Biometrie

Prins, J.E.J.

Published in:
Beveiliging

Publication date:
2001

Prins, J.E.J. (2001). Biometrie: een instrument bij privacybescherming. Verschenen in: *Beveiliging*, *14*(juni), 50-55

Biometrie: een instrument bij privacybescherming

J.E.J. Prins
Hoogleraar recht en informatisering, Katholieke Universiteit Brabant

Recht op Regie

De burger moet de regie weer in handen krijgen als het om het gebruik van zijn persoonsgegevens gaat, aldus minister Van Boxtel in zijn Nota *Contract met de toekomst. Een Visie op de elektronische relatie overheid-burger.* [1] Ook in het voorjaar 2001gepresenteerde rapport over de toekomst van de GBA, klonk deze boodschap door: de burger moet kunnen beschikken over een 'digitale kluis' waarmee hij het informationele zelfbeschikkingsrecht weer volledig in handen krijgt.[2] De burger moet naar eigen inzicht kunnen bepalen welke hem betreffende persoonsgegevens uit overheidsbestanden in zijn digitale kluis worden opgenomen en welke daaruit hij vervolgens op eigen initiatief verstrekt aan organisaties met een niet-publieke taak.

Uit deze en andere recente publikaties komt een veranderende visie op privacy naar voren: privacy als een vorm van individuele zeggenschap. Privacy staat in deze opvatting gelijk met autonomie. Welke is de rol van biometrie in deze? Alvorens een antwoord op deze vraag te formuleren, is het noodzakelijk stil te staan bij nog een visie op het recht van burgers, namelijk het recht op anonimiteit.

Recht op anonimiteit

Een recht op regie over de persoonsgegevens komt in de buurt van een recht op anonimiteit. Immers, uitgangspunt bij een recht op regie is anonimiteit en niet kenbaarheid. Ook het voorstel voor de introductie van een recht op anonimiteit kan zich

---

[1] Nota *Contract met de toekomst. Een Visie op de elektronische relatie overheid-burger*, TK 2000/2001, 26387, nr. 8, p. 28.

[2] Commissie Modernisering van de GBA, *GBA in de toekomst. Gemeentelijke Basis Administratie persoonsgegevens als spil voor toekomstige identiteits-infrastructuur*, Den Haag, maart 2001, p.47.

over een toenemende belangstelling verheugen.[3] Inmiddels hebben zich diverse voorstanders van de introductie van een dergelijk recht gemeld.[4] Het was opnieuw Minister Van Boxtel die tijdens de parlementaire behandeling van de nieuwe privacywetgeving (de Wet bescherming persoonsgegevens) aangaf, te bezien of het mogelijk is om burgers ten behoeve van de digitale communicatie met de overheid "anoniem of pseudo-certificaten beschikbaar te stellen waarbij gegevens van de persoon losgekoppeld worden van de persoon zelf."[5] Gewezen moet ook worden op de Raad voor het Openbaar Bestuur, die in januari 2000 met het rapport "ICT en het recht om anoniem te zijn" kwam.[6] Alhoewel de titel veel suggereert, gaat de Raad in het rapport zelf helaas nauwelijks in op de problematiek van anonimiteit.

Er zijn natuurlijk ook de tegenstanders van een recht op anonimiteit. Eind 1999 stonden de media vol van het bericht dat het VVD-kamerlid Cherribi anoniem surf- en communicatiegedrag op het Internet strafbaar wilde stellen. Aanleiding voor de actie van het kamerlid vormde de introductie in Nederland, door Internet Provider XS4All, van de Freedom-software. Met deze software kan een gebruiker zelf een anonieme elektronische identiteit ('nym') aanmaken en bestaan er geen mogelijkheden tot terugkoppeling tussen de werkelijke naam van de gebruiker en de gekozen elektronische identiteit. Ook de Provider als tussenpersoon kan de link tussen de beide identiteiten niet leggen.[7]

Belangen bij anonimiteit

Van oudsher is de ratio van anonimiteit gelegen in een diversiteit van belangen. Los van de specifieke omstandigheden van het Internet kan gewezen worden op het recht om zelf het moment te bepalen waarop informatie openbaar wordt, het afschermen van informatiebronnen, het onderhouden van contacten en relaties met uitsluiting van derden en het recht om zonder inmenging van anderen te communiceren en overleg te voeren. Deze belangen sluiten nauw aan bij het recht van een ieder op eerbiediging van zijn privéleven en zijn communicatie.

