Advies nr. 17/2008 van 9 april 2008

Betreft: Advies uit eigen beweging over het verwerken van biometrische gegevens in het raam van authenticatie van personen (A/2008/017)

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 29;

Gelet op het verslag van de voorzitter, de heer Willem DEBEUCKELAERE.

Brengt uit eigen beweging op 09/04/2008 het volgend advies uit:

I. TOEPASSINGSGEBIED VAN HET ADVIES

1. Dit advies uit eigen beweging handelt over het verwerken van biometrische gegevens in het raam van de authenticatie van personen.

2. Dit advies handelt niet over het gebruik van de biometrie bij grenscontroles en ook niet over de verwerkingen die verricht worden door politie- en veiligheidsdiensten (law enforcement). De Commissie blijft evenwel de actuele ontwikkelingen in deze zaken aandachtig volgen, meer bepaald op Europees niveau. Zij zal zich hierover te gelegener tijd uitspreken.

3. De authenticatie is een proces dat erin bestaat een vermeende identiteit van een bepaald wezen (zoals een persoon)[1] te verifiëren. In het algemeen kan de authenticatie gebeuren op verschillende manieren:

   - Hetzij via een element dat men als enige kent, zoals een paswoord ("wat men weet").
   - Hetzij via een voorwerp waarvan men houder is, zoals een badge ("wat men bezit").
   - Hetzij door "wat men is" zoals bij het gebruik van een biometrisch kenmerk.

4. Terwijl de identificatie toelaat de identiteit van een wezen, met andere woorden de identiteit van een individu in de schoot van een bepaalde bevolkingsgroep[2] vast te stellen, beoogt de authenticatie het verifiëren van deze identiteit (de verzekering te krijgen dat het individu wel degelijk de persoon is die hij beweert te zijn).

5. De authenticatie wordt in het algemeen gebruikt om rechten toe te kennen die in de regel voorbehouden zijn aan een bepaald publiek (toegang tot een lokaal, tot een informaticasysteem…).

---

[1] Zie de definities van ISO :

- authenticiteit : "the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information" (ISO/IEC 13335-1: 2004).

- authenticatie: "Provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication)" (ISO/IEC 18028-4: 2005)

[2] Definitie voorgesteld aan ISO: "Recognizing an entity within some context with unique identity references and additional information that characterizes the entity" (**http://www.jtc1sc27.din.de/sce/SD6**).

6. In verschillende situaties is het nuttig om na te gaan of individuen die beweren dat zij geregistreerd zijn, wel degelijk zijn wie ze beweren te zijn: dit is onder meer het geval bij de controle en het toegangsbeheer voor bepaalde voorbehouden ruimten (ingang van een gebouw, luchthavendomein, goederenopslagplaatsen…), de toegangscontrole aan voorbehouden diensten (toegang tot een PC banking systeem) of bij controle van de werktijden.

7. De Commissie brengt dit advies uit, rekening houdend met de huidige kennis van de biometrische technologie. Zij behoudt zich natuurlijk de mogelijkheid voor haar houding ter zake in de toekomst aan te passen in functie van de evolutie van de technologie en haar ervaringen op dit gebied.

II. DE BIOMETRIE: ALGEMENE VERKLARINGEN

A. Definitie en belang van de biometrie

8. Biometrie is de wetenschap van biologische variaties die als doel heeft de identiteit van het individu te bepalen of te verifiëren met behulp van procedures die steunen op de onderscheiden en individuele menselijke kenmerken[3].

9. Bepaalde kenmerken zijn inderdaad eigen aan elk individu, of zelfs uniek, waardoor ze zich onderscheiden van andere personen binnen een bepaalde bevolkingsgroep. Biometrische kenmerken vertonen de bijzonderheid « d'être des caractéristiques physiques uniques et particulières d'une personne pouvant – du moins théoriquement – lui être attribuées en tout lieu et en tout temps avec une certitude quasi absolue »[4]. (vrije vertaling : unieke en bijzondere fysische kenmerken te zijn van een persoon die –althans theoretisch – om het even waar en te allen tijde met quasi absolute zekerheid aan die persoon kunnen toegewezen worden).

---

[3] Zie bijvoorbeeld, Corien Prins, « Biometric technology law. Making our body identify for us : legal implications of biometric technologies », *Computer Law & Security Report*, Vol. 14, n°3, 1998, p. 159 et s ; Daniel Guinier, « Biométrie : classification au vu des nouveaux motifs », *Expertises*, Février 2005, p. 62 en v. ; Het « Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques » opgesteld door de Raad van Europa in februari 2005 ; Ann Cavoukian et Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy,* Information and Privacy Commissioner/Ontario, Maart 2007; Gérard Dubey, "L'identité à l'épreuve de la biométrie", in *La sécurité aujourd'hui dans la société de l'information*, Contributions réunies et coordonnées par Stéphanie Lacour, L'harmattan, Paris, 2007, p. 87 en v.

[4] Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données opgesteld door PRIVATIM, de Zwitserse commissarissen inzake gegevensbescherming, oktober 2006, n°3.1.2.

10. Die kenmerken kunnen van verschillende orde zijn, met name fysieke, gedrags- of genetische kenmerken, zoals het DNA, het netvlies, de iris, de vingerafdrukken, de geometrie van de handomtrek, gelaatsherkenning, de stem, het handschrift, de manier van typen op het klavier van een PC, de manier om zich voort te bewegen, enz....

11. Hoewel de biometrie reeds geruime tijd bestaat vertoont haar toepassing de neiging om uit te breiden, onder meer dankzij de introductie van nieuwe technologieën die het mogelijk maken de analyse- en vergelijkingsprocedures van de kenmerken van individuen te automatiseren. Die automatisering versnelt de verwerking en vermindert ook het risico op vergissingen. Overigens is de verminderde kostprijs voor het gebruik van die technologieën eveneens medeverantwoordelijk voor deze expansie.

