Anoniemer over straat door inzet nieuwe technologie? Privacy by design maakt het mogelijk!

Op welke manier vergroot ‘privacy by design’ de zorgvuldige inzet en acceptatie van nieuwe technologieën zoals automatische gezichtsherkenning?

Highlights

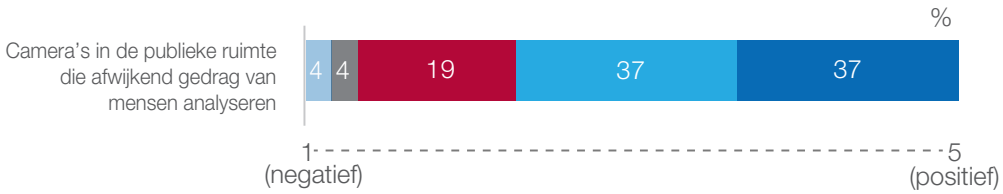
- Nieuwe technologieën, zoals automatische gezichtsherkenning, bieden steeds meer mogelijkheden voor toezicht.
- Privacy by design is een manier voor de overheid om mogelijk ingrijpende technologieën zorgvuldig en effectief in te zetten.
- Privacy by design, nu vaak nog een containerbegrip, moet de komende tijd handen en voeten krijgen.
- De overheid kan hierin zelf het goede voorbeeld geven en transparant zijn over genomen maatregelen.
- De overheid kan het delen van ‘best practices’ stimuleren.

Steeds meer organisaties in het publieke veiligheidsdomein zetten nieuwe technologische mogelijkheden, zoals automatische gezichtsherkenning met slimme camera’s, in om het toezicht te verbeteren. Veel van deze technologieën dringen binnen in de persoonlijke levenssfeer van individuen. Het toepassen van ‘privacy by design’ voorkomt dat mogelijk ingrijpende technologieën onzorgvuldig worden ingezet.

Na de aanslag op de Kerstmarkt in Berlijn afgelopen jaar werd in Duitsland direct de vraag gesteld of de mogelijke dader niet eerder zou zijn opgepakt als in de openbare ruimte meer bewakingscamera’s hadden gehangen. In het land waar persoonlijke vrijheden en privacy op een hoog voetstuk staan kenterde de publieke opinie: in de strijd tegen terreur leken mensen meer bereid te zijn om een deel van hun anonimiteit op te geven. Nieuwe technologieën bieden steeds meer mogelijkheden voor toezicht. Hoewel sommige technieken nog volop in ontwikkeling zijn en worden getest, is het met nieuwe camera’s al mogelijk om personen op straat te volgen, te identificeren en emoties van gezichten af te lezen. Niet meer anoniem over straat kunnen: voor sommigen een angstbeeld dat past bij een politiestaat, voor anderen een noodzaak om een moderne samenleving veilig te houden.

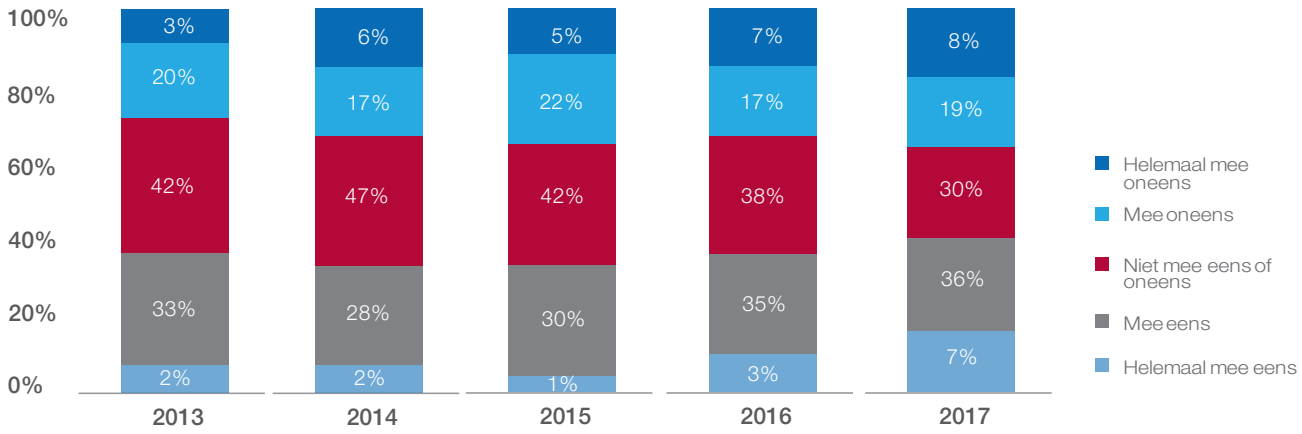
Acceptatie van privacy ingrijpende technieken in de publieke ruimte hangt in belangrijke mate af van het doel waarvoor de overheid een bepaalde techniek inzet. Uit onderzoek van Kantar TNS blijkt bijvoorbeeld dat 71% van de Nederlandse bevolking positief staat tegenover de inzet van camera’s met gezichtsherkenning als dat hun veiligheid vergroot. Slechts 43% van de Nederlandse bevolking daarentegen, heeft vertrouwen dat de overheid hun privacy voldoende beschermt. Hier valt dus winst te behalen.

