

Zinvol, betrouwbaar en veilig gebruik van biometrie

230

Trefwoorden:

Biometrie, persoonsherkenning, veiligheid, groot-schalige ICT-toepassing

Aan de hand van het recente *position paper* van het Nederlands Biometrie Forum worden twaalf aandachts- en uitgangspunten voor zinvol en veilig gebruik van biometrie geformuleerd en toegelicht. Biometrie is op den duur onmisbaar in onze informatiesamenleving, maar nieuwe technologie wordt in het begin vaak verkeerd ingezet. Groot-schalige stelsels blijken in de praktijk nauwelijks beheersbaar. Dat betekent dat de eerste grote toepassingen nare maatschappelijke risico's kunnen opleveren, waarvoor ook geen goede oplossingen beschikbaar zijn. Dit klemmt temeer omdat onveranderlijke biometrische gegevens in die toepassingen de hoofdrol spelen. Aangegeven wordt dat overbezorgdheid over privacy deze maatschappelijke risico's onbedoeld extra vergroot. Verduidelijkt wordt dat het beoordelingscriterium veiligheid wel privacybescherming impliceert, maar dat dit andersom niet het geval hoeft te zijn.

In dit artikel bouwt de auteur voort op zijn eerdere artikelen in *P&I* over biometrie, persoonsnummers en identiteitsvraagstukken.² Hij heeft het op persoonlijke titel geschreven.

1. Nederlands Biometrie Forum

Het Nederlands Biometrie Forum (NBF) is een stichting die staat voor zinvol en veilig gebruik van biometrie. Daarbij gaat de aandacht uit naar zowel het brede publiek als naar de verschillende groepen professionals. Het NBF richt zich op bewustwording van wat biometrie wel en niet kan en op beter begrip van kansen en risico's. Uiteindelijk is maatschappelijke acceptatie van deze technologie wenselijk. Daarvoor is vertrouwen nodig. Het NBF is de overtuiging toegedaan dat dit vertrouwen niet kan worden afgedwongen maar moet worden verdiend. De afgelopen twee jaar hebben binnen het NBF vele tientallen professionals uit overheid, bedrijfsleven en wetenschap gewerkt aan de formulering van uitgangspunten voor zinvol en veilig gebruik van biometrie in een zogenaamd *position paper*. Dit document wordt periodiek bijgesteld op basis van nieuwe ervaringen en inzichten. De

nieuwste versie staat in het Nederlands en in het Engels op de website van het NBF (zie <www.biometrieforum.nl>).

2. Biometrie

Met de term 'biometrie' wordt bedoeld op het herkennen van mensen aan een lichaamskenmerk met gebruikmaking van informatietechnologie. Als iemand visueel gecontroleerd wordt met een pasfoto of een signalement, spreken we niet van biometrie. Dit verandert als deze controle geautomatiseerd plaatsvindt. Informatietechnologie maakt het tegenwoordig mogelijk lichaamskenmerken snel te digitaliseren om ze vervolgens óf te kunnen afbeelden, óf om er berekeningen op los te laten. Dat kan bijvoorbeeld met de omtrek van de hand of een vinger, de afdruk van een vinger of met het patroon van de iris. Zelfs veranderlijke lichaamskenmerken zijn voor biometrische persoonsherkenning bruikbaar, zoals de stem, de schrijfbeweging wanneer men zijn handtekening zet, of het ritme waarin men bepaalde woorden typt op een toetsenbord. Bij een biometrische persoonsherkenning vergelijkt men een eerder gemeten lichaamskenmerk met het resultaat van een nieuwe meting op de plaats en het moment van de controle. Het resultaat van de eerdere meting kan vastgelegd zijn in een informatiesysteem van de controlerende instantie, of op een chipkaart of ander elektronisch document in bezit van de te controleren persoon. De technologie nodig voor biometrische persoonsherkenning is voor veel mensen moeilijk te doorgronden, omdat ze gebaseerd is op kansberekening en dus automatisch leidt tot een aantal onterechte herkenningen en onterechte afwijzingen (hoeveel hangt af van de door de exploitant zelf in te stellen tolerantiegrenzen). Zo legt biometrie dus ook foute koppelingen tussen personen en documenten of gegevens. Biometrische persoonsherkenning biedt daarom nooit de volstrekte zekerheid (100%) dat iemand de juiste persoon is. Belangrijker dan de beperkingen van biometrie bij de koppeling tussen personen en hun documenten of gegevens is het feit dat biometrie niets kan zeggen over de juistheid van deze documenten en gegevens noch over de juistheid van de koppeling zelf. Daarom kan biometrie – in tegenstelling tot wat veel mensen denken – geen uitsluitel geven over *wie* iemand is. Biometrie betreft dus alleen *persoonsherkenning*, *geen identiteitsvaststelling*!

