nrc.nl

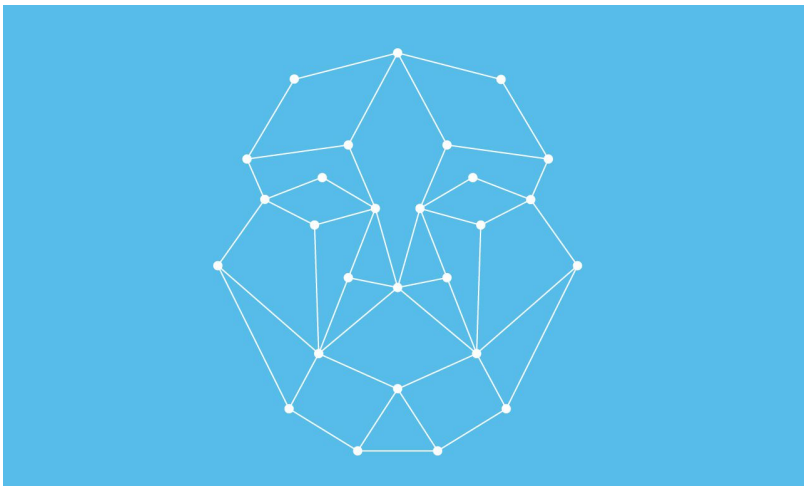
opinie

Gezichtsherkenning is een doos van Pandora

14 januari 2019

Leestijd 2 minuten

Technologie Geautomatiseerde gezichtsherkenning moet streng gereguleerd worden, betoogt *Berber Brouwer*. Anders is het straks te laat.



Studio NRC

Eind december 2018 kwam in het nieuws dat de gemeente Beijing gezichtsherkenning

gaat inzetten om illegale verhuur van sociale woningen te bestrijden. ‘Slimme sloten’ met biometrische camera’s zijn in staat om huurders te herkennen en onbekenden buiten te sluiten. Volgens de *South China Morning Post* maakt de Chinese overheid steeds vaker gebruik van camera’s met gezichtsherkenning om het gedrag van burgers te controleren.

Berber Brouwer is advocaat bij Brouwer & Law

Dit nieuws lijkt tot weinig beroering te hebben geleid. Intussen worden tools met gezichtsherkenning in ons dagelijks leven steeds gewoner, zoals gezichtsherkenning in foto’s op sociale media of de functie ‘Face ID’op de nieuwe iPhone. Deze toepassingen lijken onschuldig, maar de privacyrisico’s van deze technologie zijn ongekend groot.

De Nederlandse overheid start in 2020 een verkennend onderzoek naar de toepassing van automatische gezichtsherkenning voor identificatiedoeleinden. Door de politie wordt al gebruik gemaakt van gezichtsherkenning voor opsporing van verdachten. Dit zijn eerste stappen naar ongetwijfeld steeds ruimere inzet van gezichtsherkenningstechnieken door de overheid. Ervaring leert dat, in het belang van veiligheid en bestrijding van criminaliteit, privacy hierbij altijd het onderspit delft. Het risico op misbruik van verzamelde gegevens wordt weggewuifd met toezeggingen over zorgvuldig gebruik. Die bestaan wellicht op papier, maar beschermen onvoldoende tegen overheden en bedrijven die ons leven al volledig zijn binnengedrongen.

Eind 2017 werd door vooraanstaande wetenschappers gewaarschuwd voor zogenaamde ‘*slaughterbots*’ in een extreem beangstigende video die laat zien hoe voorgeprogrammeerde minidrones met gezichtsherkenning in staat

zijn menselijke doelwitten op te sporen en uit te schakelen met een explosieve lading. Deze autonoom opererende 'zwermdrones' zijn in precisieaanvallen effectiever dan een mens ooit zal kunnen zijn. De video is nauwelijks sciencefiction: door de combinatie van bestaande technologieën is de mens nu al in staat deze *killer drones* te maken.

Het inschakelen van een menselijk moordcommando om een Khashoggi of Ahmad Mola Nissi (een Iraanse activist die in Nederland werd geliquideerd) uit te schakelen is dan in de toekomst niet meer nodig. Iedere dictator, terreurgroepering of topcrimineel zal in de toekomst over deze technologie kunnen beschikken wanneer niet nu op internationaal niveau afspraken worden gemaakt.

Dissidenten uitschakelen zal nog nooit zo eenvoudig zijn geweest, zullen we ontdekken

Voorstanders zullen zeggen dat met gezichtsherkenning veel goede dingen gedaan kunnen worden. Dat is ongetwijfeld het geval. Maar de gevaren zijn minstens zo groot. Gezichtsherkenning biedt ongekende mogelijkheden om het gedrag van burgers te controleren. Wanneer camerasystemen met gezichtsherkenning opnames maken op iedere straathoek wordt een laatste slag toegebracht aan het recht op anonimiteit. Bedenk ook dat een groot deel van de wereldbevolking leeft onder autoritaire regimes of dictaturen met weinig waardering voor dissidente geluiden.

Technologie die per definitie vergaand ingrijpt in grondrechten zou streng gereguleerd moeten worden, zowel in de publieke als private sector. De nieuwe Europese privacyverordening (de AVG) en de Nederlandse uitvoeringswet bevatten een beginselverbod op het verzamelen van biometrische gegevens, maar laten nog steeds veel ruimte aan overheden en bedrijfsleven voor toepassing van automatische gezichtsherkenning.

Zelfs vanuit het bedrijfsleven komt nu de roep om regulering vanwege de

risico's die zijn verbonden aan deze technologie. Vorige jaar werd door de juridisch directeur van Microsoft, Brad Smith, opgeroepen tot overheidsregulering van automatische gezichtsherkenning, omdat mensenrechten in het gedrang komen bij misbruik. Ook als robots ons niet fysiek vernietigen (waarvoor Stephen Hawking waarschuwde in 2014) zal de mens spiritueel ten onder gaan wanneer privacy niet meer bestaat, nagenoeg volledige controle door overheden mogelijk is en sociale of politieke tegengeluiden niet meer gehoord worden uit angst voor represailles.

Wanneer we nu geen actie ondernemen en deze technologie ons leven laten binnendringen, is het straks te laat de doos van Pandora te sluiten. Bij regulering zou het uitgangspunt moeten zijn dat privacybezwaren in beginsel altijd doorslaggevend zijn.