

De camera ziet u, maar wilt u ook herkend worden?

De technologie voor gezichtsherkenning is er. Politiediensten staan te popelen om ze te gebruiken. Waarom zouden we er dan nog scrupules bij hebben? ‘Het is minder ingrijpend dan iedereen te moeten tegenhouden voor een identiteitscontrole.’

Wat met privaat gebruik?

Lees verder onderaan

NIKOLAS VANHECKE, DOMINIQUE DECKMYN FOTO'S FRED DEBROCK

Wie wandelde op dinsdag 17 september tussen drie en zes uur 's namiddags door de Rekolettenstraat in Kortrijk? Waren er mannen bij en hoeveel? Wie onder hen had een blauwe trui aan? En was die trui dan eerder licht- of donkerblauw? Met lange of korte mouwen? Wie had zijn hoofd bedekt? Hoeveel kinderen passeerden er? Welke auto's reden er voorbij in die drie uur? Hoeveel pick-ups en bestelwagens zaten ertussen? Hoeveel witte? Hoeveel gele? Welke fietsers reden over het voetpad? Wanneer precies deden ze dat?

Het antwoord op elk van die gedetailleerde vragen komt van software met de naam Briefcam, die de beelden van bewakingscamera's via gebruiksvriendelijke keuzemenu's analyseert. Politiezone Vlas, waarvan Kortrijk de centrale poot is, kocht de Israëlische software samen met de stad aan voor 106.961 euro. Nog deze maand, na de opleiding van een veertigtal van de driehonderd korpsleden, wordt het systeem er operationeel. De voorbije weken is het al getest, onder meer met beelden van die dinsdag 17 september.

‘Dit is géén software voor gezichtsherkenning’, benadrukt woordvoerder Thomas Detavernier een paar keer tijdens een bezoek aan de dispatching-zaal van de zone. Briefcam moet er even ingeburgerd raken als de 185 camera's waarmee ze nu al werken. Al van bij de aankondiging van het project dit voorjaar waren er kritische bemerkingen (*DS 24 mei*), omdat de toepassing heel dicht aanleunt bij gezichtsherkenning, wat uiterst gevoelig ligt.

‘Er is een sluipende voortschrijding van de technologie bezig, zodat we er stilletjes aan wennen. Als burger moeten we “stop” durven te zeggen’ MARK

COECKELBERGH Technologie-filosoof Universiteit Wenen

Detavernier: 'We begrijpen dat er veel kritiek op is. We kregen al een paar keer een vraag over Briefcam en gezichtsherkenning, maar het antwoord is eenvoudig: wij doen het niet, want het mag niet. Voor ons is het zelfs nooit aan de orde geweest.'

Identified objects

Briefcam heeft die mogelijkheid wel in zich – ook de versie die in Kortrijk wordt gebruikt. De Belgische invoerder en installateur ervan, het Ieperse bedrijf RTS, heeft de gebruiksrechten van de software moeten aanpassen om de optie in de praktijk achterwege te laten. 'We moeten onze leveranciers dikwijls uitleggen dat bepaalde zaken bij ons niet zijn toegelaten', zegt Pieter-Jan Machtelinckx van RTS. 'Zij gaan ervan uit dat iedereen al gezichtsherkenning wil.'

Die Belgische aanpassing maakt de software nauwelijks minder krachtig. Uit uren opnames van die zeventiende september distilleert het programma zelf 1.463 'objecten': personen en voertuigen. Die drukt de software samen in een video van bijvoorbeeld twintig minuten, waarbij de voetgangers en auto's elkaar voor de voeten lopen en het overzicht zoek raakt. Wanneer Machtelinckx op het scherm een knop aanklikt die lijkt op een volume-regelaar, past hij de 'dichtheid' aan.



Zelf signaleert de software geen **verdacht gedrag**. Dat is de taak van de persoon die de beelden bekijkt.

Nog eenvoudiger wordt het als je Briefcam de objecten laat filteren op basis van hun kenmerken, door er bijvoorbeeld alleen de personen met een korte witte broek uit te halen. 'Met Briefcam kunnen we de beelden van onze camera's veel gericht gebruiken', zegt Detavernier. 'Zelf zal de software geen verdacht gedrag signaleren. De technologie helpt ons om - criminele feiten op te helderen.'

Het programma doet dat op een, het dient gezegd, indrukwekkende manier. Mensen in de gaten houden, het leek nog nooit zo eenvoudig.

Wie ligt nog wakker van privacy?

Veiligheidsdiensten met software die mensen automatisch herkent, op basis van hun kledij of hun gezicht, het is slechts het stapje verder. Wanneer nieuwe technologie op de markt komt, wordt altijd snel gekeken naar wat die kan betekenen voor criminaliteitsbestrijding. 'Maar nu schakelen we toch een versnelling hoger. De technologie laat vandaag toe om massaal biometrische gegevens (*data over iemands lichaamskenmerken, red.*) te capteren', zegt Frank Schuermans van het Controleorgaan op de Politie Informatie (COC).

