgeslagen. Dit wordt bepaald door de toepassing waarvoor het biometrisch systeem wordt gebruikt en de grootte van de templates zelf. De templates kunnen op de volgende manieren worden opgeslagen:

a) in het geheugen van een biometrisch systeem;
b) in een centrale gegevensbank;
c) op plastic kaarten, optische kaarten of smartcards. Op die manier kunnen gebruikers hun templates steeds bij zich hebben en als identificatiemiddel gebruiken.

In principe is het niet nodig om voor authenticatie/verificatie de referentiegegevens in een gegevensbank op te slaan; het is voldoende de persoonsgegevens op een gedecentraliseerde manier op te slaan. Identificatie is echter pas mogelijk als de referentiegegevens in een gedecentraliseerde gegevensbank worden opgeslagen, omdat het systeem, om de identiteit van de betrokkene na te gaan, zijn of haar templates of ruwe gegevens (beeld) met de templates of ruwe gegevens van alle personen die reeds centraal zijn opgeslagen, moet vergelijken.

---

[8] In dit document worden biometrische systemen behandeld die gebaseerd zijn op templates, maar het stuk kan ook op ruwe gegevens worden toegepast. Voor ruwe gegevens zouden echter andere gegevensbeschermingseisen nodig kunnen zijn.

Een ander cruciaal punt uit het oogpunt van de gegevensbescherming is het feit dat sommige biometrische systemen gebaseerd zijn op informatie, zoals vingerafdrukken of DNA-proeven, die misschien verzameld is zonder dat de betrokkene zich hiervan bewust is omdat hij sporen kan nalaten zonder het te beseffen. Door een biometrische algoritme op vingerafdrukken op een glas toe te passen kan men nagaan[9] of de desbetreffende persoon in een gegevensbank met biometrische gegevens voorkomt, en als dat zo is, wie de persoon is, door de twee templates te vergelijken. Dit geldt ook voor andere biometrische systemen, zoals die op basis van toetsaanslaganalyse of gezichtsherkenning op afstand, afhankelijk van de specifieke aspecten van de desbetreffende technologie[10]. Problematisch is dat enerzijds het verzamelen en verwerken van gegevens misschien gebeurt zonder dat de betrokkene zich hiervan bewust is en dat anderzijds deze biometrische technologieën, ongeacht de huidige betrouwbaarheid ervan, geschikt zijn om er onbeperkt gebruik van te maken omdat zij niet diep binnendringen in de persoonlijke levenssfeer van de betrokkenen. Het lijkt dan ook aangewezen om voor deze technologieën speciale waarborgen in het leven te roepen.

3. TOEPASSING VAN DE BEGINSELEN VAN RICHTLIJN 95/46/EG

3.1. Toepassing van Richtlijn 95/46/EG

In artikel 2 a) van Richtlijn 95/46/EG worden “persoonsgegevens” gedefinieerd als “iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (…); als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische (...) identiteit”. In overweging 26 staat voorts dat “om te bepalen of een persoon identificeerbaar is, moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is *dan wel door enig ander persoon* aan te wenden zijn om genoemde persoon te identificeren”.

Volgens deze definitie zijn biometrische identificatiemaatregelen of de digitale weergave ervan in templatevorm in de meeste gevallen persoonsgegevens[11]. Biometrische gegevens kunnen eigenlijk altijd worden beschouwd als "informatie betreffende een natuurlijke persoon" aangezien het om gegevens gaat die door hun aard informatie verstrekken over een bepaalde persoon. In het kader van biometrische identificatie is de persoon meestal identificeerbaar aangezien de biometrische gegevens op een zodanige manier voor identificatie of authenticatie/verificatie worden gebruikt dat de betrokkene van een ander persoon wordt onderscheiden[12].

---

9 Om dit te kunnen doen moet men echter in staat zijn om vingerafdrukken van het glas te nemen zonder het te beschadigen, in het bezit zijn van de apparatuur om de gegevens van de vingerafdrukken te verwerken, toegang hebben tot het algoritme van de maker van de gegevensbank en/of tot de gegevensbank van de vingerafdrukken.