12. Vermits de biometrische technologieën kenmerken gebruiken die intrinsiek verbonden zijn met de persoon kunnen zij de veiligheid verbeteren en bepaalde risico's op fraude verminderen. Het gebruik van de biometrie laat in tegenstelling tot het uitsluitend gebruik van andere authenticatiemiddelen (paswoorden of badges) inderdaad toe om het bewijs te versterken, met andere woorden de band tussen de fysieke persoon en zijn identiteit. Dit verklaart waarom men de biometrie thans beschouwt als een sterk authenticatiemiddel[5].

B. Werkwijze

1) Twee inzamelingsfasen en twee functies van biometrische systemen

13. De werking van een biometrisch systeem wordt opgesplitst in twee fasen van inzameling van de informatie en twee manieren om de ingezamelde informatie te vergelijken (de twee functies van biometrische systemen):

[5] Volgens de definitie van 'authenticatie: "[...] Strong authentification is either based on strong mecanisms (e.g. biometrics) or makes use of at least two (...) factors (so-called multi-factor authentification)" (ISO/IEC 18028-4: 2005).

14. De eerste inzamelingsfase, zogenaamd de inschrijving (of de registratie) is het ogenblik waarop een biometrisch kenmerk van een individu wordt ingezameld en geregistreerd op een drager voor informatieopslag (hetzij een individuele drager zoals een chipkaart, hetzij in een databank). Deze referentie-informatie zal naargelang het gekozen systeem, ofwel een afbeelding zijn («ruwe gegevens») ofwel relevante gegevens die een uittreksel zijn van die afbeelding, template genoemd («template» of «staal» dat bestaat uit een opeenvolging van cijfers die een biometrisch element kenmerken). Het opslaan van de afbeelding vergt meer opslagruimte dan het opslaan van de template.

15. Tijdens de tweede inzamelingsfase toont het individu opnieuw zijn biometrische kenmerken aan het systeem dat hem moet authenticeren. Op dat ogenblik wordt een tweede biometrisch staal genomen (een persoon houdt bijvoorbeeld zijn vinger voor de sensor) en deze informatie (de afbeelding of de template) wordt dan vergeleken met de referentie-informatie om na te gaan of deze overeenstemmen. Als de informatie die ingezameld wordt tijdens de tweede inzameling overeenstemt met de referentie-informatie (positieve koppeling) beschouwt het systeem de persoon die zich aanbiedt als diegene die vooraf werd geregistreerd bij de inschrijvingsfase.

16. Er bestaan twee manieren om de informatie te vergelijken die verkregen werd tijdens de twee inzamelingsfasen en zij vormen de twee belangrijkste functies van de biometrie: de identificatiefunctie en de verificatiefunctie. Deze beide functies kunnen aangewend worden in het raam van de authenticatie (zie evenwel paragraaf 59 van dit advies waarin de Commissie het gebruik van de verificatiefunctie aanbeveelt in het raam van de authenticatie van personen).

17. De identificatiefunctie bestaat erin de informatie van de tweede fase te vergelijken met al de biometrische informatie die beschikbaar is in het biometrisch systeem en die per definitie opgeslagen is in een databank ("one-to-many comparison"). Deze functie zal in de eerste plaats toelaten de gebruiker te identificeren tussen alle geregistreerde personen en kan in een latere fase dienen om hem te authenticeren.

18. De verificatiefunctie bestaat erin om de informatie van de tweede fase te vergelijken met de vooraf geregistreerde informatie toebehorend aan één enkele persoon[6] ("one-to-one comparison"). Deze functie is dus bijzonder aangepast aan situaties waar de persoon zich wenst te authenticeren en dus bereid is om vrijwillig een element kenbaar te maken dat toelaat om hem te identificeren (zoals een chip-kaart of een badge) op basis waarvan de biometrische referentie-informatie zal vastgesteld worden en vervolgens vergeleken worden met het staal van de nieuwe inzameling.

2) Biometrische systemen zijn betrouwbaar maar er bestaat altijd een zekere foutenmarge

19. Er moet onderstreept worden dat de afbeelding of de template van de referentie-informatie slechts zelden zal overeenstemmen met de later vertoonde informatie. Het volstaat om het biometrisch gegeven in lichtjes gewijzigde omstandigheden te vertonen opdat de hieruit bekomen informatie eveneens zou verschillen (zo zal de lichtintensiteit de gegevens met betrekking tot het aangezicht beïnvloeden, de temperatuur de gegevens over een hand, de uitgeoefende druk de gegevens van een vingerafdruk, enz.). Dit is de reden waarom de vergelijking steeds gebeurt op basis van kansberekeningen.

20. Bijgevolg bevat ieder biometrisch systeem onvermijdelijk een zekere foutenmarge. Het gaat om de zogenaamde "foutieve verwerpingen" (False Rejection Rate) waardoor een bepaald percentage personen wordt afgewezen terwijl zij eigenlijk moesten aanvaard worden (verwerping van "gewettigde gebruikers") en ook een zeker aantal foutieve aanvaardingen (False Acceptation Rate) waardoor een zeker percentage personen wordt aanvaard dat niet aanvaard had mogen worden (aanvaarding van "bedriegers").

21. De gekozen techniek beïnvloedt de betrouwbaarheid van het systeem. Zo is thans het gebruik van de vingerafdruk betrouwbaarder dan de gelaatsherkenning. Het is eveneens mogelijk om verschillende biometrische kenmerken te combineren om aldus de betrouwbaarheid van het systeem te verhogen.

---

[6] Definitie van de verificatiefunctie voorgesteld aan ISO: "Biometric product function that performs a one-to-one comparison" (**http://www.jtc1sc27.din.de/sce/SD6**). Wij onderstrepen dat in het bijzonder kader van de biometrie de verificatiefunctie een specifieke betekenis heeft die totaal verschilt van het begrip authenticatie. Inderdaad, de authenticatie (zijnde het proces om de identiteit te verifiëren) kan gebeuren aan de hand van de twee biometrische functies, hetzij aan de hand van de identificatiefunctie, hetzij aan de hand van de verificatiefunctie (zie evenwel de paragraaf 59 van dit advies waarin de waarin de Commissie het gebruik van de verificatiefunctie aanbeveelt in het raam van de authenticatie).