1 Jan Grijpink is als raadadviseur werkzaam op het Ministerie van Justitie (informatiestrategie) en als bijzonder hoogleraar informatiekunde (Keteninformatisering) aan de Universiteit Utrecht. Hij is voorzitter Nederlands Biometrie Forum.
2 J.H.A.M. Grijpink, 'Biometrie en privacy', *P&I* 2000, p. 244-250; 'Persoonsnummers en privacy', *P&I* 2002, p. 52-56 en nr. 3, p. 100-

105; 'Identiteitsfraude als uitdaging voor de rechtstaat', *P&I* 2003, p. 148-153; 'Onze informatiesamenleving in wording, de uitdaging van groot-schalige informatie-uitwisseling in de rechtstaat', *P&I* 2005, p. 98-104; 'Een beoordelingsmodel voor de inzet van biometrie', *P&I* 2006, p. 14-17; 'Biometrie, veiligheid en privacy', *P&I* 2008, p. 10-14.

3. Toekomstperspectief voor biometrie

In een anonieme informatiesamenleving met een toenevende wereldwijde mobiliteit wordt het belang van geautomatiseerde persoonsherkenning steeds groter. Tegenover administratieve herkenningmethoden zoals pincode, wachtwoord of sleutel, is namelijk alleen biometrie gebaseerd op een persoonsgebonden lichaamskenmerk als herkenningpunt. Op den duur zal biometrie daarom onmisbaar worden, zeker voor gevoelige werkprocessen binnen overheid en bedrijfsleven. Biometrie is vooral nuttig wanneer het belangrijk is zeker te weten dat de persoon met wie men van doen heeft, de juiste persoon is, of wanneer iemand wil voorkomen dat zijn identiteit door iemand anders wordt gestolen en misbruikt. Dat stelt steeds andere eisen aan geautomatiseerde persoonsherkenning, afhankelijk van de risico's in een bepaalde context.

Twee voorbeelden

1. Een zwembad wilde met vingerafdrukcontrole een bepaalde groep jongens weren die bij herhaling meisjes lastig vielen. Prima doel, maar nu de uitwerking. Elke bezoeker/bezoekster diende zijn/haar vingerafdruk te laten registreren in het computersysteem van het zwembad. Fout dus, want als je de vingerafdrukken kent van de jongens die je wilt weren, kun je volstaan met controleren van de vingerafdruk van mannelijke bezoekers die tot de relevante leeftijdsgroep behoren. Komt iemands vingerafdruk voor op de (zwarte) lijst, dan kan hij rechtsomkeert maken. Het opslaan van vingerafdrukken is dus helemaal niet nodig. Vingerafdrukken van meisjes controleren en opslaan is helemaal onzin. Het verhaal wordt nog gekker. Een dame van 82 jaar weigerde mee te werken aan vingerafdrukcontrole en haar werd vervolgens om die reden de toegang tot het zwembad ontzegd.
Het standpunt van het NBF is: biometrie moet noodzakelijk zijn en het doel beslist over zin en onzin van de wijze waarop biometrie moet worden ingezet.
2. Een autoverhuurder ondervond veel problemen bij het terugbrengen van de auto's. Veel huurauto's werden niet of op de verkeerde plaats teruggebracht. Biometrie leek een oplossing, maar het mocht niet veel kosten. Een creatieve medewerker bedacht een oplossing zonder dure elektronica: met gel de vingerafdruk op het papieren huurcontract, onder garantie dat men bij terugbrengen van de auto het papier met de vingerafdrukken terug zou krijgen. De eerste vier maanden leverden een doorslaand succes: geen gestolen of verkeerd teruggebrachte auto's! Mooi dus. Toch blijven opletten! Enkele maanden later bleken overal in de administratie toch kopieën van huurcontracten met vingerafdrukken rond te slingeren zonder dat dit ergens voor nodig was!
Daarom vraagt het NBF aandacht voor een biometrietoe-passing als geheel, waarbij zowel de ontwikkeling van de toepassing in de loop van de tijd van belang is als praktische details zoals de administratie.

Uit deze voorbeelden blijkt hoe gemakkelijk biometrie verkeerd wordt ingezet. Daar windt het NBF zich over op, omdat biometrie op den duur onmisbaar is. Onzinnige toepassing van deze technologie roept onnodige weerstand op bij het publiek en ondermijnt de maatschappelijke acceptatie. Beide voorbeelden onderstrepen ook het belang van voorlichting aan publiek en organisaties die biometrie willen gebruiken. We moeten zuinig zijn met onze biometrische gegevens, zeker met die welke afgeleid zijn van onveranderlijke biometrische kenmerken zoals een vingerafdruk. Eenmaal gecompromitteerd, heb je daar heel lang last van zonder dat je je kunt verweren door dat biometrische kenmerk te veranderen.

