Face off! Waar de inzet van biometrie voor efficiënte toepassingen bijdraagt aan de staatsveiligheid

In hoeverre is het groeiend aantal biometrische toepassingen voor efficiëntere grenscontroles een bron van informatie voor de opsporing in de strijd tegen terrorisme?

Highlights

- Gebruik van biometrische toepassingen in de strijd tegen terrorisme.
- Kansen van biometrische toepassingen voor efficiënt reizen.
- Het belang van een goede balans tussen efficiëntie voor reizigers en het borgen van de privacy.

De maatschappelijke onrust die de laatste jaren is ontstaan door terroristische aanslagen, leidt tot een behoefte om grenzen strenger te controleren. Het gebruik van biometrische gegevens speelt hierbij een steeds grotere rol. Dit artikel beschrijft de noodzaak van biometrische toepassingen om de staatsveiligheid te verbeteren, enkele biometrietrends en geeft een kijkje in de toekomst wat betreft impact en kansen.

Noodzaak voor biometrische toepassingen

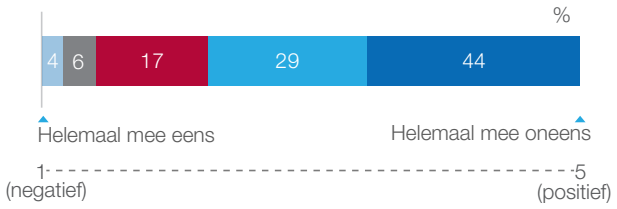
Europa is in de afgelopen jaren verschillende keren opgeschrikt door terroristische aanslagen. Met de aanslagen in onder andere Stockholm, Nice, Istanbul, Parijs, etc. nog vers in het geheugen, wordt alles op alles gezet om ongewenste en potentieel gevaarlijke reizigers aan de grens te identificeren. We willen weten wie op welk moment het land is binnengekomen en of reizigers het land ook weer hebben verlaten. Om dit mogelijk te maken is de Schengengrenscode aangepast. Nu moeten zowel burgers van de Europese Unie, als personen met een niet EU-nationaliteit, voortaan een systematische veiligheidscontrole ondergaan wanneer ze de EU binnenkomen of verlaten. Iedereen die de Europese Unie binnenkomt via de buitengrenzen, wordt opgezocht in databanken zoals het 'Schengen Informatie Systeem' (SIS) en de databank over verloren en gestolen reisdocumenten. Naast EU-burgers worden ook reizigers uit de rest van de wereld gecontroleerd. Om de veiligheid zo goed als mogelijk te borgen, worden op Schiphol door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) bepaalde procedures gehanteerd bij het controleren van passagiers en hun bagage.

Technologieën voor grenscontrole op basis van biometrische eigenschappen bieden daarbij een uitkomst in het behoud van staatsveiligheid.

Ontwikkeling van biometrische toepassingen

Al jaren is het toepassen van technologieën die gebruikmaken van vingerafdrukken populair. Op dit moment zie je een duidelijke verschuiving ontstaan naar het gebruik van andere vormen van biometrie zoals een irisscan of gezichtsherkenning. Deze technologieën worden ingezet voor het verzamelen van informatie over individuen om de maatschappelijke en staatsveiligheid te vergroten. Deze toename van andere vormen van biometrische verificatie zorgt dat de veiligheidsdiensten meer informatie tot hun beschikking krijgen om verdachte personen op te sporen en te volgen. Slimme camera's worden al op veel plekken ingezet (denk hierbij aan treinstations, luchthavens, grensovergangen) om de omgeving beter in kaart te brengen en verdachte situaties eerder te herkennen. Hiervoor is draagvlak in de samenleving. Slechts tien procent van de Nederlanders staat volgens onderzoek van Kantar TNS negatief tegenover het gebruik van biometrie bij grenscontroles.

Figuur 1: Hoe staat u tegenover biometrie bij grenscontroles die (mogelijk) wordt ingezet om uw veiligheid te vergroten?