10 Zie punt 3 over de toepassing van Richtlijn 95/46/EG en met name 3.3 over de verplichte informatieverstrekking aan de betrokkene.

11 In de gevallen waarin biometrische gegevens, zoals een template, zijn opgeslagen op een zodanige manier dat door de voor de verwerking verantwoordelijk of enig ander persoon geen enkel redelijk middel kan worden gebruikt om de betrokkene te identificeren, kunnen deze gegevens niet worden aangemerkt als persoonsgegevens.

12 De identificeerbaarheid van de persoon hangt ook af van de beschikbaarheid van andere gegevens die het - samen of apart - mogelijk maken de desbetreffende persoon te identificeren. De mogelijkheid van “directe identificatie”

Volgens artikel 3, lid 1, van Richtlijn 95/46/EG zijn de gegevensbeschermingsbeginselen van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. De richtlijn is niet van toepassing indien de gegevens worden verwerkt door een natuurlijke persoon tijdens een persoonlijke of huishoudelijke activiteit. Talrijke biometrische toepassingen voor huishoudelijk gebruik behoren tot deze categorie.

Naast deze specifieke uitzonderingen kan verwerking van biometrische gegevens alleen als rechtmatig worden beschouwd indien alle procedures, te beginnen bij de registratie, worden uitgevoerd overeenkomstig de bepalingen van Richtlijn 95/46/EG.

In dit document worden niet alle vraagstukken behandeld die verband houden met de toepassing van Richtlijn 95/46/EG op biometrische gegevens. Alleen de meest belangrijke komen aan bod en daarom geeft dit document geen volledig overzicht van de gevolgen van de toepassing van de richtlijn.

3.2. Beginsel van doelbinding en evenredigheid

Volgens artikel 6 van Richtlijn 95/46/EG moeten persoonsgegevens verzameld worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen zij niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden. Voorts moeten persoonsgegevens toereikend, ter zake dienend en niet bovenmatig zijn, uitgaande van de doeleinden waarvoor zij worden verzameld en/of verder verwerkt (beginsel van doelbinding).

Voor de naleving van dit beginsel moet in eerste plaats het doel worden vastgesteld waarvoor de biometrische gegevens worden verzameld en verwerkt. Voorts moet worden nagegaan of de beginselen van evenredigheid en rechtmatigheid zijn nageleefd, waarbij rekening moet worden gehouden met de risico's voor de bescherming van de fundamentele rechten en vrijheden van personen en waarbij moet worden nagegaan of het beoogde doel kan worden bereikt op een manier die de persoonlijke levenssfeer minder aantast. Evenredigheid is het belangrijkste criterium geweest in vrijwel alle beslissingen die de gegevensbeschermingsautoriteiten tot dusverre m.b.t. de verwerking van biometrische gegevens hebben genomen[13].

Wat toegangscontrole betreft (authenticatie/verificatie), is de Groep van mening dat biometrische systemen gebaseerd op fysieke kenmerken die geen sporen achterlaten (bv. vorm van de hand maar niet de vingerafdrukken) of biometrische systemen die gebaseerd zijn op fysieke kenmerken die weliswaar sporen achterlaten maar die niet op een drager zijn opgeslagen die in het bezit is van een andere persoon dan de betrokkene (met andere woorden, de gegevens zijn niet opgeslagen in de toegangscontrolevoorziening of in een centrale gegevensbank) minder risico's opleveren voor de bescherming van de fundamentele rechten en vrijheden van personen[14]. Verschillende

---

met “een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke identiteit” wordt uitdrukkelijk vermeld in de definitie van persoonsgegevens in artikel 2 a) van Richtlijn 95/46/EG.

[13] Bv. beslissingen van de Nederlandse, Franse, Duitse, Italiaanse en Griekse autoriteiten.