22. Bovendien is de schaal van toegestane vergissingen aanpasbaar en zal deze door de leverancier van biometrische systemen geval per geval aangepast worden in functie van de voorziene gebruiksdoeleinden en de noden van de verantwoordelijke voor de verwerking. Om voldoende snel te zijn in het gebruik en om te vermijden dat een persoon verschillende keren na mekaar zijn biometrische kenmerken moet aanbieden, of zelfs moet overgaan tot een nieuwe registratie, is het aangewezen om een systeem te voorzien met een zo laag mogelijk percentage valse verwerpingen. Inderdaad, indien men gebruik maakt van een systeem met een te hoge verwerpingsschaal vereist men een zeer grote gelijkenis tussen het aangeboden biometrisch gegeven en de referentie-informatie. Zo'n systeem heeft voor gevolg dat een gebruiker die aanvaard moest worden (gewettigde gebruiker) sneller zal verworpen worden omdat hij zijn biometrisch kenmerk niet heeft getoond op een voldoende gelijkaardige wijze als bij het opslaan van zijn referentie-informatie. Doch het verminderen van dit aantal foutieve verwerpingen verhoogt onvermijdelijk het percentage foutieve aanvaardingen waardoor het veiligheidsniveau van het systeem vermindert omdat het risico dat personen onterecht geaccepteerd worden ("bedriegers") vergroot. Het vinden van het juiste evenwicht zal derhalve moeten overlegd worden tussen de leverancier van biometrische oplossingen en de verantwoordelijke voor de verwerking.

23. Er dient onderstreept te worden dat biometrische systemen in het algemeen goed presterende systemen zijn. Men mag evenwel niet uit het oog verliezen dat een zeker risico op vergissingen, inherent aan het systeem, blijft bestaan en dat dergelijke systemen bijgevolg niet als onfeilbaar kunnen beschouwd worden.

24. Bovendien zijn biometrische systemen niet altijd bruikbaar voor iedereen. Zo beschikt bijvoorbeeld 4% van de bevolking niet over voldoende waarneembare vingerafdrukken om automatisch herkend te worden door een biometrisch systeem[7]. Bepaalde personen met een handicap zouden eveneens in de onmogelijkheid kunnen verkeren om gebruik te maken van een biometrisch systeem. Er zou dus moeten vermeden worden dat de biometrie aanleiding zou geven tot discriminatie door personen te marginaliseren die geen gebruik kunnen maken van deze systemen[8].

---

[7] Zie het verslag « Identity Management for eGovernment, Study and assessment of Biometric techniques for eGovernment application », *op. cit.*, blz. 15. Andere bronnen spreken van 2%, zie de « Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données » uitgebracht door PRIVATIM, *op. cit*.

[8] Dr Jean-Philippe Walter (Préposé fédéral suppléant à la protection des données in Zwitserland), "Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé", 26e Conférence internationale des Commissaires à la protection des données et à la vie privée Wroclaw, 14 – 16 september 2004.

III. TOEPASBAARHEID VAN DE WET BETREFFENDE DE VERWERKING VAN PERSOONSGEGEVENS (WVP)

A. Het biometrisch gegeven is een persoonsgegeven

25. Overeenkomstig artikel 1 §1 van de WVP moet "onder persoonsgegevens" iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon worden verstaan, (...) als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van één of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

26. Het biometrisch gegeven, of het nu een afbeelding betreft dan wel het gegevensuittreksel van die afbeelding (de template) is een fysiek kenmerk van een individu. Dit gegeven kan op zich informatie onthullen over een natuurlijke persoon maar ook de omstandigheden van de inzameling kunnen bijkomende persoonlijke informatie opleveren (zo kan de verwerking van gegevens betreffende de plaats en het ogenblik van de inzameling toelaten de aanwezigheid van een persoon op een bepaald ogenblik op een bepaalde plaats te achterhalen).

27. Vanaf het ogenblik dat het verband tussen het biometrisch gegeven en een fysieke persoon met behulp van redelijke middelen kan worden gelegd door de verantwoordelijke voor de verwerking of enig ander persoon, gaat het om een persoonsgegeven.

28. Bijgevolg beschouwt de Commissie de biometrische gegevens in principe als persoonsgegevens.[9]

[9] In zeldzame gevallen is een biometrisch gegeven geen persoonsgegeven. Het gaat hier bijvoorbeeld over een biometrisch gegeven waarvan het verband met een betrokkene niet met redelijke middelen kan worden aangetoond. Dit is afhankelijk van de kwaliteit van het ingezameld gegeven (gedeeltelijke digitale vingerafdruk die niet bruikbaar is) of de omstandigheden waaronder een gegeven werd ingezameld (omstandigheden van plaats en tijd die het niet mogelijk maken om de doelgroep waarvan de betrokkene deel uitmaakt voldoende te bepalen). Het is echter essentieel te onderstrepen dat een biometrisch gegeven dat op een bepaald ogenblik geen persoonsgegeven is, het later wel kan worden (nieuwe feitelijke omstandigheden of nieuwe technologieën die het mogelijk maken dat een identificatie gemakkelijker kan gebeuren).

B. Het biometrisch gegeven kan een gevoelig gegeven[10] zijn

29. Bepaalde biometrische gegevens kunnen informatie vrijgeven over de gezondheidstoestand of de raciale herkomst.[11]

30. Wanneer biometrische gegevens gebruikt worden om er informatie uit af te leiden die betrekking heeft op bijvoorbeeld de gezondheidstoestand of de raciale herkomst, dienen die gegevens beschouwd te worden als gevoelige gegevens.