Actuele initiatieven

Naast het vergroten van de staatsveiligheid maken deze technologieën ook bepaalde processen efficiënter, zoals grenscontroles. Steeds meer luchthavens bieden reizigers de mogelijkheid om zonder boardingpass en paspoort door de verschillende controles heen te kunnen. De controle die plaatsvindt, wordt namelijk gedaan op basis van gelaatsherkenning. Een greep uit de actuele initiatieven voor de toepassing van biometrische gegevens bij grenscontroles:

1. Op de luchthavens in de Verenigde Staten maakt de douane nu gebruik van speciale systemen die geschikt zijn voor gezichtsherkenning. Via scanners wordt het gezicht van een reiziger vergeleken met de pasfoto op het paspoort. Door middel van koppeling met politiesystemen zouden de scanners kunnen aantonen of iemand een vals identiteitsbewijs gebruikt.
2. Als onderdeel van het US-VISIT Biometric Entry and Exit programma worden de grensovergangen tussen de VS en Mexico uitgerust met vingerafdruk- en irisscanners. Deze technologie werd eerder al met succes getest bij grensovergangen tussen Afghanistan en Irak.
3. Met het programma Schiphol NeXt probeert de Nederlandse luchthaven de beveiliging efficiënter te laten werken door slimme camera's en robots mensen op te laten sporen die zich verdacht gedragen
4. Met Aruba Happy Flow wordt publieke grenscontrole aan private passagiersdata gekoppeld met als doel een snel, veilig en eenvoudig passagiersproces.
5. Australië wil met haar Seamless Traveler project in 2020 90% van de inreizigers doorlaten op basis van een geautomatiseerd passagiersproces dat gebruik maakt van biometrische kenmerken.

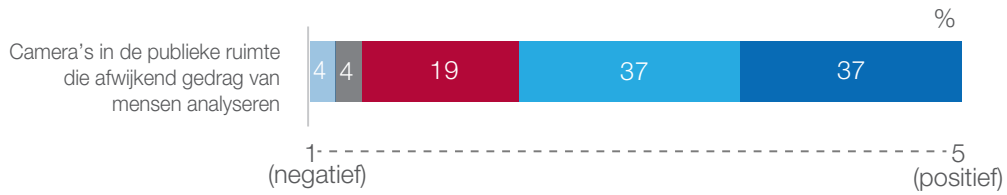
Deze initiatieven hebben met elkaar gemeen dat biometrische kenmerken van een reiziger worden vastgelegd en gecontroleerd bij het passeren van een landsgrens over land of door de lucht. Naast het staatsveiligheidsbelang dat hiermee gediend