4. Niveauvergissing

In de informatiekunde, zoals ook in andere sociale wetenschappen, ontlenen we inzichten vaak aan kleinschalige toepassingen, bijvoorbeeld op het niveau van een persoon of een organisatie. Die inzichten vertalen we doorgaans meestal klakkeloos naar grootschaliger toepassingen, bijvoorbeeld op het niveau van een keten of een maatschappelijke sector. We maken dan meestal ongemerkt een niveauvergissing (een zogenaamde *'fallacy of the wrong level'*), want inzichten zijn gebonden aan het niveau waarop ze zijn opgedaan en zijn op andere niveaus (hoger of lager) vaak niet geldig! Dat heeft tot gevolg dat allerlei veronderstellingen en uitgangspunten van grootschalige stelsels onjuist zijn waardoor deze meer tekortkomingen en risico's hebben dan men denkt of verwacht.

Twee voorbeelden: het biometrische paspoort en het biometrische visum

1. Het eerste voorbeeld betreft het nieuwe biometrische paspoort. Dat is gebaseerd op het inzicht dat men iemand trefzeker kan herkennen aan zijn vingerafdruk. Dit in beginsel kleinschalige inzicht mag men niet zomaar doortrekken naar de nationale of internationale schaal van grensbewaking. Anders is het onzeker of het biometrische paspoort oplevert wat men ervan verwacht. Grootschalige stelsels werken in de praktijk immers anders dan kleinschalige. Maatschappelijke ketens hebben geen overkoepelend gezag en ketenprocessen zijn moeilijk beheersbaar en nauwelijks voorspelbaar. Het gaat om enorme aantallen betrokkenen (burgers, reizigers, patiënten) en samenwerkende autonome organisaties en professionals.
Biometrie werkt op dat grootschalige niveau (keten, sector, land) anders dan je denkt, soms ook averechts. Door nabootsen of namaken van de vingerafdruk die op het paspoort staat kan iemand anders ongemerkt door de controle komen zonder dat naderhand kan worden nagegaan wie dat gedaan heeft. Opschalen zonder nader onderzoek naar de risico's van de grootschalige situatie is dus eigenlijk riskant. En zelfs dan verdient het aanbeveling om ook in de opschaling een geleidelijke weg te kiezen, bijvoorbeeld eerst vingerafdrukcontrole bij aanvraag en uitgifte zonder vingerafdrukken op het paspoort,

vervolgens voor bepaalde doelgroepen op vrijwillige basis ook de vingerafdrukken op het paspoort, bijvoorbeeld voor wie naar de VS wil reizen.

2. Het biometrische visum, het tweede voorbeeld, is al eerder ingevoerd om vreemdelingen die in Nederland ongewenst zijn, te kunnen weren voordat ze daadwerkelijk naar Nederland komen. Op de Nederlandse ambassade in het land van herkomst worden daarom bij een visumaanvraag de vingerafdrukken van de reiziger vastgelegd en naar Nederland gestuurd. Als die vingerafdrukken vóórkomen in de databank met vingerafdrukken van ongewenste vreemdelingen, wordt het visum geweigerd.

Biometrie werkt op dat grootschalige niveau soms ook averechts. Stel dat een crimineel netwerk iemand naar Nederland wil sturen voor een gespecialiseerde klus. Door het weigeren van het visum weet het netwerk nu, dat ze óf iemand anders moeten sturen óf een route moeten kiezen waarbij de controle minder goed georganiseerd is. Dat betekent dat in plaats van de verwachte grotere greep op het binnenkomende reizigersverkeer, dit reizigersverkeer nu ongemerkt onzichtbaar is geworden en wel met betrekking tot de doelgroep waar het juist om te doen is!

Merk op dat om technische redenen geen vingerafdrukken op het visum kunnen worden vermeld, zoals we dat op het paspoort nu wel doen. Visumaanvragers controleren we dus alleen met de vingerafdrukken in de databank. Met deze varianten kunnen we in de toekomst bij onverwachte veiligheidsproblemen uitproberen welk van de twee biometrische stelsels het meest flexibel is. Zo'n experiment vooraf zou natuurlijk nuttiger zijn geweest, want eenmaal ingevoerd kun je dit type grootschalige stelsels nauwelijks meer veranderen.

5. Identiteitsfraude als toetssteen voor een biometrische applicatie

Met identiteitsfraude bedoelen we dat iemand met kwade bedoelingen bewust de schijn oproept van een identiteit die niet bij hem hoort, daarbij gebruikmakend van de identiteit van iemand anders of van een niet-bestaande persoon. Een identiteitsfraudeur heeft daarvoor geen document of identiteitsbewijs nodig, hij kan ook een persoonsnummer, foto, gebeurtenis of een biometrisch gegeven gebruiken, omdat ze allemaal een suggestie bevatten waaruit mensen afleiden wie ze tegenover zich hebben. Identiteitsfraude blijkt gemakkelijk en zonder veel risico. Lukt de identiteitsfraude, dan heeft men het niet in de gaten terwijl het voordeel langdurig en aanzienlijk kan zijn. Loopt men tegen de lamp, dan heeft men (nog) niets misdaan! Officiële hulpmiddelen voor persoonsherkenning, zoals identiteitsbewijs, burgerservicenummer of een biometrisch gegeven op het paspoort, zijn voor identiteitsfraudeurs extra waardevol omdat ze overal gebruikt moeten en kunnen worden. Daar komt nog bij dat officiële persoonscontroleprocedures bekend, uniform en voorspelbaar zijn. Uitzonderingsprocedures voor situaties waarin de normale procedure niet kan worden gevolgd ('Ik ben mijn paspoort vergeten...' of uitval van apparatuur), zijn meestal

slordig en improviserend van aard. Ten slotte gebruiken we bij deze controles nauwelijks andere controlegegevens dan die welke de gecontroleerde bij zich heeft. Zodoende is de pakkans gering.