Mensen die in bepaalde situaties anoniem wensen te blijven in hun handelen, hebben soms echter wel de behoefte 'herkenbaar' te zijn. De bekendste voorbeelden zijn te vinden in de literaire en muziekwereld. Auteurs wensen weliswaar hun ware naam niet te onthullen, maar willen zich wel naar een grotere groep individualiseren (en aldus met hun

---

[3] Zie bijvoorbeeld de diverse bijdragen in de speciale editie over anonimiteit van het tijdschrift *The Information Society* (http://web.mit.edu/gtmarx/www/anon.html

[4] Zie: K. Spaink, Parool 28 juni 1999; L. Asscher, Niemand als consument. Naar een evenwichtig grondrecht op anonimiteit', in: De *e*-Consument. Consumentenbescherming in de Nieuwe Economie, Elsevier 2000; J.E.J. Prins, "What's in a name? De juridische status van een recht op anonimiteit", *Privacy & Informatie*, 2000-4, pp. 153 ev.

[5] TK '99-'00, 25 892, nr. (vergadering 17 november 1999).

[6] Raad voor het Openbaar Bestuur, 'ICT en het recht om anoniem te zijn', Den Haag, januari 2000.

[7] www.zeroknowledge.com/media/freedom-fs.asp

werk herkenbaar zijn). Hiertoe hanteren ze een pseudoniem. Er zijn overigens ook andere redenen waarom bepaalde auteurs zich niet onder hun ware naam bekend maken : zo kan de verzonnen naam beter aanslaan bij het publiek of wordt het pseudoniem gekozen uit mode-overwegingen.
Ook in een elektronische omgeving wensen mensen soms anoniem, maar toch herkenbaar te zijn. Een voorbeeld is het 'chatten'. In dit geval gaat het ook om de algemene bekendheid onder het pseudoniem (veelal 'nym' genoemd). De belangrijkste reden voor mensen om op het Internet hun identiteit volledig te verhullen, dus zelfs geen pseudoniem te gebruiken, is momenteel gelegen in de wens niet te worden blootgesteld aan de informatiedrang van derden. Kort gezegd is het belang gelegen in privacyoverwegingen. Toepassingen als Freedom zijn primair ontwikkeld om gebruikers van het Internet de mogelijkheid te bieden tot het anoniem verzenden van e-mails, het anoniem zoeken van informatie op websites, anoniem chatten, anonieme deelname aan spelletjes, etc.

Toch staat niet iedereen te springen om een maatschappij waarin vele handelingen volstrekt anoniem dan wel onder een pseudoniem plaatsvinden. Om meerdere redenen is het wenselijk mensen te identificeren. Een belangrijk oogmerk van kenbaarheid van de persoon is dat de handeling aan een bepaald persoon is te relateren zodat hij op dit handelen kan worden aangesproken (bijvoorbeeld bij fraude). Dit betekent bijvoorbeeld dat een pseudoniem te herleiden moet zijn tot de daadwerkelijke identiteit en dat individualiseerbaarheid dan te maken heeft met traceerbaarheid. Bij een dergelijk elektronisch pseudoniem zal de individuele *persoonlijkheid* van de persoon die de handeling verricht veelal niet relevant zijn. Wel zal de persoon als zodanig relevant zijn in verband met vragen als "wie draagt het risico voor bepaalde schade?" en "is de persoon die de schade moet betalen te achterhalen?".

Biometrie

Welke rol kan biometrie spelen bij de wens tot anonimiteit? Om deze vraag te kunnen beantwoorden, dient allereerst duidelijk te zijn wat precies biometrie is.

Biometrie komt kort gezegd neer op het gebruik van fysieke kenmerken of gedragskenmerken van een persoon ten einde zijn of haar identiteit vast te stellen of te verifiëren. Voorbeelden van biometrische technieken die gebruik maken van fysieke kenmerken zijn de vingerafdruk-herkenning, de handgeometrie-herkenning, de iris-scan, de retina-scan, de gelaatsherkenning, enz. Bij gedragskenmerken valt te denken aan het herkennen van dynamische handtekeningen en stemherkenning. Een groot voordeel van het gebruik van biometrie is gelegen in het feit dat fysieke of gedragskenmerken niet overdraagbaar of vervalsbaar zijn, en dat derhalve een hoger niveau van beveiliging kan worden gehaald dan met behulp van bijvoorbeeld PIN-codes. Vooralsnog wordt in de

(project)situaties waar biometrie wordt toegepast gebruik gemaakt van chipkaart voorzien van biometrie in combinatie met een PIN.[8]

Voordat men gebruik kan maken van een met biometrie beveiligde chipkaart moet deze worden gepersonaliseerd, dat wil zeggen, de chipkaart moet worden voorzien van gegevens van de betreffende persoon. Het biometrie-proces kent daarom twee fases: de invoerfase (ook wel personaliseringsfase genoemd) en de gebruiksfase.