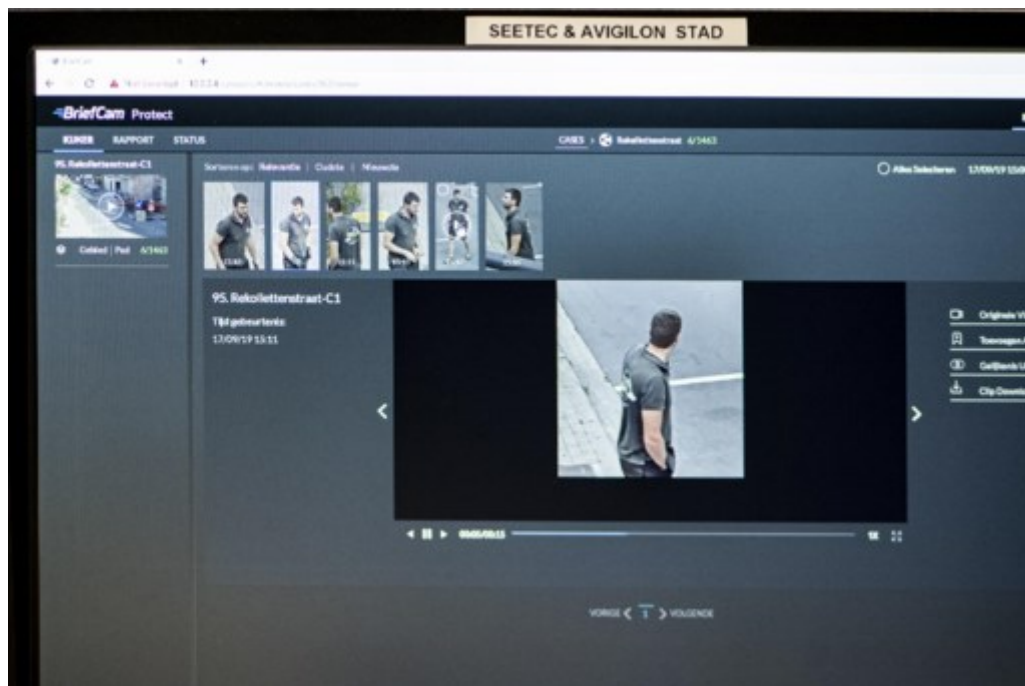
Briefcam filtert 'objecten' op basis van hun kenmerken, zoals een korte witte broek. Mensen in de gaten houden, het leek nog nooit zo eenvoudig

'De opslag van telefoniegegevens gebeurt óók massaal, en je kunt er veel mee te weten komen over iemands privéleven, maar dit is toch nog iets anders. Biometrie gaat echt over wie je bent, het is een unieke identifier. De volgende stap is volgens mij de massa-opslag van DNA-gegevens. De evolutie gaat al in die richting.'

Schuermans, die voorheen jarenlang advocaat-generaal was in Gent, merkt dat er vroeger 'meer gêne' bestond over privacygevoelige maatregelen. 'Wie ligt er vandaag nog echt wakker van privacy, behalve als men zelf slachtoffer is? In dit soort politiek-maatschappelijke discussies helt de consensus al snel over naar de efficiëntie van de handhaving. We kunnen de evolutie moeilijk tegenhouden, wel zo goed mogelijk omkaderen en controleren. Net daar knelt soms nog het schoentje: te vaak begint de politie met toepassingen die heel performant zijn, om zich pas daarna te bekommeren om de beveiliging van de informatie. Sinds de nieuwe regels rond gegevensbescherming begint de mentaliteit bij de politie te veranderen, al is er nog een hele weg af te leggen.'

De fout van Zaventem

Bij een project rond gezichtsherkenning dat de federale politie op Brussels Airport op poten had gezet, liep het grondig mis. Na de aanslagen van 22 maart 2016 werd de beveiliging op de luchthaven van a tot z herdacht, inclusief gezichtsherkenning. Maar de federale politie overtrad de wetten die bepalen over wie ze gegevens mag bijhouden. Half september moest het project in allerijl worden gestaakt (*DS 21 september*).



Via gebruiksvriendelijke **keuzemenu's** analyseert Briefcam de beelden.

Om op de luchthaven aan de hand van gezichten na te gaan of er zich geseinde criminelen onder de duizenden dagelijkse reizigers bevinden, heb je twee databanken nodig. De ene bevat de biometrische gegevens van die gezochte misdadigers – daar is volgens de wet geen probleem. De tweede bevat biometrische gegevens van de voorbijwandele reizigers, op basis van de beelden van camera's op de luchthaven. Zonder enig onderscheid te maken tussen beide databanken werden tijdelijk de gegevens opgeslagen van een heleboel mensen die strafrechtelijk nooit iets mispeuterd hadden. En dat is een overtreding van de regels.

Mag gezichtsherkenning door opsporingsdiensten op dit moment dan helemaal niet? Philippe Van Linthout, co-voorzitter van de Vereniging van Onderzoeksrechters, meent van wel. 'Als we weten dat er een specifieke persoon rondloopt met een bom in zijn rugzak én er is op die plek technologie voor gezichtsherkenning beschikbaar, dan kunnen we die inzetten, net zoals we andere bijzondere onderzoeksmethoden zouden gebruiken.'