31. Door slechts een deel van de gegevens ontleend uit de afbeelding (de template) te verwerken en niet de afbeelding zelf, kan men een verwerking van gevoelige gegevens vermijden.[12]

C. Het gebruik van de biometrie impliceert een gegevensverwerking

32. De WVP definieert de “verwerking” als elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens.[13]

33. Het gebruik van biometrische systemen veronderstelt de inzameling, de registratie en de opslag van al dan niet biometrische persoonsgegevens en dit met behulp van geautomatiseerde middelen.

---

[10] In het raam van de bescherming van het privéleven zijn gevoelige gegevens de gegevens die bedoeld worden in de artikelen 6,7 en 8 van de WVP.

[11] De DNA-gegevens bijvoorbeeld maar ook andere soorten van biometrische gegevens zoals de digitale vingerafdruk of de geometrie van de handomtrek (zo zou een dergelijk systeem een gezondheidsprobleem aan het licht kunnen brengen dat geregeld fysieke variaties van de hand tot gevolg heeft en dat het gebruik van het biometrisch systeem voor die persoon zou bemoeilijken).

[12] Zo zullen de gegevens die de gezondheidstoestand of de raciale herkomst kunnen onthullen, misschien worden getoond op de afbeelding maar niet meer in de gegevens die afgeleid worden uit deze afbeelding (template). Zie in dit verband eveneens punt 74 van het « Rapport d’étape sur l’application des principes de la Convention 108 à la collecte et au traitement des données biométriques », *op. cit*.

[13] Artikel 1 §2 van de WVP.

34. Het gebruik van deze systemen impliceert dus een verwerking van persoonsgegevens.

IV. TOEPASSING VAN DE BEGINSELEN VAN DE WET BETREFFENDE DE VERWERKING VAN PERSOONSGEGEVENS (WVP)

A. Rechtmatigheid en proportionaliteit[14]

1) Het rechtmatigheidsbeginsel

35. Elk persoonsgegeven moet verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden.

36. Om gerechtvaardigd te zijn moet elk doeleinde onder meer voldoen aan een van de voorwaarden van artikel 5 van de WVP.

37. Het gebruik van biometrische gegevens voor authenticatie van personen is in principe mogelijk wanneer de betrokkenen hun toestemming[15] hebben verleend. Deze toestemming draagt ongetwijfeld bij tot de sociale aanvaarding van deze nieuwe technologieën door de gebruikers.

38. De Commissie onderstreept dat een geldige toestemming een vrije, specifieke en op informatie berustende toestemming[16] is.

39. De aandacht dient er eveneens op gevestigd te worden dat het verkrijgen van een toestemming een overmatige verwerking niet rechtvaardigt (zie paragraaf 41 hierna). Dit is onder meer het geval wanneer de biometrische verwerking niet absoluut noodzakelijk is om het beoogde resultaat te bereiken.

40. Overigens zal de verwerking eveneens kunnen toegestaan worden indien zij voorzien is door een wet[17] of wanneer de verantwoordelijke voor de verwerking een gerechtvaardigd belang

---

[14] Artikelen 4 en 5 van de WVP.

[15] Artikel 5 a) van de WVP.

[16] Zie de definitie van toestemming in artikel 1 §8 van de WVP.

[17] Artikel 5 c) van de WVP.

kan doen gelden dat zwaarder doorweegt dan de belangen of de fundamentele rechten en vrijheden van de betrokkene[18].

2) Proportionaliteitsbeginsel: afweging van de aanwezige belangen

41. Een rechtmatig doeleinde houdt eveneens in dat de verwerking niet overmatig is: het algemeen belang of het gerechtvaardigd belang van de verantwoordelijke voor de verwerking moeten afgewogen worden tegenover het recht op de bescherming van het privéleven van de betrokkenen.

a. Belang van de verantwoordelijke voor de verwerking

42. Het gebruik van de biometrie kan aan de verantwoordelijke voor de verwerking bepaalde voordelen bieden vermits het authenticatieproces geautomatiseerd verloopt, meer zekerheid biedt dan andere klassieke systemen en soms ook goedkoper is.

43. Behoudens de voordelen met betrekking tot de kostprijs en de gebruiksvriendelijkheid is het specifieke voordeel van het gebruik van een biometrisch systeem in vele gevallen zeker en vast de verbeterde veiligheid. Inderdaad, het biometrisch systeem wordt beschouwd als een sterk authenticatiemiddel[19].

44. De beveiliging perfectioneren kan tot een betere bescherming leiden van personen en goederen of tot een grotere doeltreffendheid van de strijd tegen fraude. De biometrie maakt inderdaad de strijd tegen fraude mogelijk (bijvoorbeeld de ongeoorloofde toegang tot diensten) door te vermijden dat een authenticatiemiddel (zoals een paswoord of een badge) bewust aan een derde wordt doorgegeven of wordt misbruikt. Wanneer bijvoorbeeld het werktijdenbeheer van medewerkers enkel gebaseerd is op het gebruik van een badge is het altijd mogelijk dat sommigen hun badge doorgeven aan collega's om hun aanwezigheid te veinzen ("prikklokfraude") wat niet langer mogelijk is indien men er een biometrisch authenticatiemiddel aan toevoegt.

b. Belang van de betrokkenen wat de eerbiediging van hun privéleven betreft

[18] Artikel 5 f) van de WVP.

[19] Volgens de definitie van authentificatie: "[...] Strong authentification is either based on strong mecanisms (e.g. biometrics) or makes use of at least two (...) factors (so-called multi-factor authentification)" (ISO/IEC 18028-4: 2005). De bedoelde factoren zijn de authenticatie door de kennis, het bezit of de persoonlijke kenmerken.