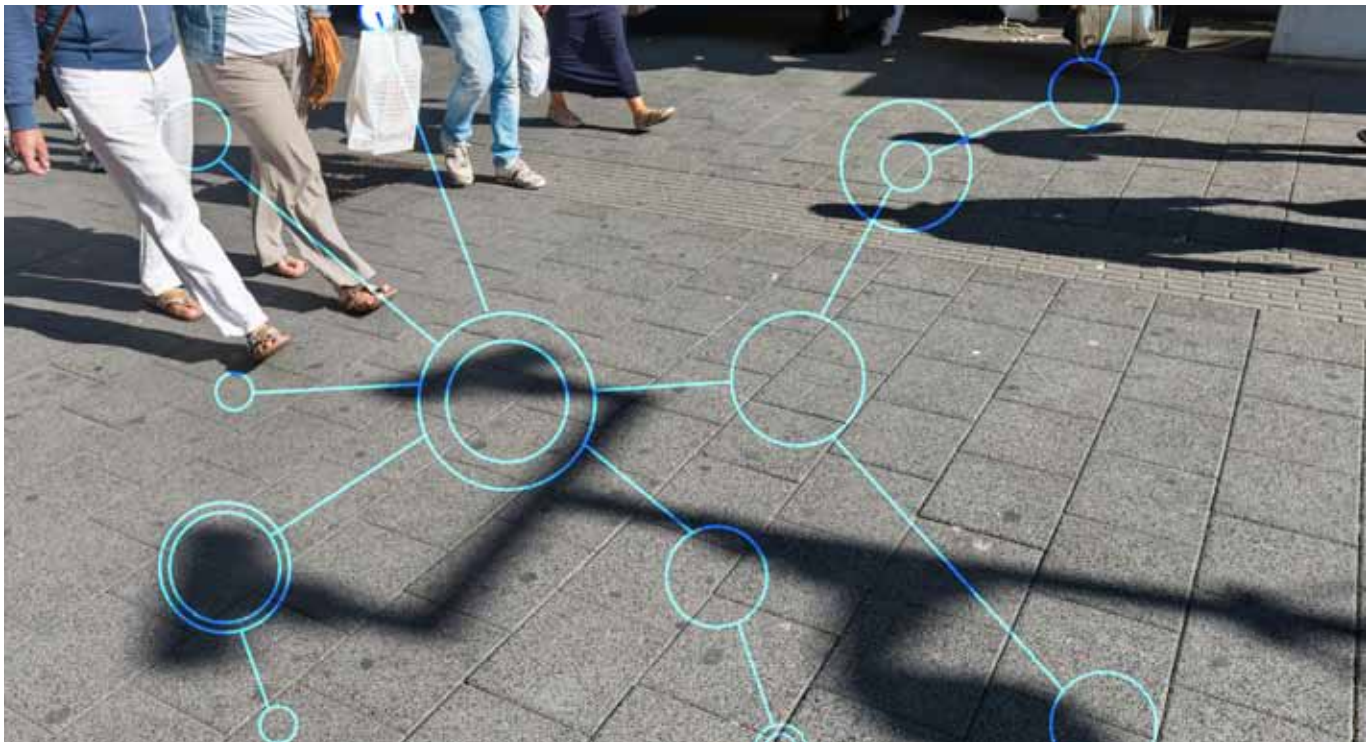
wordt, ontstaan grote voordelen voor reizigers. Zo worden wachttijden voor douane en paspoortcontroles drastisch verkort. Daarnaast wordt het risico op diefstal van identificatiepapieren verkleind, doordat reizigers deze al snel, na slechts één keer tonen, veilig kunnen opbergen.

Veiligheid en gebruiksgemak

Bovenstaande voorbeelden van biometrische technologieën worden veelal in één adem genoemd met het beheersbaar maken van maatschappelijke dreigingen. Naast de noodzaak van deze technologieën in de strijd tegen onder andere terrorisme, bieden deze ook veel kansen voor reizigers. Het succes van initiatieven als Aruba Happy Flow en Schiphol NeXt is te danken aan een combinatie van vele factoren. De initiatieven maken efficiënter werken mogelijk waardoor minder personeel in hoeft te worden gezet, passagiers hoeven niet meerdere keren hun reispapieren te laten zien en men voelt zich veiliger in de wetenschap dat scherp toezicht wordt gehouden. De toepassingen maken het mogelijk personen op bijvoorbeeld luchthavens van het moment van binnenkomen tot het weggaan te volgen. Dit biedt mogelijkheden voor handhavings- en opsporingsdoeleinden. Hiervoor is ook draagvlak in de samenleving. Uit onderzoek van Kantar TNS blijkt dat de ontwikkeling van hulpmiddelen als bodycams, biometrie en camera's in de publieke ruimte met gezichtsherkenning die worden gebruikt om de veiligheid te vergroten door 7 op de 10 Nederlanders als positief wordt ervaren.

Figuur 2: Hoe staat u tegenover de onderstaande technologieën die (mogelijk) worden ingezet om uw veiligheid te vergroten?