Hiertegenover staat de zwakke positie van het slachtoffer. In een digitaliserende wereld laat identiteitsfraude wel steeds meer (technische) sporen na, maar deze wijzen niet naar de dader, maar juist naar het slachtoffer, dat vervolgens moet bewijzen dat hij iets *niet* heeft gedaan. Voor een veilig gebruik van biometrie moet de voorspelbaarheid van identiteitscontroles daarom sterk worden verminderd en de kwaliteit van uitzonderingsprocedures fors worden verhoogd. Sterker nog, biometrie zou daarbij moeten helpen.

We moeten dus nagaan of met een biometrische persoonsherkenning identiteitsfraude kan worden voorkomen in plaats van juist gemakkelijker gemaakt. Het gaat om een specifiek aspect van de veiligheid van een biometrische applicatie, dat bijvoorbeeld kan worden belicht met de volgende vragen. Kan iemand door nabootsen van het biometrische gegeven van iemand anders met succes door de identiteitscontrole komen en zodoende voor de rechtmatige houder worden aangezien? Hoe zou men de meting zelf kunnen beïnvloeden met hetzelfde resultaat? Kan men door het resultaat van de controle informatie verkrijgen waarop met kwade bedoelingen kan worden ingespeeld (zie het voorbeeld van het biometrische visum)? Zo fungeert het fenomeen identiteitsfraude als toetssteen voor *veilige* biometrie. Bij het beoordelen van de veiligheid gaat het steeds om het geheel van de biometrische toepassing, dus met inbegrip van techniek, organisatie, procedures en niet in de laatste plaats de mate waarin mensen meewerken of juist belang hebben bij fouten of misbruik.

Zo ziet ook het NBF identiteitsfraudebestrijding als toetssteen voor een veilige biometrietoeëpassing. Het standpunt van het NBF is bijvoorbeeld dat als biometrie identiteitsfraude moeilijker moet maken, het bijvoorbeeld nodig is om *gelijktijdig* gebruik te maken van meerdere biometrische gegevens of technieken, in combinatie met andere gegevens of hulpmiddelen, omdat een identiteitsfraudeur deze niet allemaal tegelijk met succes naar zijn hand kan zetten.

6. Privacy en veiligheid

De sporen die identiteitsfraude achterlaat leiden naar het slachtoffer, niet naar de dader. Identiteitsfraude maakt op deze wijze een ernstige inbreuk op de privacy van het slachtoffer. Dit geldt speciaal voor identiteitsfraude met een onveranderlijk biometrisch gegeven, omdat deze vorm van identiteitsfraude iemand lang kan blijven achtervolgen zonder dat men er veel tegen kan doen. Officiële instanties blijken het slachtoffer in eerste instantie voor de dader te houden, omdat alle sporen in zijn richting wijzen. Dan moet men vervolgens vaak bewijzen dat men niet de dader is. Dat lukt meestal niet, waardoor er ten onrechte een verdacht luchtje aan het slachtoffer blijft hangen. Bij biometrie blijkt privacy zodoende nauw samen te hangen met veiligheid en reputatie, afhankelijk van de aard van het misbruik. Rond biometrie zal de discussie over *privacy* daarom niet snel verminderen, maar

deze discussie zal wel abstract blijven als men de relatie met iemands *veiligheid* niet uitdrukkelijk legt. De in privacydiscussies veelgehoorde stelling 'van mij mogen ze alles weten, want ik heb niets te verbergen' wordt verkondigd door mensen die nog niet zijn geconfronteerd met een onterechte beschuldiging. Als die mede gebaseerd is op een misbruikt onveranderlijk biometrisch gegeven, lijkt verweer bij voorbaat weinig kansrijk. Dit is geen denkbeeldig risico. Biometrietoe toepassingen zijn op dit moment bijna allemaal onveilig, zeker in geval van grootschalig gebruik van een onveranderlijk biometrisch gegeven. Wie zich zorgen maakt over privacy kan zich daarom in de visie van het NBF in deze fase beter richten op de veiligheid van grootschalig gebruik van biometrische persoonsgegevens, rekening houdend met de toepassing als geheel en met doelgroepen met andere belangen. Dat begrip 'veiligheid' gaat veel verder dan de gebruikelijke privacydiscussies over de *beveiliging* van deze gevoelige persoonsgegevens.