45. Het gebruik van biometrische gegevens roept enkele bijzondere bedenkingen op met betrekking tot de gegevensbescherming. Inderdaad, de biometrische gegevens zijn een specifieke categorie gegevens vermits zij voortvloeien uit het menselijk lichaam en in een normale situatie levenslang onveranderlijk blijven[20]. De integriteit van het menselijk lichaam en de manier waarop hiermee wordt omgesprongen vormen overigens een aspect van de menselijke waardigheid[21].

46. Bovendien is een biometrisch gegeven een identificatiemiddel[22] dat toelaat een individu in een bepaalde context op een unieke wijze te identificeren[23].

47. Er bestaan eveneens risico's die verbonden zijn aan het gebruik van de biometrie zoals de identiteitsdiefstal. De identiteitsdiefstal vormt een des te groter risico omdat de doelstelling van de biometrie er net in bestaat een sterkere authenticatie op te leveren (met andere woorden, een sterkere band tussen de gebruiker en zijn identiteit)[24]. Bovendien worden de gevolgen van identiteitsdiefstal vaak onderschat en zijn zij moeilijk aan te tonen[25]. Anderzijds kan het gebruik van de biometrie nieuwe fysieke risico's inhouden voor de gebruikers. Zo werd vastgesteld dat bij diefstallen van luxewagens de dieven niet geaarzeld hebben om fysiek geweld te gebruiken om de biometrische veiligheidsmaatregelen waarmee het voertuig was uitgerust te omzeilen[26].

48. Er moet worden benadrukt dat de risico's op privacyinbreuken kunnen variëren in functie van het soort biometrische gegevens dat wordt gebruikt. Bijvoorbeeld, bij de biometrische systemen die verwijzen naar fysieke kenmerken die geen sporen nalaten is het risico dat de

[20] Zie punt 107-1 van het « Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques », *op. cit*. Deze bijzondere verhouding met het lichaam laat toe het verband tussen het gegeven en de persoon te versterken (« linkability ») en impliceert derhalve ook een groter risico inzake mogelijkheden tot profilering, koppelingen van informatie aan de hand van dit identificatiemiddel en bijgevolg op inbreuk op de privacy (zie het verslag « Identity Management for eGovernment, Study and assessment of Biometric techniques for eGovernment application », Instituut voor Breedband Technologie (IBBT), Juni 2007, n°3.3.2, p. 13).

[21] Zo zou de menselijke waardigheid onder meer kunnen worden aangetast « lorsque des procédés biométriques –parfois combinés avec d'autres applications techniques- conduisent à considérer l'être humain exclusivement comme un objet ou un numéro, en d'autres termes, comme une marchandise », (vrije vertaling: wanneer biometrische systemen – soms in combinatie met andere technische toepassingen – er zouden toe leiden de mens louter als een voorwerp of een nummer te beschouwen of met andere woorden als koopwaar) zie de Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données opgesteld door PRIVATIM, *op. cit*

[22] Identity Management of eGovernment, Deliverable 4.1, "Study and assessment of biometric techniques for eGovernment applications, Het Interdisciplinair instituut voor Breedband Technologie (IBBT), projet IDEM, , June 2007, p. 13

[23] Het Comité consultatif national français d'éthique pour les sciences de la vie et de la santé heeft eveneens de bijzondere risico's onderstreept van identificatietechnieken voor personen gebaseerd op hun biologische kenmerken en meer bepaald het verschuiven van de identiteitscontrole naar een controle op het gedrag en de persoonlijkheid, van de koppeling van gegevens en het verkrijgen van deze laatste buiten het medeweten van de betrokkenen.

[24] Identity Management of eGovernment, Deliverable 4.1, "Study and assessment of biometric techniques for eGovernment applications, Het Interdisciplinair instituut voor Breedband Technologie (IBBT), projet IDEM, June 2007, p. 14

[25] *Ibidem*.

[26] De dief zou de vinger van de eigenaar hebben afgesneden, zie de website van BBC news http://news.bbc.co.uk , informatie verstrekt op 31 maart 2005

bescherming van de privacy wordt aangetast kleiner dan bij systemen die gebruik maken van fysieke kenmerken die sporen nalaten."[27]

49. "De biometrische kenemerken die sporen nalaten" zijn fysieke, biometrische bijzonderheden die worden achtergelaten daar waar de betrokken persoon fysiek aanwezig is geweest en die dus "sporen heeft nagelaten" (zoals vingerafdrukken op voorwerpen of verloren haren die zijn DNA bevatten). Andere biometrische kenmerken laten geen sporen na (zoals de aders van de vinger of de hand, de handomtrek, de iris of het netvlies).

50. De Commissie onderstreept dat systemen die gebruik maken van fysieke kenmerken die geen sporen nalaten minder risico's vormen voor de bescherming van de fundamentele rechten en vrijheden van personen. Inderdaad, de biometrische systemen "met sporen" vormen een groter risico op hergebruik van de gegevens voor andere doeleinden dan deze die oorspronkelijk waren voorzien.

51. Meer in het algemeen wenst de Commissie de aandacht te vestigen op de maatschappelijke keuze die gepaard gaat met een veralgemening van het gebruik van de biometrie. De uitbreiding van biometrische systemen zou een groot risico op desensibilisering van het publiek kunnen meebrengen ten aanzien van het steeds toenemende gebruik van hun gegevens en de gevolgen die deze verwerkingen zouden kunnen hebben op hun dagelijks leven[28]. De Groep 29[29] onderstreept bijvoorbeeld dat het gebruik van de biometrie in schoolbibliotheken het risico inhoudt dat de kinderen zich minder bewust zullen zijn van de risico's die verbonden zijn aan de gegevensbescherming en de gevolgen die dit kan hebben voor hun latere leven[30].

---

[27] Zie het werkdocument over de biometrie van de Groep artikel 29, op.cit. blz. 6-7.

[28] Zie het werkdocument over de biometrie van de Groep artikel 29, GT80, aangenomen op 1 augustus 2003, blz. 2-3

[29] De Groep 29 omvat onder meer de vertegenwoordigers van alle nationale Europese overheden inzake gegevensbescherming.

