Ministerie van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Datum 20 november 2019
Onderwerp Waarborgen en kaders bij gebruik gezichtsherkenningstechnologie

Ons kenmerk
2747528

Gezichtsherkenningstechnologie en andere technologieën die gebruik maken van biometrische gegevens kunnen bijdragen aan de veiligheid in ons land. Of het nu gaat om de beveiliging van gevoelige overheidslocaties, vitale infrastructuur of de beveiliging van individuele burgers. Gezichtsherkenning is niet nieuw. Al tientallen jaren vergelijkt de politie met het menselijk oog gelaatsafbeeldingen. Dat is een arbeidsintensief en tijdrovend proces. Met de enorme toename van het beschikbare beeldmateriaal (het referentiebestand van de politie bevat miljoenen afbeeldingen) is handmatige vergelijking bijna onbegonnen werk. Geautomatiseerde gezichtsherkenning is daarom noodzakelijk voor de taakuitvoering van de politie. Om te voorkomen dat de inzet van deze techniek in onze samenleving tot ongewenste effecten leidt, is het belangrijk dat de bestaande waarborgen tegen de risico's en bij de toepassing van de techniek bij de tijd worden gebracht.

Tijdens het Algemeen Overleg Nationale Veiligheid en Crisisbeheersing van 20 juni 2019 heb ik uw Kamer toegezegd over een aantal aspecten een brief te sturen. Hiermee beantwoord ik tevens de gestelde vragen uit het VAO van 25 juni en het AO van 14 november jl. Daarbij ga ik in op de kaders die specifiek zien op de politie en nationale veiligheid. In algemene zin valt de bescherming van de rechten van burgers, waaronder de privacy regelgeving zoals de AVP en de WPG, onder de verantwoordelijkheid van de minister voor Rechtsbescherming.

Tevens stelde uw Kamer vragen over de aanwezigheid van gezichtsherkennings-systemen afkomstig van de leveranciers Hikvision en Dahua. Apparatuur van deze leveranciers worden zowel aan bedrijven als particulieren verkocht. De overheid houdt geen zicht op deze verkoop. Het is dan ook niet mogelijk om een uitspraak te doen over het aantal camera's van deze twee leveranciers in Nederland.

De werking van gezichtsherkenningstechnologie
Het maken van camerabeelden en het gebruiken van gezichtsherkennings-technologie staan los van elkaar. Gelaatsafbeeldingen worden gemaakt met (gewone) camera's. De camera zelf herkent geen gezichten. Die gelaatsafbeelding kan vervolgens worden geïmporteerd in een gezichtsherkenningssysteem dat de afbeelding analyseert en vergelijkt met andere gelaatsafbeeldingen. Het gaat dus om twee los van elkaar staande processen: het maken (verkrijgen) van de

afbeelding en het uitvoeren van de gezichtsvergelijking. Deze twee processen vallen ieder onder een ander wettelijk regime. Er bestaan overigens wel geïntegreerde systemen die de gemaakte afbeelding direct analyseren en vergelijken.

Er zijn verschillende typen toepassingen van gezichtsherkenningstechnologie. Ik noem twee veelvoorkomende typen. In de eerste plaats het gebruik van gezichtsherkenningstechnologie voor toegang tot een fysieke plaats, zoals een gebouw, of toegang tot een apparaat. De technologie kijkt dan of een gezicht overeenkomt met een referentie bestand van iemand die toegangsrecht heeft. In de tweede plaats het gebruik van gezichtsherkenningstechnologie om onbekende personen te herkennen. Bijvoorbeeld naar aanleiding van een met een bewakingscamera gefilmd strafbaar feit. De personen die zichtbaar zijn op de beelden kunnen worden vergeleken met de gelaatsafbeeldingen van verdachten en veroordeelden (waarvan de identiteit wel bekend is) waar de politie over beschikt.

Bij het toepassen van gezichtsherkenningstechnologie is er een goede gelaatsafbeelding nodig van de persoon van wie de mogelijke identiteit moet worden vastgesteld. Elementen als de camerahoek en de lichtomstandigheden zijn van invloed op de bruikbaarheid van een afbeelding. Dit is bij toegangscontrole evident eenvoudiger dan in het opsporingsdomein waar de afbeeldingen vaak niet onder ideale omstandigheden zijn gemaakt.

Vooropgesteld moet worden dat de techniek geen oordeel kan geven dat de personen op de te bestuderen afbeelding met 100% zekerheid dezelfde is als die van het referentiebestand. Zover is de techniek niet.
Van zowel de te vergelijken gelaatsafbeelding als van de gelaatsafbeeldingen in het referentiebestand worden bepaalde biometrische kenmerken vastgesteld. Deze kenmerken worden geautomatiseerd met elkaar vergeleken. Het systeem genereert vervolgens een schaalscore die aangeeft in welke mate de technische biometrische kenmerken van de verdachte overeenkomen met de gelaatsafbeeldingen in het referentiebestand. Deze technische vergelijking geschiedt sneller (enkele milliseconden) dan een menselijke vergelijking.