Met het oog op grootschalige veiligheid bevat het *position paper* van het NBF diverse concrete vereisten waaraan in de nabije toekomst voldaan moet worden. Deze kunnen nu al helpen bij het beoordelen van de maatschappelijke toelaatbaarheid van een specifieke biometrische toepassing.

Voorbeeld

Het biometrische paspoort biedt een interessant voorbeeld. De privacydiscussie in Duitsland heeft ertoe geleid dat er twee vingerafdrukken op de Duitse paspoorten worden vermeld zonder dat de overheid op enigerlei wijze hiervan een kopie bewaart. Dat betekent dat alleen de vingerafdrukken van de gecontroleerde kunnen worden vergeleken met de vingerafdrukken op het paspoort. In kleinschalig denken lijkt dat best aardig, maar dat is bij grootschalig gebruik beslist onvoldoende. Dan wreekt zich dat de Duitse overheid na de uitgifte niet meer kan controleren of de vingerafdrukken op het paspoort nog de originele vingerafdrukken zijn en evenmin, of de gecontroleerde persoon echt dezelfde is als de officiële houder van het paspoort. Daarvoor heb je de vingerafdruk van een andere vinger nodig, omdat die op het paspoort nagebootst of nagemaakt kunnen zijn. Om die reden heeft Nederland ervoor gekozen om de afdruk van vier vingers in een decentrale gemeentelijke databank op te slaan, de twee vingerafdrukken die op het paspoort staan en twee andere. De eerste twee maken het steeds mogelijk de integriteit van het paspoort te controleren, de andere twee om steeds rechtstreeks, dus buiten het paspoort om, na te kunnen gaan of het echt wel om de officiële houder van het paspoort gaat. Met deze decentrale databanken kan in beginsel identiteitsfraude worden ontdekt en voorkómen, mits goed ingezet. De privacydiscussie richt zich nu juist tegen deze achterliggende databanken en dreigt daarmee de veiligheid van deze grootschalige biometrietoe toepassing teniet te doen. Zo kan de overbezorgdheid voor privacy de maatschappelijke risico's van grootschalige biometrietoe toepassingen onbedoeld enorm vergroten. Voor wie privacy een belangrijk aandachtspunt is, moge duidelijk zijn geworden dat het beoor-

delingscriterium veiligheid privacybescherming impliceert, maar dat dit andersom niet het geval hoeft te zijn.

7. Twaalf aandachts- en uitgangspunten voor zinnol en veilig gebruik van biometrie³

1. Biometrie is gebaseerd op kansberekening en leidt dus automatisch tot een aantal onterechte herkenningen en onterechte afwijzingen (hoeveel hangt af van de door een exploitant zelf in te stellen tolerantiegrenzen). Biometrische kenmerken en daarvan afgeleide biometrische gegevens kunnen bovendien ook nagebootst en nageemaakt worden.
2. Biometrie kan wel een persoon koppelen aan een document of gegeven, maar die biometrie zegt niets over de juistheid van dat document of gegeven, of over de juistheid van die koppeling. Biometrie kan dus alleen personen herkennen, maar geen identiteiten vaststellen.
3. Een grootschalige toepassing van biometrie is door niet-beheersbare organisatorische en menselijke factoren alleen met veel extra inspanningen voldoende veilig te maken. In de praktijk blijkt dat nog niet te realiseren. Bij het beoordelen van de veiligheid van een biometrische toepassing gaat het steeds om het geheel van de toepassing, dus met inbegrip van techniek, organisatie, procedures en de mate waarin mensen meewerken of juist belang hebben bij fouten of misbruik.
4. Biometrie wint snel aan betrouwbaarheid en veiligheid als het biometrische gegeven gebruikt wordt in combinatie met een ander biometrisch gegeven (vingerafdruk + irispatroon) en niet-biometrisch gegeven, bijvoorbeeld een pincode (het principe van 'ten minste driemaal kloppen'). Gebruik van een *los* biometrisch gegeven is daarom maatschappelijk niet verantwoord.
5. Toepassing van biometrie moet echt nodig zijn voor het beoogde doel en niet door andere, lichtere maatregelen kunnen worden vervangen. Daarom moeten triviale toepassingen van biometrie actief ontmoedigd worden.
6. Biometrische gegevens in een toepassing dienen zo beheerd te worden, dat het onmogelijk is deze daarbuiten niet zijn te (her)gebruiken.
7. Aan het biometrische gegeven moet men kunnen zien binnen welke toepassing het is ontstaan.
8. Als men wordt onderworpen aan een biometrische persoonsherkenning, heeft men er recht op dat aan een aantal eisen is voldaan. Het NBF hanteert een checklist met zeven eisen die kan worden gebruikt als toets voor maatschappelijk verantwoorde inzet van biometrie.
9. De overheid moet zorgen voor extra beleid en wetgeving met het oog op misbruik van biometrische gegevens en daarop gebaseerde identiteiten.
10. Biometrische gegevens mogen uitsluitend vervormd en versleuteld worden opgeslagen. Opslag van biometrische gegevens is bovendien alleen toegestaan wanneer dit voor de desbetreffende toepassing onvermijdelijk is en

³ De integrale tekst van het NBF *position paper* is opgenomen als bijlage bij dit artikel.

hergebruik van die biometrische gegevens buiten deze toepassing praktisch onmogelijk is.