[30] Zie het werkdocument over de biometrie van de Groep artikel 29, GT80, aangenomen op 1 augustus 2003, blz. 3

c. Gevolgen van de toepassing van het proportionaliteitsbeginsel voor de verantwoordelijke voor de verwerking:

- Strikte beoordeling van het proportionaliteitsbeginsel en rechtvaardiging van het gebruik

52. De Commissie meent dat de beoordeling van de proportionaliteit van de verwerkingen van biometrische gegevens moet gedaan worden door de verantwoordelijken voor de verwerking op een strikte wijze en mits rekening te houden met de gevolgen op lange termijn voor de betrokkenen.

53. De verantwoordelijken voor de verwerking moeten een concrete en nauwkeurige afweging maken van de aanwezige belangen en moeten de redenen die hun voornemen om gebruik te maken van een biometrisch systeem rechtvaardigen duidelijk definiëren, motiveren en ter kennis brengen van de betrokkenen.

- Verificatie van de reële noodzaak om persoonsgegevens te verwerken

54. Zo moeten de verantwoordelijken voor de verwerking zich in de eerste plaats afvragen of een controle van de identiteit van de betrokkenen werkelijk noodzakelijk is (authenticatie). De beperkte toegang tot een gebouw of een dienst betekent niet altijd dat een verwerking van persoonsgegevens noodzakelijk is. Zo zouden de consumenten de mogelijkheid moeten krijgen om anoniem te consumeren of in te schrijven voor bepaalde diensten.

- Opteren voor een biometrisch systeem dat de privacy eerbiedigt en de gegevensverwerkingssystemen vergelijken die op de markt zijn.

55. Wanneer de verantwoordelijke voor de vewerking een biometrisch systeem wenst te gebruiken, moet hij kiezen voor het systeem dat het meest de privacy eerbiedigt en dat bijgevolg propotioneel is.

56. Onder bepaalde voorwaarden kan het opteren voor een biometrisch systeem op zich al beschouwd worden als proportioneel. Indien de voorwaarden niet vervuld zijn, dient de verantwoordelijke voor de verwerking eerst het biometrisch systeem dat hij wenst te gebruiken te vergelijken met de andere bestaande gegevensverwerkingssystemen (niet-biometrische) op de markt.

- *Een biometrisch systeem dat op zich proportioneel is*

57. De Commissie beschouwt de optie voor een biometrisch systeem als proportioneel op zich als de verantwoordelijke voor de verwerking:

1) Geconfronteerd wordt met een situatie waar de verwerking van persoonsgegevens noodzakelijk of proportioneel is;
2) Gebruik maakt van een biometrisch systeem dat betrekking heeft op fysieke kenmerken die geen sporen nalaten (zie de paragrafen 48-50 van dit advies);
3) De hiernavolgende aanbevelingen naleeft:

➲Geen biometrische systemen te kiezen die referentie-informatie opslaan in een databank

58. Inderdaad, wanneer men een biometrisch systeem gebruikt voor authenticatie van personen is het niet noodzakelijk de biometrische referentie-informatie te verzamelen in een centrale databank. Deze informatie zou bij voorkeur moeten opgeslagen worden op een beveiligde verwijderbare drager[31] (zoals een chipkaart) die bewaard wordt door de betrokkene of, in voorkomend geval, in het toestel waarin de biometrische sensor geplaatst is (bijvoorbeeld aan de ingang van het gebouw) en dat beveiligd is en slechts lokaal toegankelijk (zonder mogelijke koppeling met andere informaticasystemen) .

59. Bijgevolg dient de verificatiefunctie van het biometrisch systeem gebruikt te worden ("one-to-one" vergelijking, zie paragrafen 17 en 18 van dit advies) en niet de identificatiefunctie ("one-to-many vergelijking") die noodzakelijkerwijs het gebruik van een databank vereist.

[31] Zie punt 88 van dit document voor verdere informatie over de veiligheidsmaatregelen voor de drager.

60. Het gecentraliseerd opslaan van biometrische gegevens verhoogt het risico op een later hergebruik van de gegevens voor onverenigbare doeleinden alsook het risico dat de gegevens zouden gebruikt worden als sleutel voor het koppelen van verschillende databanken[32].

61. Het feit dat de opslag in een databank het biometrisch systeem gebruiksvriendelijker maakt (dit laat inderdaad authenticatie toe zonder dat men een bijkomende verwijderbare drager zoals een chipkaart bij zich moet hebben) laat niet toe de bijkomende risico's voor de gegevensbescherming, die veroorzaakt worden door de opslag in een databank, te rechtvaardigen.

62. De gegevens opslaan op een beveiligde verwijderbare drager die in het bezit blijft van de betrokkene laat deze laatste bovendien toe de controle te bewaren over zijn biometrische gegevens.

➲ Geen onbewerkte biometrische gegevens (de afbeeldingen) op te slaan maar templates

63. Het is niet noodzakelijk om de onbewerkte biometrische gegevens op te slaan zoals bijvoorbeeld de afbeelding van de vingerafdruk. Enkel de template, met andere woorden de relevante gegevens die verkregen werden uit de onbewerkte gegevens zouden moeten bewaard worden.

64. Het opslaan van de afbeelding verhoogt het risico op het opnieuw kruisen van informatie en het koppelen van databanken.

[32] Zie het werkdocument over de biometrie van de Groep 29, *op. cit.*, blz. 8 ; alsook het verslag « Identity Management for eGovernment, Study and assessment of Biometric techniques for eGovernment application », *op. cit.*, n°3.3.4, blz. 14

➲ **Geen technologieën te gebruiken die toelaten om biometrische gegevens in te zamelen of te verwerken buiten het medeweten van de betrokkene.**

65. De biometrische technologieën moeten transparant zijn voor de betrokkenen (zie hiervoor onder punt B, paragraaf 78) en het is aangewezen geen biometrische gegevens in te zamelen of te verwerken buiten het medeweten van de betrokkene. Sommige biometrische systemen zoals de gelaatsherkenning van op afstand, het inzamelen van vingerafdrukken of stemopnamen vertonen in dit opzicht meer risico's[33].

