



Privacy waarborg biometrie



Verschil tussen Afis en commerciële systemen

Als er gesproken wordt over privacy en biometrie moet men direct kijken over wat voor systeem men praat. Bij de systemen van de overheid (politie, paspoort etc.) wordt er uitgegaan van een systeem waarbij men plaatjes opslaat (Afis systemen). Deze systemen kunnen, als zij in verkeerde handen vallen of verkeerd gebruikt worden, de privacy van mensen schenden. De commerciële systemen zoals op deze locatie gebruiken een algoritme en zijn niet te herleiden tot een echte afdruk dus niet te herleiden tot een natuurlijk persoon. Deze systemen worden gebruikt in het bedrijfsleven voor bijvoorbeeld: tijd-, toegang- en aanwezigheid systemen. Maar ook in de zorg voor patiënten herkenning, bij scholen voor examenregistratie, abonnementen voor zonnebanken, toegang tot serverruimtes etc.

Van lichaamskenmerk tot template

De vingerafdruk wordt gescand, dit plaatje wordt in de scanner al omgevormd tot een template. Deze template is de uitkomst van een algoritme en bestaat uit een cijfer van 364 posities. Het algoritme is gepatenteerd en het is ook nog eens beveiligd met encryptie (aes256, de hoogste vorm van encryptie).

Zelfs al zou de code gekraakt worden, dan nog moet men het algoritme kraken. En zelfs al zou het algoritme gekraakt worden dan nog is het onmogelijk om van de opgeslagen uitkomst een originele afdruk te maken.

Het is dus onmogelijk om van een opgeslagen template een plaatje te maken van een vingerafdruk die men daarna kan vergelijken met vingerafdrukken in een andere database of een aangetroffen plaatje.



Wetgeving

Nederlands Juridisch Kader Op biometrische gegevens zijn wettelijke regels van toepassing. Met name regels over de bescherming van persoonsgegevens of privacy.

Biometrische gegevens zijn persoonsgegevens omdat met die gegevens mensen van elkaar onderscheiden en geïdentificeerd worden. De biometrische persoonsgegevens worden opgeslagen in een gestructureerd bestand, dus vallen deze bestanden onder de Wet Bescherming Persoonsgegevens (Wbp in werking sinds 1 juli 2001). Deze wet is het gevolg van de Europese richtlijn 95/46/EG die na 1995 door de Europese lidstaten omgezet moest worden in een nieuwe wet. De Wbp is de opvolger van de Wet Persoonsregistraties (Wpr) en de Nederlandse vertaling van de richtlijn. Omdat er sprake is van gestructureerde bestanden met biometrische gegevens van natuurlijke personen vallen deze gegevens onder de Wbp. Belangrijke bepalingen zijn: Artikel 6 zegt dat: Persoonsgegevens worden in overeenstemming met de wet, en op behoorlijke en zorgvuldige wijze verwerkt. Artikel 7 schrijft voor dat: Persoonsgegeven worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld. Dus eerst het doel bepalen en beschrijven en dan pas verzamelen. Artikel 8 geeft gronden of redenen die verwerking rechtvaardigen. Van belang bij het gebruik van het systeem is het volgende: artikel 8 sub f: de gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van een verantwoordelijke of van een derde aan wie de gegevens worden verstrekt.

Toegangscontrole, tijdregistratie, patiënten herkenning kunnen zo'n gerechtvaardigd belang zijn. De verantwoordelijke is diegene die bepaalt voor welk doel(en) welk systeem zal worden gebruikt. Het mag niet zo zijn dat de bescherming van de persoonlijke levenssfeer van diegenen van wie biometrische gegevens worden verzameld belangrijker is dan het belang van de verantwoordelijke. Artikel 9 schrijft voor dat: Persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinde waarvoor ze zijn verkregen. Dat betekent dat eenmaal verzamelde gegevens niet zomaar voor een ander doel gebruikt mogen worden. Het nieuwe doel moet passen bij het oude doel of doelen.

Artikel 10 zegt dat: Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt. Met dit artikel wordt – kort gezegd – dat er zo kort mogelijke bewaartermijnen moeten gelden. Verder geldt vanzelfsprekend dat (o.a. op grond van artikel 11) er niet meer wordt verzameld dan nodig en dat de gegevens correct moeten zijn en blijven. Artikel 13 zegt: De verantwoordelijke legt passende en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Dit artikel betekent dat er een beveiligingsplicht geldt zodat de gegevens niet aangetast/veranderd of zo maar doorgegeven kunnen worden. En dat iemand die de gegevens niet mag zien die ook niet ziet. Het moeten passende maatregelen zijn waarbij rekening gehouden kan worden met de stand van de techniek.

Op grond van de artikelen 33 t/m 38 Wbp regelt kort gezegd het inzage, correctie en verwijderingsrecht van diegenen over wie gegevens worden verwerkt. Degenen over wie die gegevens worden verwerkt moeten op de hoogte zijn van die verwerking, wat er wordt verwerkt en waarom.