11. Koppeling van een bestand met biometrische gegevens aan externe bestanden moet uitsluitend zijn toegestaan in door de wet geregelde situaties. Daarnaast zouden biometrische gegevens in beginsel alleen gescheiden van biografische persoonsgegevens mogen worden opgeslagen.
12. Voor persoonsregistraties met biometrische gegevens moet een verplichte registratie worden ingevoerd bij een centraal landelijk orgaan, waar ook misbruik van biometrisch verankerde identiteiten kan worden gemeld. Dit centrale orgaan dient alert te zijn op onnodige of onveilige opslag van biometrische gegevens en te controleren of door de exploitant voldoende preventieve maatregelen zijn genomen tegen diefstal en misbruik van de door hem beheerde biometrische gegevens.

In deze fase van introductie van biometrietoepassing gaat het vooral om het voorkomen van kinderziekten en het opdoen van ervaring met het gebruik van biometrische gegevens op kleinere schaal. Bij het opschalen van biometrietoepassingen moet meer aandacht zijn voor op dat grootschaliger niveau ongeldige aannames en uitgangspunten. Risicoanalyses moeten zicht geven op de veiligheidsproblemen op die grotere schaal. Risicobeheersing moet een essentieel onderdeel vormen van goed beheer van biometrische gegevens. Bij het beoordelen van veiligheid en betrouwbaarheid gaat het wel steeds om het geheel van een toepassing, met inbegrip van techniek, organisatie, procedures en niet in de laatste plaats de mate waarin mensen meewerken of juist belang hebben bij fouten of misbruik.

Bijlage

Nederlands Biometrie Forum (NBF)⁴

Betrouwbaar en veilig gebruik van biometrie

Preambule

In de moderne samenleving wordt het steeds belangrijker dat iemand trefzeker kan worden herkend, om onze informatiesamenleving veiliger te maken. Ook voor de persoon zelf, bijvoorbeeld om te voorkomen dat iemand anders met zijn identiteit of bezit aan de haal gaat. Omdat biometrische gegevens het mogelijk maken iemand aan een uniek fysiek kenmerk te herkennen, zal biometrie in de toekomst onmisbaar zijn en toegepast worden in allerlei verschillende processen en omgevingen.

Maar biometrie is geen wondermiddel, het kan fouten maken, worden nagebootst en misbruikt. Biometrie heeft nog een andere inherente beperking. Biometrie kan wel een persoon koppelen aan een document of gegeven, maar die biometrie kan niets over de juistheid van dat document of gegeven of over de juistheid van die koppeling zeggen. Dus biometrie kan alleen personen herkennen, geen identiteiten vaststellen. Iemands identiteit vaststellen impliceert immers

een uitspraak over de juistheid van het aan een persoon gekoppelde document of gegeven én over de juistheid van de biometrische koppeling zelf. Dat kan biometrie niet. Niettemin is biometrie een belangrijk extra hulpmiddel, mits gebruikt in combinatie met andere gegevens en instrumenten.

Nieuwe technologie gaat onvermijdelijk gepaard met kinderziekten, die juist in de beginfase identiteitsmisbruik door iemand anders extra gemakkelijk maken. Het zou te betreuren zijn, als het vertrouwen in biometrie in de beginfase onnodig op de proef wordt gesteld door onverstandige en riskante toepassingen.

Met het oog op deze beperkingen en risico's formuleert het NBF in dit document vanuit haar maatschappelijke verantwoordelijkheid haar visie op betrouwbaar en veilig gebruik van biometrie in de vorm van aanbevelingen. Uiteindelijk is een brede maatschappelijke acceptatie van biometrische technieken noodzakelijk. Het NBF zal daartoe naar vermogen bijdragen, o.a. door onderzoek naar de maatschappelijke acceptatie van biometrie.

Begrippen

Onder *biometrie* verstaat het NBF het herkennen van mensen aan een lichaamskenmerk met gebruikmaking van informatietechnologie. Informatietechnologie maakt het mogelijk lichaamskenmerken snel te digitaliseren om ze vervolgens te vergelijken met eerder opgeslagen gegevens. Naast technische en organisatorische aspecten spelen bij toepassing van deze technologie ook de veiligheid van de gebruiker en de bescherming van diens persoonlijke levenssfeer een grote rol.

Degene die met zijn of haar biometrie wordt gecontroleerd, kan verschillende rollen hebben. Tegenover de overheid wordt hij/zij in dit document aangeduid met de term '*burger*', die daarbij verschillende posities kan hebben: onderdaan (belasting betalen), vrije burger (kiezen en gekozen worden, recht van vereniging) of klant van de overheid (vergunningen, paspoorten). Ook een combinatie is denkbaar.