➲ **Een beveiligd biometrisch systeem te gebruiken**

66. Het biometrisch systeem moet eveneens gekozen worden in functie van de veiligheidsmaatregelen die het bevat ter bescherming van de biometrische gegevens (zie hierna onder punt D, paragraaf 84).

- Noodzaak om het gewenst biometrisch systeem te vergelijken met andere op de markt bestaande gegevensverwerkingssystemen (niet-biometrische) en naleving van de aanbevelingen

67. Omgekeerd, wanneer de verantwoordelijke voor de verwerking een systeem wenst te gebruiken dat verwijst naar fysieke kenmerken die sporen nalaten, moet hij eerst zijn biometrische systeem vergelijken met de andere bestaande gegevensvewerkingssystemen op de markt.

68. De verantwoordelijke voor de verwerking moet bijgevolg een concrete afweging maken van de verschillende verwerkingssystemen die te zijner beschikking staan om het gewenste resultaat te bereiken en bij voorkeur deze gebruiken die het privéleven het meest eerbiedigen en algemeen aanvaard worden door de samenleving. De verantwoordelijke voor de verwerking moet dus een vergelijking maken tussen de verschillende authenticatiesystemen en nagaan of hetzelfde resultaat niet zou kunnen bereikt worden met een systeem dat minder ingrijpend is voor het privéleven, zoals een visuele herkenning (vergelijking met de foto van een kaart of een badge)

[33] Zie het werkdocument over de biometrie van de Groep 29, *op. cit.*, blz. 9

69. De biometrie is een sterk authenticatiemiddel[34] dat zou moeten voorbehouden worden voor situaties die een dergelijk veiligheidsniveau vergen.

70. Men kan bijvoorbeeld de noodzaak van het veralgemeend gebruik van biometrische systemen in schoolmiddens in twijfel trekken. Enkel wanneer de bijzondere situatie van de instelling een controle op hoog niveau zou rechtvaardigen, zou dat de maatregel als proportioneel kunnen beschouwd worden.

71. Hetzelfde geldt voor het werktijdenbeheer van de medewerkers. Hoewel in dit opzicht de biometrie een bijzonder voordeel oplevert in de strijd tegen de fraude, zouden de verantwoordelijken voor de verwerking een voorafgaande analyse moeten uitvoeren om de aard en het bijzonder belang van de fraude voor de instelling te evalueren ten opzichte van de impact van de overwogen biometrische maatregelen voor de betrokkenen. Er moet natuurlijk ook rekening gehouden worden met het aantal medewerkers van het bedoelde bedrijf vermits een beperkt aantal medewerkers de risico's op fraude op natuurlijke wijze vermindert.

72. De biometrische systemen zouden niet enkel mogen aangewend worden omdat zij handig zijn maar wel omdat zij de enige manier zijn om het oorspronkelijk gestelde doeleinde te bereiken.

73. Hoewel er overigens bij de afweging tussen de belangrijke nood aan een sterke authenticatie en het recht op privacy van de betrokkenen eveneens rekening mag gehouden worden met het economisch voordeel, kan dit voordeel niet alleen het aanwenden van biometrische maatregelen rechtvaardigen.

74. Nadat de verantwoordelijke voor de verwerking de verschillende verwerkingssystemen aan elkaar heeft afgewogen en opteert voor een biometrisch systeem, dient hij in alle geval ook de aanbevelingen in paragrafen 58 tot 66 van dit advies na te leven.

[34] Volgens de definitie van authentificatie: "[...] Strong authentification is either based on strong mecanisms (e.g. biometrics) or makes use of at least two (...) factors (so-called multi-factor authentification)" (ISO/IEC 18028-4: 2005). De bedoelde factoren zijn de authenticatie door de kennis, het bezit of de persoonlijke kenmerken.

- De toepassing van het biometrisch systeem beperken tot de noodzakelijke aanwendingen

75. Indien de verantwoordelijke voor de verwerking meent dat de authenticatie absoluut moet gebeuren via een biometrisch systeem, dient het gebruik hiervan in de eerste plaats beperkt te worden tot de ruimten/diensten die dergelijke bijzondere maatregelen rechtvaardigen. Wat bijvoorbeeld de toegangscontrole betreft, kan een site bepaalde ruimten omvatten die vrij toegankelijk zijn en andere die het gebruik van de biometrie rechtvaardigen (een zaal of een gebouw dat waardevolle voorwerpen bevat, zeer vertrouwelijke informatie die moet beschermd worden, een informaticalokaal waar gevoelige gegevens bewaard worden enz.). De toegang aan de hand van biometrische systemen zou kunnen beperkt worden tot deze ruimten en de verwerkte biometrische gegevens zouden kunnen beperkt blijven tot de personen die gemachtigd zijn om deze ruimten te betreden.

76. Om anderzijds de toegang tot een ruimte te beperken tot een bepaalde groep individuen is het niet steeds noodzakelijk om gegevens te verwerken die een directe identificatie toelaten (zoals de naam) van de personen die beschikken over een recht op toegang. Zolang een persoon dus beschikt over een recht op toegang en de biometrie toelaat dit te controleren is het onnodig de biometrische informatie te koppelen aan bijkomende identificatiemiddelen.