Figuur 2: Hoe staat u tegenover camera's die (mogelijk) worden ingezet om uw veiligheid te vergroten?



Figuur 2: De bevolking is verdeeld in haar vertrouwen ten aanzien van de privacybescherming door de overheid.

Ik heb er vertrouwen in dat de overheid mijn privacy voldoende beschermt



Privacy by design is een manier voor de overheid om mogelijk ingrijpende technologieën zorgvuldig en effectief in te zetten, transparant te zijn en tegelijkertijd niet onnodig in de persoonlijke levenssfeer van burgers binnen te dringen. Het is dan wel van belang dat privacy by design, nu vaak nog een containerbegrip, de komende tijd handen en voeten krijgt. De overheid kan hierin een rol spelen door zelf het goede voorbeeld te geven en het delen van 'best practices' te stimuleren.

Automatische gezichts- en emotie-herkenning

De techniek om automatisch gezichten te herkennen is de laatste tijd sterk verbeterd. Onder automatische gezichtsherkenning wordt verstaan: 'het automatisch verwerken van digitale afbeeldingen die gezichten van individuen bevatten, met als doel de identificatie, verificatie of categorisatie van deze individuen'[1]. Het Rathenau Instituut benoemt in hun in 2015 gepubliceerde rapport 'Dicht op de huid: emotie- en gezichtsherkenning in Nederland' vijf soorten toepassingen waarbij het gezicht als informatiebron wordt gebruikt: verifiëren, identificeren, matching, categoriseren en emotieherkenning[2]. Het Rathenau Instituut omschrijft de vijf toepassingen als volgt:

- Verifiëren: controleren of een persoon is wie hij claimt te zijn. Het gezicht wordt vergeleken met een eerder opgeslagen sjabloon (template) of afbeelding van zijn eigen gezicht.
- Identificeren: het vergelijken van een live beeld van een persoon met afbeeldingen of sjablonen in een database. Het gezicht wordt met een hele database vergeleken.
- Matching: afbeeldingen in een database met elkaar vergelijken, in plaats van een live beeld met een database. Het doel van matching is om afbeeldingen van dezelfde persoon bij elkaar te zoeken.
- Categorisatie: categorisatie is erop gericht om informatie uit gezichten te halen die niet direct verbonden zijn aan één persoon, zoals groepskenmerken als leeftijd, ras en sekse.
- Emotieherkenning: gezichtsuitdrukkingen of andere kenmerken van een persoon vertalen naar diens emoties of algemene gemoedstoestand.

[1] Vertaald uit: Article 29 data protection working party 2012, p. 2.
[2] Dicht op de huid: emotie- en gezichtsherkenning in Nederland, Rathenau Instituut, 2015, p.11.