'Het verschil zit hem in de context: als je constant scant wie er allemaal op een bepaald plein aanwezig is, is er sprake van een bestuurlijke maatregel en is gezichtsherkenning niet toegelaten. Als je in de massa op zoek gaat naar één specifieke persoon, dan gaat het om een gerechtelijke maatregel die valt te motiveren: het gaat om de opheldering van een ernstig misdrijf in een lopend onderzoek en er zijn geen andere mogelijkheden om dat te doen – tenzij misschien een strenge identiteitscontrole van iedereen op dat plein, maar dat lijkt me een grotere inbreuk op de privacy dan die gezichtsherkenning.'

'We kunnen de evolutie moeilijk tegenhouden, wel zo goed mogelijk omkaderen en controleren. Net daar knelt soms nog het schoentje'

FRANK SCHUERMANS Controleorgaan op de Politie Informatie (COC)

Dan nog blijft het de vraag of er geen regels overtreden worden door, al is het maar heel kortstondig, een databank uit te bouwen van gescande personen. Precies dát soort onduidelijkheden maakt van gezichtsherkenning door veiligheidsdiensten een donker grijze zone.

Valsposities

Ontslagnemend minister van Binnenlandse Zaken Pieter De Crem (CD&V) is alvast van plan om via een wetswijziging het proefproject in Zaventem opnieuw te laten lopen. Meer nog: in het parlement noemde hij gezichtsherkenning, naar aanleiding van een vraag over het project, ‘essentieel om de samenleving te beschermen tegen terrorisme en georganiseerde misdaad’.

Maar die ‘essentiële’ methode is niet zaligmakend: ‘De mensen die je écht wilt vinden, weten hoe ze zulke software kunnen vermijden’, zegt Bart Preneel, computerwetenschapper aan de KU Leuven. ‘Ik verwacht zelfs een soort “wapenwedloop” tussen de ontwikkelaars van de technologie en de mensen die ze willen ontlopen, door telkens een andere manier van vermommen te zoeken.’

Behalve die praktische obstakels is de technologie op zich niet feilloos. ‘Stel dat ze in Zaventem honderd keer per dag ten onrechte een terrorist herkennen en er is één persoon die dat moet controleren, dan zou de politie daar waarschijnlijk heel tevreden mee zijn’, zegt Preneel. ‘Maar voor die honderd mensen is dat wel knap vervelend.’

Het risico dat je verkeerdelijk gecontroleerd wordt, is een van de pijnpunten van het systeem. Bij mensen met een donkere huidskleur komen valsposities nog vaker voor, omdat de algoritmes getraind worden met foto’s van blanken. Daar komt nog bij dat niet elke camera zomaar te gebruiken is. ‘Ze moeten ongeveer ter hoogte van het gezicht hangen en je mag niet meer dan twintig graden naar links of naar rechts kijken’, zegt Pieter-Jan Machtelinckx van het beveiligingsbedrijf RTS. ‘De resolutie speelt ook een rol.’

Zeker in België moet ook rekening worden gehouden met de beperkte technische capaciteiten van de politie. ‘Die werkt met totaal verouderde datasystemen’, zegt Frank Schuermans. ‘De Algemene Nationale Gegevensbank (*de belangrijkste politiedatabank, red.*) heeft technologie uit de jaren 2000. Ik begrijp dat er wordt gezocht naar manieren om de politie performanter te maken, maar dat kan niet zonder een goede discussie in het parlement.’

Overdosis surveillance



Mark Coeckelbergh is technologie-filosoof aan de Universiteit van Wenen en maakt deel uit van de AI-expertengroep die de Europese Commissie adviseert over dit soort zaken. Hij vindt het gebruik van gezichtsherkenning gerechtvaardigd 'als er geen enkele andere manier is om veiligheid te garanderen'. Maar daarbij moeten mensen minstens worden ingelicht dat de technologie gebruikt wordt, én dat gebruik moet worden beperkt in tijd en locatie. 'Een algemene toepassing is heel gevaarlijk. Nu hebben we

herkenning van nummerplaten op de weg, met wat bijkomende technologie kun je daar ook gezichtsherkenning toepassen. Dat lijkt me een overdosis surveillantie die niet gerechtvaardigd is.'

'Er is een sluipende voortschrijding van de technologie, zodat we er langzamerhand aan wennen. Maar uiteindelijk dreigen we wel af te glijden naar een surveillantiestaat. Het is belangrijk dat we als burger "stop" durven te zeggen, en er een maatschappelijk debat over voeren'.

Wat met privaat gebruik?

Briefcam en dergelijke software worden ook door winkelcentra en bedrijven gebruikt. In Europa mag daarbij in principe de **gezichtsherkenning op publieke plaatsen niet worden geactiveerd**: de GDPR-privacywetgeving legt heel strenge voorwaarden op aan het gebruik van die technologie. Zonder uitdrukkelijke toestemming van ieder die eraan wordt onderworpen, kan het volgens de meeste experts niet. (*dod*)