- Als de authenticatie kan gebeuren zonder een identificatie, mag de verwerking van biometrische systemen niet gecombineerd worden met andere identificatiemiddelen

77. Het is soms mogelijk om een authenticatie door te voeren zonder dat de identiteit van de betrokken persoon bij elk gebruik gekend moet zijn. Het is bijvoorbeeld mogelijk dat de toegang tot een plaats voorbehouden is aan een groep individuen. Om te verhinderen dat een derde persoon toegang krijgt, is het niet noodzakelijk om bij iedere toegang de identiteit te kennen van de individuen uit de groep. Zolang een persoon tot de groep behoort en in het bezit is van een biometrisch gegeven van de groep (bijvoorbeeld een chipkaart van de groep die zijn biometrische gegeven bevat), is het niet noodzakelijk om de biometrische informatie te koppelen aan bijkomende identificatiegegevens (zoals de naam of het personeelsnummer van de betrokken persoon). Indien men aan deze persoon de toegang wil ontzeggen, volstaat het om de drager te recupereren die zijn biometrische informatie bevat.

B. Informatieverstrekking aan de betrokkenen

78. Bij elke gegevensverwerking moeten de personen ingelicht worden over de doeleinden van de verwerking, over de identiteit van de verantwoordelijke voor de verwerking en de bestemmelingen (of categorieën bestemmelingen) van de gegevens alsook over het bestaan van een recht op toegang en verbetering[35].

79. Om de transparantie voor de betrokken personen te verzekeren is het eveneens aangewezen om spontaan informatie te verstrekken over het type van biometrisch systeem dat gebruikt wordt (onder andere de manier van opslaan), over het bestaan van een foutenmarge bij de herkenning die inherent is aan elk biometrisch systeem en over de procedure die de betrokken persoon moet volgen wanneer het systeem hem zogezegd niet herkent.

80. Er moet inderdaad over gewaakt worden dat biometrische systemen niet als onfeilbaar worden afgeschilderd. Ze kunnen evenmin beschouwd worden als onfeilbare bewijssystemen. Daarom is het aangewezen om steeds aan de betrokken persoon de mogelijkheid te bieden om met alle rechtsmiddelen het tegendeel te bewijzen.

C. Opslagtermijn van de gegevens

81. De biometrische gegevens en de bijkomende gegevens die het resultaat zijn van de omstandigheden van de inzameling (zie paragraaf 26) zouden niet langer mogen bewaard worden dan noodzakelijk is voor de verwezenlijking van het geplande doeleinde[36].

82. Zo moeten bijvoorbeeld de gegevens die opgeslagen werden op een verwijderbare drager en gebruikt om de toegang tot een arbeidsplaats te beheren, verwijderd worden zodra de gebruiker zijn toegangrecht tot die ruimte verliest.

83. Bovendien zou de biometrische sensor die toelaat het biometrisch gegeven in te zamelen niet langer een kopie van dit gegeven moeten bewaren dan de tijd die nodig is om de vergelijking te maken.

---

[35] Artikel 9 van de WVP

[36] Artikel 4, §1, 5° van de WVP.

D. Veiligheidsmaatregelen

84. De verantwoordelijke voor de verwerking en desgevallend zijn verwerker, moeten de nodige technische en organisatorische veiligheidsmaatregelen[37] treffen om de biometrische en andere persoonsgegevens die zij verwerken te beschermen tegen al dan niet toevallige vernietiging, tegen toevallig verlies, alsook tegen wijziging, toegang en iedere andere ongeoorloofde verwerking van persoonsgegevens.

85. Rekening houdend met de bijzondere aard van biometrische gegevens en de risico's op schending van de beveiliging van die gegevens[38], moet het beveiligingsniveau bijzonder hoog zijn.

86. Het is aangewezen om voor elke fase in de verwerking van biometrische gegevens beveiligingsmaatregelen te voorzien[39].

87. Er moet bijvoorbeeld absoluut worden vermeden dat tijdens de inschrijvingsfase een niet gemachtigde persoon zich laat registreren als gemachtigd. Om deze reden zou de inschrijving van de referentie-informatie (en het aanmaken van de beveiligde verwijderbare drager) moeten plaatsvinden in een vertrouwelijke en beveiligde omgeving. Het aantal personen dat gemachtigd wordt om de referentie-informatie te registreren zou moeten beperkt worden.

88. De drager met de biometrische gegevens zou moeten beveiligd worden teneinde onrechtmatig gebruik te vermijden. Zo zou men kaarten kunnen gebruiken waarvan de inhoud beveiligd wordt door coderingsleutels, door systemen van elektronische handtekening of door een scrambling-functie (bijvoorbeeld hashing)[40].

89. Er zouden eveneens maatregelen moeten genomen worden opdat de sensor die de biometrische gegevens inzamelt niet zou kunnen gekraakt worden.

---

[37] Artikel 16 van de WVP

[38] Voor een beschrijving van de veiligheidsrisico's, zie punt 2.3.2 van het verslag « Identity Management for eGovernment, Study and assessment of Biometric techniques for eGovernment application », *op. cit.*, blz. 8

[39] Zie de suggestie voor verschillende veiligheidsmaatregelen in de « Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données » opgesteld door PRIVATIM, *op. cit*, n°3.2.

[40] Zie het werkdocument over de biometrie van de Groep 29, *op. cit.*, blz. 10 en 11

90. De integriteit en de vertrouwelijkheid van de informatie die uitgewisseld wordt tussen de beveiligde verwijderbare drager en de sensor moet eveneens op passende wijze beveiligd worden.

91. Tenslotte is het onontbeerlijk dat de verantwoordelijke voor de verwerking de technologische evoluties nauwgezet opvolgt teneinde de veiligheidsmaatregelen hierop af te stemmen[41]. Het kiezen voor een oplossing die de veiligheid bevorderdt, zoals een biometrisch systeem, impliceert onvermijdelijk een verantwoordelijkheid inzake opvolging van de technologische evolutie.

92. Overeenkomstig artikel 15 bis van de WVP kan de verantwoordelijke voor de verwerking verantwoordelijk gesteld worden voor de schade die zou te wijten zijn aan de niet-naleving van de veiligheidsmaatregelen.

Voor de Administrateur m.v., De Voorzitter
Het Afdelingshoofd O&RM

(get.) Patrick Van Wouwe (get.) Willem Debeuckelaere

[41] Artikel 16 van de WVP