Privacy-impact gezichtsherkenning

De impact op de privacy van het individu verschilt per toepassing, maar hangt zeker samen met het doel waarvoor - en de context waarin - die wordt ingezet. De impact van verifiëren, identificeren en matchen van afbeeldingen is misschien kleiner wanneer het individu hierover vooraf is geïnformeerd in een context waarin het te verwachten is (bijvoorbeeld bij de douane op Schiphol), dan wanneer het ongemerkt op een locatie gebeurt waar men zich anoniem waant. Categorisatie is mogelijk zeer gevoelig omdat kenmerken als ras, leeftijd en geslacht veel informatie over onze identiteit prijsgeven. Wanneer het onmogelijk is om informatie te herleiden naar een individu (bijvoorbeeld wanneer uitsluitend is af te lezen dat de persoon in kwestie een man is) is de impact uiteraard geringer of zelfs afwezig. Bij emotieherkenning is de impact met name groot wanneer men zich anoniem waant en zich niet bewust is van zijn of haar gezichtsuitdrukking. Ook nieuwe technische ontwikkelingen, zoals het steeds gemakkelijker aan elkaar koppelen van databases, zorgen mogelijk voor een grotere impact op de privacy van het individu. Wat precies de impact op de privacy is van een bepaalde techniek en toepassing is dus moeilijk in zijn algemeenheid vast te stellen.

Toepassingen gezichts- en emotieherkenning in het veiligheidsdomein

Cameratoezicht met automatische gezichtsherkenning is niet nieuw. Organisatoren van grote (inter)nationale evenementen zoals de Olympische Spelen, het WK-voetbal, de Amerikaanse Super Bowl en nationale voetbalwedstrijden passen de technologie al ruimschoots toe. Ook luchthavens zijn proeven gestart om passagiers sneller door de douane te leiden. Schiphol doet bijvoorbeeld in navolging van de luchthaven op Aruba een test met automatische gezichtsherkenning om passagiers sneller door de douane te leiden. Passagiers hoeven nog maar eenmalig hun paspoort te laten zien in de terminal. Door middel van gezichtsherkenning kan de passagier vervolgens inchecken, de bagage inleveren, de grens passeren en aan boord gaan van het vliegtuig zonder paspoort of boarding pass nogmaals te hoeven tonen. Hier wordt een match gemaakt tussen het live beeld en de foto op het paspoort. Automatische gezichtsherkenning wordt ook in talloze lokale initiatieven toegepast. In Rotterdam passen tramlijnen waar voor bepaalde mensen een OV-verbod geldt de technologie toe. In de VS passen lokale politieteams de technologie toe om tijdens aanhoudingen direct een foto te maken en tegen een database aan te houden. De FBI onderzoekt in haar programma Next Generation Identification (NGI) de mogelijkheden om ten behoeve van de nationale veiligheid gezichtsherkenning uit te breiden en databases aan elkaar te koppelen. Wanneer deze ontwikkeling zich internationaal uitbreidt, leidt dit onherroepelijk tot privacydiscussies.

Privacy by design

Privacy krijgt de laatste jaren steeds meer aandacht als gevolg van de opkomst van nieuwe technologieën. Wetgevers reageren hierop door het opstellen van wetgeving die de rechten van individuen beter moet beschermen. Nieuwe Europese wetgeving, de General Data Protection Regulation (GDPR), schrijft voor dat bij de ontwikkeling van nieuwe technieken en diensten ‘privacy by design’ (of ‘data protection by design’) moet worden toegepast.

Privacy by design bestaat in ieder geval uit de volgende elementen:

- Neem de bescherming van de privacy van individuen over wie persoonsgegevens verwerkt worden direct mee bij het ontwerp van een systeem of dienst.
- Neem passende technische maatregelen om toegang tot - en omgang met - persoonsgegevens te regelen en veilig te laten plaatsvinden.
- Neem passende organisatorische maatregelen om toegang tot, en omgang met persoonsgegevens te regelen volgens bepaalde afspraken en voorschriften.