In de eerstgenoemde fase moet men zich er allereerst van vergewissen dat de ingevoerde gebruiker inderdaad een geautoriseerde gebruiker is. Als de identiteit van de gebruiker is geverifieerd kan het eigenlijke personaliserings- of enrollment-proces beginnen. Tijdens dit proces wordt een biometrisch kenmerk van de gebruiker opgenomen (analoog signaal) en na conversie naar een digitaal signaal opgeslagen op de chipcard.

Alvorens het gedigitaliseerde signaal wordt opgeslagen kan het bewerkt worden teneinde onderscheidende kenmerken te benadrukken en de data te comprimeren. Het bewerkte en op de chipkaart opgeslagen digitale biometrische signaal wordt wel aangeduid als de 'template'.

Er zijn aldus twee verschillende biometrische gegevens: het oorspronkelijke (analoog) signaal en het bewerkte (digitale) signaal, de template. Bij het omzetten van het analoge signaal naar de template wordt gebruik gemaakt van een algoritme. Toepassing van een dergelijk algoritme is niet omkeerbaar; men kan vanuit de template derhalve niet meer terug kan naar het volledige signaal.

In de gebruiksfase wordt de opgeslagen biometrische template gebruikt om de identiteit van de gebruiker te verifiëren. Als de identiteit van een gebruiker geverifieerd moet worden, wordt opnieuw een biometrisch kenmerk opgenomen met behulp van een sensor (hierbij komt een analoog signaal beschikbaar). Het verkregen (analoge) signaal wordt omgezet in een digitaal signaal; er wordt een biometrische 'template' van het signaal gemaakt (dit levert de zogenaamde 'live scan' op). De template wordt vervolgens vergeleken met de template die tijdens het enrollment proces is verkregen en opgeslagen.[9]

---

[8] Meer in detail: R. van Kralingen, J.E.J. Prins, J. Grijpink, 'Het lichaam als sleutel', ITeR-reeks no. 8, Samsom, Alphen aan den Rijn 1997; R. Hes, T.F.M. Hooghiemstra, J.J. Borking, *At face value. On biometrical identification and privacy*, Registratiekamer 1999.

[9] Bij de verificatie wordt gebruik gemaakt van een vergelijkingsalgoritme dat bepaalde afwijkingen toelaat. Dit algoritme genereert een resultaat dat de mate van overeenkomst aangeeft. Als het resultaat binnen de grenzen van het acceptabele valt, levert de match een positief resultaat, anders een negatief resultaat. Als de grenzen te ruim zijn, kan biometrie niet worden aangemerkt als een adequaat beveiligingsmechanisme. Als de grenzen te krap worden ingesteld kunnen geautoriseerde gebruikers problemen ondervinden bij de verificatie-procedure.

Biometrie en privacyregels

In hoeverre staat de geldende privacywetgeving het gebruik van biometrie in de weg, of stelt ze nadere randvoorwaarden voor het gebruik? Centraal staat dan de vraag of er bij het gebruik van biometrie sprake is van de verwerking van persoonsgegevens. Indien dit het geval is, vallen de handeling binnen de reikwijdte van de wet.[10]

In de invoerfase zal veelal sprake zijn van een verwerking van persoonsgegevens onder de nieuwe privacywetgeving (Wbp), die naar verwachting 1 september 2001 van kracht wordt. Er wordt immers eerst vastgesteld of de in te voeren gebruiker inderdaad een geautoriseerde gebruiker is om vervolgens de biometrische kenmerken op te nemen. Aldus zullen de bepalingen van de wet in acht genomen moeten worden.