[14] Onderscheid kan gemaakt worden tussen biometrische gegevens die centraal worden verwerkt en het geval waarin als referentie gebruikte biometrische gegevens op een mobiele voorziening zijn opgeslagen en de vergelijking op de kaart gebeurt maar niet op de sensor, zelfs wanneer de sensor eveneens een onderdeel is van de mobiele voorziening.

gegevensbeschermingsautoriteiten zijn deze mening toegedaan; zij geven er de voorkeur aan dat biometrische gegevens niet in een gegevensbank worden opgeslagen maar alleen op een drager die uitsluitend ter beschikking staat van de gebruiker, zoals een chipkaart, een mobiele telefoon, een bankkaart, enz[15]. M.a.w., authenticatie/verificatie-toepassingen die kunnen worden uitgevoerd zonder centrale opslag van biometrische gegevens zouden geen aanleiding geven tot excessieve identificatietechnieken.

Daarom is de Groep van oordeel dat het gebruik van andere soorten toepassingen (bv. gebaseerd op digitale vingerafdruktemplates in de terminal of een centrale database) zorgvuldig moet worden beoordeeld voordat dergelijke toepassingen worden ingevoerd. Indien een dergelijk systeem wordt uitgevoerd, bv. in gevallen waarin hoge veiligheidseisen aan installaties[16] worden gesteld, kan ervan worden uitgegaan dat de gegevensverwerking risico's inhoudt in de zin van artikel 20 van Richtlijn 95/46/EG en eerst aan de gegevensbeschermingsautoriteit moet worden voorgelegd in overeenstemming met nationale wetgeving (zie punt 3.5).

Richtlijn 95/46/EG verbiedt verwerking van gegevens op een wijze die onverenigbaar is met het doel waarvoor de gegevens zijn verzameld. Bv. in het geval waarin biometrische gegevens worden verwerkt voor toegangscontrole, zou het gebruik van die gegevens om de gemoedstoestand van de betrokkene na te gaan of om toezicht te houden op de werkplek, niet verenigbaar zijn met het oorspronkelijke doel van de verzameling. Alle maatregelen moeten worden genomen om dergelijk oneigenlijk hergebruik te voorkomen[17]. Richtlijn 95/46/EG voorziet in uitzonderingen op het verwerkingsverbod voor onverenigbare doeleinden, maar er zijn speciale voorwaarden van toepassing.

In het algemeen gaat men ervan uit dat het risico dat biometrische gegevens die verkregen zijn op basis van fysieke sporen die onbewust door personen zijn achtergelaten (bv. vingerafdrukken) voor onverenigbare doelen worden hergebruikt, vrij laag is indien de gegevens niet in gecentraliseerde gegevensbanken worden opgeslagen, maar bij de desbetreffende persoon blijven en niet toegankelijk zijn voor een derde partij. Het gecentraliseerd opslaan van biometrische gegevens doet ook het gevaar toenemen dat biometrische gegevens worden gebruikt om verschillende gegevensbanken met elkaar te verbinden, hetgeen tot een gedetailleerd inzicht kan leiden in de gewoonten van personen, zowel in de publieke als in de particuliere sector. Vanwege het doelbindingsbeginsel kunnen ook vraagtekens worden gezet bij de interoperabiliteit van verschillende systemen die gebruikmaken van biometrie. De noodzakelijke standaardisatie voor interoperabiliteit kan tot een ruimere onderlinge verbinding van gegevensbanken leiden.

Het gebruik van biometrie roept ook vragen op in verband met de evenredigheid van elke categorie verwerkte gegevens ten aanzien van het doel waarvoor de gegevens worden verwerkt. Biometrische gegevens mogen volgens de richtlijn alleen worden gebruikt als

---

15 Rekening moet worden gehouden met mechanismen die de problemen moeten oplossen in verband met gestolen, kwijtgeraakte of beschadigde kaarten en die mechanismen die niet tot de opslag van biometrische gegevens leiden, moeten worden bevorderd. In de mate van het mogelijke moeten de gegevens direct bij de betrokkene worden verzameld.

16 Gezien de huidige stand van de biometrietechnologie zijn betrouwbare, real-time identificatieoplossingen voor een populatie van om het even welke reële grootte niet voorhanden, en zullen die in de nabije toekomst waarschijnlijk ook nog niet ter beschikking zijn.