Private organisaties, instellingen, bedrijven en overheidsinstanties kunnen voor een betrouwbare en veilige dienstverlening biometrie toepassen en in bijzondere situaties zelfs eisen om burgers en klanten en medewerkers trefzeker te herkennen. Deze organisaties worden in dit document aangeduid met de term '*exploitant*' van een biometrisch stelsel. De exploitant is te beschouwen als de verantwoordelijke in de zin van de Wet bescherming persoonsgegevens. Onder zijn gezag functioneren systeembeheerders en uitvoerders.

Sommige bedrijven zijn *fabrikant* of *leverancier* van biometrische producten. Op hen rust de verantwoordelijkheid voor de technische en functionele kwaliteit van biometrische apparatuur, met inbegrip van een effectieve beveiliging ervan. De veiligheid en de betrouwbaarheid van de toepassing zijn voor het overige in handen van de exploitant.

Ten slotte kan de overheid nog worden aangeduid als *wetgever*, om vanuit die rol de regelgeving tot stand te brengen die voor iedereen gelijke randvoorwaarden en voorzie-

4 <www.biometrieforum.nl>

ningen garandeert voor veilig en betrouwbaar biometriegebruik.

Toepassingen van biometrie in Nederland

Er komen steeds meer kleinschalige en grootschalige toepassingen van biometrie, waarbij nu eens het accent valt op gemak en dienstverlening, dan weer op beveiliging, bescherming of rechtshandhaving. We onderscheiden daarbij vier toepassingsgebieden van biometrie:

1. de overheid (o.a. identiteitsmanagement, grensbewaking);
2. het bedrijfsleven (o.a. grootschalige toegangsbeveiliging, logistieke processen, betalingsverkeer);
3. private organisaties en instellingen (o.a. zwembaden, disco's, musea, verenigingen);
4. privé-toepassingen (o.a. toegang pc/laptop, beveiliging van auto's en huizen).

Op elk van deze gebieden zijn al tal van toepassingen van biometrie beschikbaar.

Wat kan biometrie oplossen en wat niet?

De technologie nodig voor biometrische persoonsherkenning is voor veel mensen moeilijk te doorgronden, omdat ze gebaseerd is op kansberekening en dus automatisch leidt tot een aantal onterechte herkenningen en onterechte afwijzingen (hoeveel hangt af van de door de exploitant zelf in te stellen tolerantiegrenzen). Naast deze inherente kans op foute koppelingen tussen personen en documenten of gegevens kan biometrie geen uitspraak doen over juistheid van deze documenten en gegevens, noch over de juistheid van de koppeling zelf. Daarom kan biometrie – in tegenstelling tot wat veel mensen denken – geen uitsluitel geven over wie iemand is, alleen over de waarschijnlijkheid dat iemand de persoon is die hoort bij het eerder vastgelegde biometrische gegeven.

Ook de toepassingen zelf bevatten risico's, die echter met passende maatregelen in concrete situaties kunnen worden ingeperkt. Door nauwelijks beheersbare organisatorische en menselijke factoren is toepassing van biometrie op grote schaal alleen met veel extra inspanningen zo te organiseren, dat een toepassing voldoende veilig is voor het beoogde doel. Een 100% waterdichte herkenning van mensen zal biometrie dus niet opleveren, zeker niet als alleen een losstaand biometrisch gegeven wordt gebruikt. Biometrie wint snel aan betrouwbaarheid en veiligheid als het biometrische gegeven gebruikt wordt in combinatie met een ander biometrisch gegeven (vingerafdruk + irispatroon) en niet-biometrisch gegeven, bijvoorbeeld een pincode. Daarmee wordt de kans op bewuste misleiding (zogenaamde *spoofing*) aanzienlijk gereduceerd. Bij het beoordelen van veiligheid en betrouwbaarheid gaat het wel steeds om het geheel van een toepassing, met inbegrip van techniek, organisatie, procedures en niet in de laatste plaats om de mate waarin mensen meewerken of juist belang hebben bij fouten of misbruik.

Wanneer is biometrie zinvol en gerechtvaardigd?

- Biometrie kan alleen personen herkennen, geen identiteiten vaststellen. Biometrie is vooral nuttig wanneer het

belangrijk is zeker te weten dat de persoon met wie men van doen heeft, de juiste persoon is of wil voorkomen dat iemand zijn identiteit misbruikt.

- Toepassing van biometrie moet, gegeven het in deze omgeving vereiste beveiligingsniveau, echt nodig zijn voor het beoogde doel en niet door andere, lichtere maatregelen kunnen worden vervangen. Daarom moeten triviale toepassingen van biometrie actief ontmoedigd worden.
- Biometrie is alleen gerechtvaardigd als de toepassing transparant is en als verspreiding en gebruik van iemands biometrisch gegeven buiten die toepassing niet mogelijk is.
- Biometrische gegevens dienen altijd veilig beheerd te worden, op zo'n wijze dat:
 - a. hergebruik van biometrische gegevens onmogelijk is buiten de toepassing waarbinnen het beheerd wordt;
 - b. aan het biometrische gegeven kan worden gezien binnen welke toepassing het is ontstaan en wordt beheerd.