Voor wat betreft de vraag of ook tijdens de gebruiksfase sprake is van een verwerking van persoonsgegevens, ligt het ingewikkelder. Relevant criterium is hier of de verkregen templates centraal (in een achterliggende databank) dan wel gedistribueerd, dat wil zeggen op de chipkaart zelf, zijn opgeslagen. Als de templates in een database zijn opgeslagen zal in veel gevallen sprake zijn van identificeerbare gegevens, omdat de digitale gegevens van de template via de database worden gekoppeld aan het tijdens de invoerfase verkregen oorspronkelijk (analoge) signaal alsmede andere gegevens (zoals Naam-Adres-Woonplaats-gegevens).[11]

Het verschil heeft te maken met de wijze waarop de verificatie plaatsvindt. Bij een online systeem wordt voor het verificatie-proces contact gezocht met een database om de verschillende gegevens met elkaar te vergelijken. Bij offline verificatie behoeven de in de gebruiksfase verkregen gegevens alleen met de op de chipkaart opgeslagen template te worden vergeleken. Hiervoor is in principe geen nadere informatie vereist en behoeft de biometrische informatie niet in verband te staan of te worden gebracht met andere informatie (zoals identificerende gegevens).

Een 'losse' template, dat wil zeggen een template die niet via een database aan andere persoonsgegevens is gekoppeld, wordt niet als persoonsgegeven aangemerkt. Op basis van de template alleen is een persoon immers niet direct dan wel indirect te herleiden tot een individueel natuurlijk persoon. Het vraagt een onevenredige inspanning om bij de template behorende individuele persoon te herleiden. Koppelen via een achterliggende database van de template aan andere gegevens kan de benodigde inspanning reduceren, en er derhalve voor zorgen dat de template als persoonsgegeven moet worden gekwalificeerd.

---

[10] Zie voor een uitgebreide behandeling van de nieuwe privacywet: J.E.J. Prins, J.M.A. Berkvens, "De Wet bescherming persoonsgegevens", in: *Privacyregulering in theorie en praktijk*, Kluwer Deventer 2000, pp. 77 ev.

[11] Bij een centrale opslag van templates is niet per definitie sprake van identificatie. Het is bijvoorbeeld mogelijk dat een gebruiker een username of een PIN opgeeft en dat vervolgens slechts de bij die username opgeslagen template wordt vergeleken met de 'live scan'.

De Memorie van Toelichting bij art. 1 Wbp stelt op dit punt: "Zo zijn biometrische kenmerken omtrent een persoon, wanneer deze zijn vastgelegd op een gegevensdrager en daaraan impliciet of expliciet aanvullende informatie is verbonden, persoonsgegevens. Deze aanvullende informatie kan immers met hem in verband worden gebracht, zodra de biometrische kenmerken worden vergeleken met de kenmerken van de persoon waarvan zij afkomstig zijn."

Het onderscheid tussen de twee vormen van gebruik van biometrie (offline dan wel online) heeft ook implicaties voor de afwegingen onder de Wbp. Bij de keuze voor biometrie zal de vraag aan de orde zijn of de gekozen biometrische toepassing noodzakelijk is gegeven het beoogde doel, of dat met een minder ingrijpend alternatief kan worden volstaan. In veel gevallen is immers identificatie (online biometrie) niet noodzakelijk, maar kan ook worden volstaan met verificatie (offline biometrie).

Anonimiteit en Biometrie

Het bovenstaande maakt duidelijk dat anonimiteit niet op een lijn gesteld mag worden met traceerbaarheid dan wel identiteit. Technologische ontwikkelingen bieden de mogelijkheid om de mate van anonimiteit te variëren afhankelijk van de omstandigheden en de personen die bij een transactie of communicatie betrokken zijn. Zo kunnen in principe anonieme transactie uiteindelijk wel verifieerbaar zijn. Het bovenstaande maakt eveneens duidelijk dat biometrie en identificatie ook niet op een lijn gesteld mogen worden. Ook bij de toepassing van biometrie bestaan variatie-mogelijkheden. Deze kunnen er zelfs in resulteren dat biometrie volledige anonimiteit garandeert. Kortom: wanneer naar aanleiding van de roep om meer privacybescherming het instrument van de anonimiteit op tafel wordt gelegd, moet zorgvuldig worden nagaan waarover men het precies heeft. Primair zal aan alle partijen, en daarbij in het bijzonder aan de betrokken burgers, duidelijk gemaakt moeten worden of we het hebben over identificeerbaarheid, traceerbaarheid dan wel echte anonimiteit. Bij de vervolgvraag voor welke vorm van 'identificatie' van mensen gebruik gemaakt gaat worden, spelen de bepalingen van de nieuwe privacywetgeving mede een rol.