17 Zoals hierboven is aangegeven moet het doel duidelijk worden omschreven.

ze toereikend, ter zake dienend en niet bovenmatig zijn. Dit betekent dat de noodzaak van de verwerking en de evenredigheid ervan strikt in de gaten moeten worden gehouden[18]. Het Franse CNIL heeft bijvoorbeeld het gebruik van vingerafdrukken geweigerd om de toegang van kinderen tot een schoolrestaurant te controleren[19], maar heeft voor hetzelfde doel wel handpalmanalyse aanvaard. De Portugese gegevensbeschermingsautoriteit heeft zich onlangs negatief uitgesproken over het gebruik van een biometrische systeem (vingerafdruk) door een universiteit om de aanwezigheid van niet onderwijzend personeel te controleren[20]. De Duitse gegevensbeschermingsautoriteit heeft ingestemd met het gebruik van biometrische kenmerken voor identiteitspapieren om vervalsing ervan tegen te gaan, op voorwaarde dat de gegevens op de microchip van de kaart worden opgeslagen en niet in een gegevensbank waarin zijn met de vingerafdrukken van de eigenaar zouden worden vergeleken.

Een specifiek probleem kan zich voordoen omdat biometrische gegevens vaak meer informatie bevatten dan wat voor identificatie of authenticatie/verificatie nodig is. Dit komt waarschijnlijk vaker voor bij het originele beeld (ruwe gegevens) aangezien de template mag en, technisch gezien, alleen maar op een zodanige manier kan worden opgesteld dat verwerking van gegevens die niet noodzakelijk zijn, uitgesloten is. Niet noodzakelijke gegevens moeten zo spoedig mogelijk worden vernietigd[21]. Bovendien kunnen sommige biometrische gegevens informatie bevatten over raciale of etnische afkomst of over gezondheid. (zie punt 3.7.).

Tot slot moet worden vermeld dat het gebruik van biometrische systemen misschien op zodanige manier kan gebeuren dat zij kunnen beschouwd worden als een technologie die de privacybescherming bevordert, omdat zij de verwerking van andere persoonsgegevens zoals naam, adres, woonplaats, enz. kunnen beperken.

3.3. Eerlijke verwerking en informatieverstrekking

Biometrische gegevens moeten op een eerlijke manier worden verzameld en verwerkt[22]. De voor de verwerking verantwoordelijke moet de betrokkene informatie verstrekken overeenkomstig artikel 10 en 11 van Richtlijn 95/46/EG[23]. Met name moet onder meer

---

18 In sommige gevallen moet het gebruik van anonimiteit of pseudoniemen mogen blijven. Rekening moet worden gehouden met mechanismen die de problemen moeten oplossen in verband met gestolen, kwijtgeraakte of beschadigde kaarten en die mechanismen die niet tot de opslag van biometrische gegevens leiden, moeten worden bevorderd. In de mate van het mogelijke moeten de gegevens direct bij de betrokkene worden verzameld.

19 De gegevensbeschermingsautoriteit in het VK heeft naar het schijnt wel het gebruik van vingerafdrukken onder soortgelijke omstandigheden aanvaard, maar alleen als er passende garanties voorhanden zijn.

20 De Portugese gegevensbeschermingsautoriteit was van mening dat het gebruik van dergelijke systemen niet in verhouding stond tot het doel van de gegevensverwerking. Het systeem zou deze gegevens in een biometrische voorziening opslaan en ruim 140 personen zouden worden gecontroleerd.

21 In dit verband zij ook gewezen op het belang van artikel 6, lid 1, onder e) van Richtlijn 95/46/EG waarin staat dat persoonsgegevens *niet langer* mogen worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt, noodzakelijk is.

22 Artikel 6, a), van Richtlijn 95/46/EG.

23 De uitzonderingen op de informatieplicht waarin de artikelen 10 en 11 van Richtlijn 95/46/EG voorzien, moeten gebaseerd zijn op een wettelijke maatregel en de verplichte informatieverstrekking mag alleen worden beperkt indien dit noodzakelijk is om de belangen die zijn opgenomen in artikel 13 van Richtlijn 95/46/EG (de veiligheid van de Staat of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, enz.) te vrijwaren.

het doel van de verwerking precies worden omschreven en moet de identiteit van de voor de verwerking verantwoordelijke worden bekendgemaakt (vaak is dit degene die het biometrisch systeem beheert of de biometrische techniek toepast).