Organisaties die verantwoordelijk zijn voor de verwerking van persoonsgegevens moeten per toepassing goed nadenken wat passende technische en organisatorische maatregelen zijn om de privacy van individuen te beschermen. Technische maatregelen hebben betrekking op informatiebeveiliging, zodat de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen een organisatie is gegarandeerd. Een voorbeeld van privacyvereisten waarvoor technische maatregelen moeten worden genomen is: de eis dat uitsluitend bevoegde en geautoriseerde personen voor een duidelijk gedefinieerd doel bij bepaalde informatie mogen. Hiervoor moeten in systemen de juiste autorisaties worden ingericht. Andere voorbeelden zijn dat gegevens slechts gedurende een bepaalde tijd mogen worden bewaard, op de juiste manier moeten worden vernietigd en een betrokkene op een effectieve manier controle moet kunnen uitoefenen over zijn of haar gegevens. Hiermee moet rekening worden gehouden tijdens het ontwerpen van een systeem. Organisatorische maatregelen hebben bijvoorbeeld betrekking op bewustwording bij mensen die met (gevoelige) persoonsgegevens werken, transparantie richting de mensen van wie persoonsgegevens worden verwerkt en duidelijke communicatie.

Wanneer privacy direct bij het ontwerp van toepassingen wordt meegenomen, kan privacy als ‘enabler’ werken om de juiste toepassingen, op de juiste manier, voor de juiste vooraf bepaalde doelen in te zetten. Op die manier wordt voorkomen dat achteraf blijkt dat een toepassing onzorgvuldig is geïntroduceerd en hiervoor in de samenleving weinig draagvlak is.

Rol overheid

De overheid kan een cruciale rol spelen in het creëren van draagvlak voor nieuwe technologieën. De overheid kan bijvoorbeeld een afwegingskader ontwikkelen voor organisaties die nieuwe technologieën inzetten waarin altijd een zorgvuldige weging plaatsvindt tussen het doel van een nieuw middel en de inbreuk op de persoonlijke levenssfeer van burgers. Vervolgens kan de overheid het goede voorbeeld geven door transparant te zijn over deze afweging en de privacyverhogende maatregelen die zij neemt wanneer nieuwe technieken worden ingezet.

Tot slot kan de overheid stimuleren dat best practices op het gebied van privacy by design worden gedeeld. Effectief toezicht met moderne technieken en voldoende privacybescherming van individuen staan elkaar niet per definitie in de weg. Nieuwe technieken bieden ongekende mogelijkheden, maar het is van belang dat bij de ontwikkeling hiervan direct aandacht is voor privacy. Wat passende technische en organisatorische privacy maatregelen zijn verschilt per techniek en toepassing. Privacy by design moet de komende tijd meer handen en voeten krijgen. Het angstbeeld dat werd geschetst door George Orwell in ‘1984’ dat je moest leven in de veronderstelling dat elk geluid dat je maakte werd afgeluisterd en elke beweging nauwkeurig werd bestudeerd - ‘Big Brother is watching you’ - hoeft niet uit te komen. Paradoxaal genoeg zou automatische gezichtsherkenning er zelfs voor kunnen zorgen dat we anoniemer over straat kunnen doordat een computer en niet een mens (zoals bij beveiligingscamera’s) de beelden bekijkt. Het is dan wel van belang dat de overheid transparant is over de inzet van nieuwe technieken en de manier waarop zij privacy by design bij de ontwikkeling hiervan invult.

Privacy by design houdt in dat bij de bepaling van de middelen waarmee persoonsgegevens worden verwerkt en bij de verwerking van persoonsgegevens zelf, passende technische en organisatorische maatregelen moeten worden genomen om voldoende privacybescherming te beiden. Er moet dus al direct bij het ontwerp van processen en systemen aandacht zijn voor privacy.

Over de auteurs

Christian le Clercq LLM MSc en Bart Bikkers MSc zijn beide senior consultant bij Capgemini Consulting en richten zich specifiek op vraagstukken op het vlak van privacy, nationale veiligheid en crisismanagement.

Voor meer informatie kunt u contact opnemen met de auteurs via:
christian.le.clercq@capgemini.com, www.linkedin.com/in/christian-le-clercq-7a74239, @cleclercq en bart.bikkers@capgemini.com, www.linkedin.com/in/bartbikkers, @BartBikkers