Met staatsveiligheid als hoger doel worden (of kunnen) biometrische gegevens gecombineerd (worden) met verschillende databronnen. Denk hierbij aan het gebruik van bronnen als Automated Number Plate Recognition (ANPR), Closed Circuit Television (CCTV), Passenger Name Records (PNR), maar ook politiebronnen die worden gecombineerd met biometrische gegevens van reizigers (zoals de vingerafdruk in je paspoort). Het combineren van verschillende databronnen met biometrische gegevens brengt enorme kansen met zich mee voor passagiers en luchtvaartmaatschappijen, maar ook voor opsporing en handhaving. Bijvoorbeeld het traceren van een (op het vliegveld) vermist kind, het traceren van personen die hun bagage hebben ingecheckt maar niet op tijd bij de gate zijn, het koppelen van personen aan niet geclaimde bagage, maar ook commerciële mogelijkheden als het aanbieden van de juiste advertentie aan de juiste reiziger. Gebruik van data analytics kan inzicht geven in looppatronen binnen het vliegveld, de voorkeuren in koopgedrag van reizigers of de voorspelling van reizigers die vermoedelijk de vlucht zullen vertragen. Analyse van deze gecombineerde databronnen kan ook leiden tot patronen van personen die zich afwijkend gedragen en personen met criminele of terroristische intenties.Het analyseren van gedrag van reizigers kan in theorie zowel op het individu toegespitst gebruiksgemak als individuele en algemene veiligheid ten goede komen.

Risico's

Hoewel we graag gefaciliteerd worden in een vlotte doorstroom tijdens onze reis, brengt dit enkele belangrijke veiligheidsvraagstukken met zich mee. Tegenover het scala aan kansen dat biometrische technologieën biedt, staan ook privacy- en securityvraagstukken. Bij het gebruik van persoonsgegevens dient strikt gekeken te worden of het gebruik van de gegevens proportioneel is ten opzichte van de doeleinden waarvoor zij verzameld zijn. Bovendien is transparantie over de gegevensverzameling van belang en is soms zelfs toestemming nodig om gegevens te mogen verwerken. Daarnaast zijn biometrische eigenschappen weliswaar uniek, maar dit betekent niet dat deze niet te hacken zijn. Intussen is al aangetoond dat biometrische gelaatskenmerken kunnen worden 'gehackt' door plastische chirurgie of zelfs een plastic vingerafdruk die wordt gemaakt op basis van een foto in hoge resolutie van een echte vingerafdruk.

De roep om de controle terug te krijgen over grenzen, zorgt ervoor dat landen in toenemende mate maatregelen treffen om inzicht te krijgen in wie, wanneer en waar de grenzen passeert. Toepassingen waar gebruik wordt gemaakt van biometrische verificatie worden op steeds meer plekken ingezet om verdachte personen op te sporen. Daarnaast zie je dat reizigers op luchthavens de mogelijkheid wordt geboden om door middel van biometrie geen 'last' meer hebben van de reguliere controles. In beide gevallen wordt een biometrisch kenmerk van een passagier gebruikt.

Of de inzet van deze toepassingen daadwerkelijk gaat leiden tot een veiligere situatie moet nog blijken. Wel zie je de trade off tussen veiligheid en privacy sterk verschuiven. Of, en in hoeverre, we onze privacy steeds meer willen opgeven voor een sterker veiligheidsgevoel en toepassingen die ons leven efficiënter maken is een belangrijke vraag die we steeds moeten blijven stellen.

Over de auteurs

Gijs Daalmijer MSc is bestuurs- en veiligheidskundige en als consultant werkzaam bij Capgemini. Hij is actief op het gebied van openbare orde en veiligheid en biometrie. Lieke Schepers MSc is criminoloog en als senior consultant werkzaam bij Capgemini. Lieke richt zich op vraagstukken in de openbare orde- en veiligheidsmarkt met een focus op Intelligence en digitale opsporing.

Voor meer informatie kunt u contact met de auteurs opnemen via:
gijs.daalmijer@capgemini.com, www.linkedin.com/in/gijsdaalmijer en lieke.schepers@capgemini.com, www.linkedin.com/in/liekeschepers