Systemen die biometrische gegevens verzamelen zonder dat de betrokkene hiervan kennis heeft, mogen niet worden gebruikt. Sommige biometrische systemen zoals gezichtsherkenning op afstand, verzamelen van vingerafdrukken, het aftappen van gesprekken, houden wat dit betreft meer risico's in.

3.4. Criteria voor de rechtmatigheid van de gegevensverwerking.

Verwerking van biometrische gegevens moet beantwoorden aan de criteria van rechtmatigheid waarin artikel 7 van Richtlijn 95/46/EG voorziet (in de richtlijn "toelaatbaarheid"). Indien instemming van de betrokkene door de voor de verwerking verantwoordelijke gebruikt wordt als rechtvaardiging voor de verwerking, moet volgens de Groep worden voldaan aan de voorwaarden van artikel 2 van Richtlijn 95/46/EG (elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt).

3.5. Voorafgaand onderzoek - aanmelding

De Groep heeft reeds eerder aangegeven dat zij instemt met het gebruik van biometrische systemen die geen sporen achterlaten in toegangscontroleapparatuur noch informatie opslaan in een centrale gegevensbank (zie punt 3. 2.). Maar indien dergelijke systemen toch moeten worden gebruikt en gezien het gevaar voor hergebruik voor andere doeleinden alsmede de specifieke risico’s in geval van ongeautoriseerde toegang, acht de Groep het nuttig dat lidstaten de verwerking eerst voorleggen aan de gegevensbeschermingsautoriteiten, overeenkomstig artikel 20 van Richtlijn 95/46/EG, aangezien dit soort verwerkingen specifieke risico's inhoudt voor de rechten en vrijheden van de betrokkenen. Indien lidstaten een beroep willen doen op voorafgaand onderzoek m.b.t. de verwerking van biometrische gegevens, moeten nationale gegevensbeschermingsautoriteiten worden geraadpleegd voordat dergelijke maatregelen worden ingevoerd.

3.6. Beveiligingsmaatregelen

De voor de verwerking verantwoordelijke moet, in overeenstemming met artikel 17 van Richtlijn 95/46/EG, alle passende technische en organisatorische maatregelen neemt om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet toegestane verspreiding of toegang, met name wanneer de verwerking doorzending van biometrische gegevens in een netwerk omvat. Beveiligingsmaatregelen moeten worden genomen als biometrische gegevens worden verwerkt (opslag, doorsturen, extractie van kenmerken en vergelijkingen, enz.) en met name wanneer de voor de verwerking verantwoordelijke dergelijke gegevens via internet doorstuurt. Voor de beveiliging kan men bijvoorbeeld gebruikmaken van encryptie van de templates en de bescherming van de encryptiesleutels, naast toegangscontrole en -bescherming, zodat het virtueel onmogelijk wordt om de originele gegevens aan de hand van de templates te reconstrueren.

In dit verband moet rekening worden gehouden met nieuwe technologieën. Een interessante ontwikkeling is de mogelijkheid om biometrische gegevens als encryptiesleutels te gebruiken. Dit zou minder risico's voor de betrokkene opleveren aangezien het decoderen alleen mogelijk is aan de hand van een nieuwe verzameling van

biometrische gegevens van de betrokkene zelf; op die manier zijn er geen gegevensbanken met templates van biometrische gegevens nodig die voor andere doeleinden zouden kunnen worden gebruikt.