Het NBF streeft naar een goed begrip van de betekenis, voordelen en beperkingen van de biometrische technologie bij alle betrokkenen en wil actief de ontwikkeling bevorderen van technieken die voorkomen dat een biometrisch gegeven weglekt naar andere toepassingen dan die waarin het is ontstaan, en van technieken die het mogelijk maken de herkomst van een biometrisch gegeven te traceren als dat onverhoopt toch buiten de oorspronkelijke applicatie terecht komt.

Welke rechten moet iemand hebben bij biometrische toepassingen?

Iemand heeft recht op:

- een heldere doelbinding, waarbij duidelijk onderscheid wordt gemaakt tussen wat men vrijwillig en wat men verplicht moet doen of nalaten;
- een eenvoudige en eenduidige bezwaar- en klachtenprocedure, bijvoorbeeld voor wanneer men ten onrechte niet wordt herkend, of voor wie vanwege een lichamelijke beperking de biometrische identiteitscontrole niet zinvol is, gegeven de specifieke doelstelling van die toepassing;
- een – gegeven het risico ten minste gelijkwaardige – *fall back* procedure voor wanneer men niet mee kan doen, of de techniek niet goed functioneert;
- een adequaat pakket van preventieve maatregelen waarmee diefstal of misbruik van iemands biometrie of van de eraan gerelateerde identiteit wordt voorkomen;
- actieve ondersteuning vanuit de exploitant van een biometrisch stelsel, gericht op schadevergoeding en eerherstel bij diefstal of misbruik van iemands biometrie of van de eraan gerelateerde identiteit;
- mededelingen door de beheerder van de toepassing aan betrokkene wie zijn of haar biometrische gegevens heeft geraadpleegd;
- duidelijke maatregelen tegen een persoon die biometrische gegevens die niet van hem of haar zijn, probeert te

misbruiken of daarin is geslaagd (los van strafrechtelijke stappen).

Welke maatregelen moet de overheid nemen ten aanzien van het toepassen van biometrie?

De overheid moet het wettelijke kader aanvullen met het oog op misbruik van biometrische gegevens en identiteiten.

Voorts zijn de volgende punten van belang:

- Voor persoonsregistraties met biometrische gegevens moet een verplichte registratie worden ingevoerd bij een centraal landelijk orgaan, waar ook misbruik van biometrisch verankerde identiteiten kan worden gemeld en correctie van fouten kan worden gevraagd. Dit centrale orgaan dient actief te waken tegen onnodige of onveilige opslag van biometrische gegevens en te controleren of door de exploitant voldoende preventieve maatregelen zijn genomen tegen diefstal en misbruik van de door hem beheerde biometrische gegevens.
- Kritische en maatschappelijk gevoelige toepassingen moeten worden gecertificeerd en de daarvoor benodigde normen moeten worden ontwikkeld als ze nog niet beschikbaar zijn. Voor andere toepassingen moet het gebruik van gecertificeerde biometrische producten worden bevorderd evenals ontwikkeling van de daarvoor benodigde normen als ze nog niet beschikbaar zijn.
- Voor elke toepassing van biometrie moet worden aangegeven wat de grenzen van het gebruik van de desbetreffende biometrische gegevens zijn.
- Opslag van biometrische gegevens is alleen toegestaan wanneer dit voor de desbetreffende toepassing onvermijdelijk is en hergebruik van die biometrische gegevens buiten deze toepassing onmogelijk is. Biometrische gegevens mogen uitsluitend vervormd en versleuteld worden opgeslagen met inbegrip van een op de desbetreffende toepassing herleidbaar technisch merkteken.
- Overheid, bedrijfsleven en andere private organisaties dienen biometrie steeds te gebruiken in combinatie met andere biometrische of niet-biometrische gegevens, bijvoorbeeld in combinatie met een ander biometrisch gegeven en een pincode, om de kans op bewuste misleiding (zogenaamde *spoofing*) aanzienlijk te reduceren. Het principe van 'ten minste driemaal kloppen'. Gebruik van een *los* biometrisch gegeven is daarom maatschappelijk niet verantwoord.
- Koppeling van een bestand met biometrische gegevens aan externe bestanden moet uitsluitend toegestaan zijn in door de wet geregelde situaties. Daarnaast zouden, ook in interne databanken, biometrische gegevens in beginsel gescheiden van biografische persoonsgegevens moeten worden opgeslagen, om voor het eigen personeel de mogelijkheid tot oneigenlijk gebruik en misbruik sterk te beperken.

De actuele versie van het *position paper* kan men downloaden van de website van het NBF: <www.biometrieforum.nl>