De noodzakelijke beveiligingsmaatregelen zouden dan vanaf het begin van de verwerking kunnen worden toegepast, en met name tijdens de registratiefase, wanneer de biometrische gegevens worden omgevormd tot templates of beelden. Elke aantasting van de volledigheid, vertrouwelijkheid en beschikbaarheid van de informatie in de gegevensbanken zal nadelig zijn voor alle toekomstige toepassingen die gebaseerd zijn op deze informatie en zal de betrokkenen onherstelbare schade berokkenen. Bv. indien de vingerafdrukken van iemand in verband worden gebracht met de identiteit van een ander persoon, kan laatstgenoemde toegang krijgen tot de diensten van eerstgenoemde zonder daartoe het recht te hebben. Dit zou leiden tot identiteitsdiefstal waardoor, ongeacht het feit of dit al dan niet wordt opgespoord, de vingerafdrukken van de betrokkene niet meer betrouwbaar zijn voor latere toepassingen zodat zijn of haar vrijheid wordt beperkt.

Fouten in biometrische systemen kunnen ernstige gevolgen hebben; met name de onterechte weigering van geautoriseerde personen en de onterechte aanvaarding van niet geautoriseerde personen kunnen op talrijke verschillende niveaus heel wat ernstige problemen opleveren. Het gebruik van biometrische gegevens zal van tevoren deze risico's moeten uitsluiten. Het systeem kan echter ook de illusie wekken dat de identificatie of authenticatie/verificatie van de betrokkene altijd correct is. De betrokkene vindt het misschien moeilijk of zelfs onmogelijk om het tegendeel te bewijzen. En systeem zou bijvoorbeeld per vergissing een betrokkene kunnen identificeren als iemand die een vliegtuig niet mag nemen of een bepaald land niet in mag komen en deze betrokkene zou weinig mogelijkheden hebben om dit probleem op te lossen wanneer hij geconfronteerd wordt met "onweerlegbare" bewijzen tegen hem. In dergelijke gevallen kan elk besluit met rechtsgevolgen voor een persoon alleen genomen worden nadat het resultaat van de geautomatiseerde verwerking overeenkomstig artikel 15 van Richtlijn 95/46/EG is bevestigd.

En tot slot moet ook vermeld worden dat het gebruik van biometrie de procedures voor de controle van bv. toegang tot gegevens van derde partijen, bijvoorbeeld voor de beveiliging tegen diefstal of misbruik (autorisatieprocedures), kan verbeteren.

3.7. Gevoelige gegevens

Sommige biometrische gegevens kunnen worden beschouwd als gevoelige gegevens in de zin van artikel 8 van Richtlijn 95/46/EG en met name gegevens over raciale of etnische afkomst of over gezondheid. In biometrische systemen die gebaseerd zijn op gezichtsherkenning kunnen bijvoorbeeld gegevens die informatie geven over raciale of etnische afkomst worden verwerkt. In dergelijke gevallen moeten de speciale garanties waarin artikel 8 voorziet, worden toegepast, naast de algemene beschermingsbeginselen van de richtlijn.

Dit betekent niet dat elke verwerking van biometrische gegevens noodzakelijkerwijze gevoelige gegevens omvat. Of een verwerking gevoelige gegevens bevat, is een kwestie van appreciatie die verband houdt met de gebruikte biometrische kenmerken en de biometrische toepassing zelf. Waarschijnlijk is dit meer het geval als biometrische gegevens in de vorm van beelden worden verwerkt, aangezien in principe ruwe gegevens niet aan de hand van de template mogen worden gereconstrueerd.

3.8. Unieke identificatiecode

Biometrische gegevens zijn uniek en de meeste genereren een unieke template (of beeld). Indien de gegevens op ruime schaal worden gebruikt, met name voor een groot deel van de bevolking, kunnen zij beschouwd worden als een identificatiemiddel dat algemeen van toepassing is, in de zin van Richtlijn 95/46/EG. In dit geval is artikel 8, lid 7, van Richtlijn 95/46/EG van toepassing en moeten lidstaten de voorwaarden voor de verwerking vaststellen.

Als het de bedoeling is biometrische gegevens te gebruiken om toegang te krijgen tot gegevensbanken waarin persoonsgegevens[24] zijn opgeslagen, kunnen er zich behoorlijk moeilijke problemen voordoen indien de betrokkene geen mogelijkheid heeft om zich tegen de verwerking van de biometrische gegevens te verzetten. Dit kan voorkomen in de relaties tussen burgers en autoriteiten.

Het is dan ook raadzaam templates en hun digitale voorstellingen te verwerken met mathematische handelingen (encryptie, algoritmen of hash-functies), waarbij voor elk biometrisch product verschillende parameters worden gebruikt om de combinatie van persoonsgegevens uit verschillende gegevensbanken via een vergelijking van templates of digitale voorstellingen te voorkomen.

3.9. Gedragscode en gebruik van privacybeschermingbevorderende technologie

De Groep dringt er bij het bedrijfsleven op aan om biometrische systemen te vervaardigen die de toepassing van de aanbevelingen in dit werkdocument vergemakkelijken en indien er Europese of internationale normen op dit gebied moeten worden ontwikkeld, dat deze worden uitgewerkt in samenwerking met de gegevensbeschermingsautoriteiten, teneinde biometrische systemen te promoten die op een voor de gegevensbescherming vriendelijke manier worden ontwikkeld, de sociale risico's tot een minimum beperken en misbruik van de gegevens voorkomen. De Groep wil in dit verband ook wijzen op het belang van privacybeschermingbevorderende technologieën (PETS = Privacy Enhancing Technologies), om het verzamelen van gegevens zoveel mogelijk te beperken en onrechtmatige verwerkingen te voorkomen.

Voorts wil de groep wijzen op het belang van de gedragscodes die moeten bijdragen aan een deugdelijke toepassing van de gegevensbeschermingsbeginselen, waarbij rekening wordt gehouden met de specifieke kenmerken van de verschillende sectoren, in overeenstemming met artikel 27 van Richtlijn 95/46/EG. Communautaire codes kunnen worden voorgelegd aan de Groep, die dan zal vaststellen of de ontwerpen beantwoorden aan de nationale bepalingen inzake gegevensbescherming die overeenkomstig Richtlijn 95/46/EG zijn goedgekeurd.

CONCLUSIES

De Groep is van oordeel dat de meeste biometrische gegevens de verwerking van persoonsgegevens inhouden. Het is daarom noodzakelijk dat bij de ontwikkeling van biometrische systemen de gegevensbeschermingsbeginselen van Richtlijn 95/46/EG

---

[24] Zie ook punt 3.2 over compatibel hergebruik.

volledig worden nageleefd, waarbij rekening wordt gehouden met de speciale aard van biometrie, onder meer met de mogelijkheid om biometrische gegevens te verzamelen zonder dat de betrokkene hiervan op de hoogte is en het feit dat een koppeling met de persoon vrijwel zeker is.

Naleving van het evenredigheidbeginsel, dat de kern vormt van de bescherming die door Richtlijn 95/46/EG wordt geboden, houdt, met name in het kader van authenticatie/verificatie, in dat duidelijk voorkeur moet worden gegeven aan biometrische toepassingen die geen gegevens verwerken die verkregen zijn op basis van fysieke sporen die onbewust door personen zijn achtergelaten of niet in een gecentraliseerd systeem worden bewaard. Dit biedt voor de betrokkene de mogelijkheid om beter controle uit te oefenen op de persoonsgegevens die over hem of haar worden verwerkt.

De Groep zal dit werkdocument herzien in het licht van de ervaring van de gegevensbeschermingsautoriteiten en de technologische ontwikkelingen m.b.t. biometrische toepassingen. Nu biometrische gegevens steeds meer gebruikt worden voor verschillende soorten toepassingen en bij talrijke verschillende gelegenheden, moet zo snel mogelijk werk gemaakt worden van een goede regeling, met name in het kader van werkgelegenheid, visa en immigratie en veiligheid bij het reizen.

Aangezien het de taak is van het bedrijfsleven om biometrische systemen te ontwikkelen die verenigbaar zijn met gegevensbescherming, zou het vanuit alle oogpunten heel nuttig zijn om tussen alle belanghebbende partijen, waaronder de gegevensbeschermingsautoriteiten, een dialoog tot stand te brengen op basis van een ontwerp voor een gedragscode.

Gedaan te Brussel, 13 juni 2003
Voor de Groep
De Voorzitter
Stefano RODOTÀ