Bij de politie is het proces zo ingericht dat na het opleveren van de scores getrainde menselijke experts een vergelijkingsproces uitvoeren. Een expert beoordeelt of er tussen de kandidaten, in de door het systeem geproduceerde kandidatenlijst, een match zit. Deze kijkt enerzijds naar het algemene beeld: komen de personen op de twee afbeeldingen voor menselijke ogen gelijkend over? Dit op basis van algemene morfologische overeenkomsten zoals de vorm van de neus, lippen, oren etc. Als er een mogelijke match wordt geconstateerd wordt de gelaatsafbeelding uit het onderzoek én alleen de mogelijke gelaatsafbeelding van de match doorgezet naar twee andere experts. De twee andere experts beoordelen de mate van overeenkomst of verschil van gelaat tussen de twee afbeeldingen. Deze kijken zeer gericht naar de morfologische details, bijvoorbeeld de vorm van een oor of andere specifieke kenmerken. Zij moeten op basis van dit onderzoek, onafhankelijk van elkaar, een conclusie geven uit een vooraf vastgestelde standaardlijst met conclusies. De meest vergaande conclusie is dat er ‘veel overeenkomsten’ zijn tussen de gelaatsafbeelding van de verdachte en een gelaatsafbeelding uit het referentiebestand. Ook de experts geven dus niet de (stellige) conclusie ‘het is dezelfde persoon’. De procedure is zo

ingericht dat het risico op *false positives*[1] zoveel mogelijk wordt geminimaliseerd, om zo de rechten van de betrokkenen zoveel mogelijk te beschermen. Zo wordt bij een ongelijke conclusie van de twee experts altijd de meest conservatieve conclusie gerapporteerd als eindconclusie. In mijn antwoord op Kamervragen[2 en 3] ben ik nader in gegaan op het gebruik van deze technologie voor de opsporing.

Juridisch kader en privacy bij politie

In onze democratische rechtsorde en omwille van onze nationale veiligheid dient het gebruik van technologieën als gezichtsherkenningstechnologie onderworpen te zijn aan duidelijke kaders. De bescherming van de persoonlijke levenssfeer is immers een grondrecht. Inbreuk op dat grondrecht – en het vastleggen van iemand gelaat is dat - is alleen toegestaan als aan een aantal wettelijke waarborgen wordt voldaan. Het gegevensbeschermingsrecht is in dit verband een belangrijk juridisch stelsel, dat geldt voor zowel de AVG als de WPG waar het om het politiedomein gaat. Vanuit zijn verantwoordelijkheid voor deze kaders als ook voor de normering van de rechten van burgers heeft de minister voor Rechtsbescherming reeds een rechtsverkennend onderzoek uitgezet bij het WODC op gezichtsherkenning zover dit waarborgen voor de privacy tussen burgers onderling en tussen burgers en bedrijven betreft (de horizontale privacy). Het rapport zal begin volgend jaar worden uitgebracht en zal tevens aanleiding zijn om ook de waarborgen bij verhouding tussen overheid en burger (verticale privacy) op dit gebied te bezien.

Voor de politie geldt het onderstaande stelsel. In het Wetboek van Strafvordering zijn grondslagen opgenomen voor het verkrijgen van gegevens, zoals afbeeldingen en camerabeelden. De Wpg biedt de grondslag en nadere regulering voor het verwerken van deze gegevens. Bij de toepassing van gezichtsherkenningstechnologie wordt gebruik gemaakt van biometrische gegevens. Biometrische gegevens zijn bijzondere persoonsgegevens waarvoor strengere regels gelden. De politie mag deze gegevens alleen verwerken als dit onvermijdelijk is voor het doel van de verwerking en in aanvulling op het verwerken van andere politiegegevens over de betreffende persoon. Ook is het op grond van de Wpg niet toegestaan om op basis van persoonsgegevens (vol)automatisch te besluiten zonder menselijke tussenkomst[4]. Dit beperkt de mogelijkheden voor de toepassing van gezichtsherkenningstechnologie in het politiedomein tot die gevallen waar dat onvermijdelijk is.

Hiernaast gelden verplichtingen ten aanzien van informatiebeveiliging. Iedere verantwoordelijke voor gegevensverwerking is uit hoofde van informatiebeveiliging verplicht om technische en organisatorische maatregelen te treffen. Dat geldt met name voor de toepassing van gezichtsherkennings-technologie waarvoor, door het verwerken van biometrische gegevens, een extra streng regime geldt[5].

---

[1] Er is sprake van een false positive wanneer ten onrechte de conclusie wordt getrokken dat een gezicht op een afbeelding gelijk is aan het gezicht op een betreffende afbeelding uit het referentiebestand. Bij een false negative wordt ten onrechte de conclusie getrokken dat een gezicht op een afbeelding niet gelijk is aan het gezicht op een betreffende afbeelding uit het referentiebestand.

[2] Aanhangsel van de Handelingen, vergaderjaar 2018-2019, nr. 3932

[3] Aanhangsel van de Handelingen, vergaderjaar 2019-2020, nr. 584

[4] Wpg, artikel 7a

[5] Wpg, artikel 4a en 5

In het debat in juni van dit jaar is kort stil gestaan bij de vraag of de inzet van gezichtsherkenningstechnologie opweegt tegen de nadelen in termen van privacy en burgerrechten. In dat kader wijs ik op de wijze waarop gezichtsherkenning binnen de opsporing plaatsvindt. Er worden afbeeldingen gebruikt die rechtmatig, al dan niet middels de inzet van bijzondere opsporingsmiddelen, zijn verkregen. Dat kan een beeld zijn uit een bewakingscamera of een op een andere wijze gemaakt beeld. Die worden dan achteraf, en alleen na een concrete aanleiding, vergeleken met een referentiebestand op de hierboven beschreven wijze. Voor de taakuitvoering van de Nederlandse politie is er dus ook geen sprake van een systematische inzet van camera's die geïntegreerde gezichtsherkennings-technologie toepassen.

In het debat op 20 juni gaf mevrouw Buitenweg aan dat zij zich vooral zorgen maakt over het gebruik van camera's waarbij mensen continu in kaart worden gebracht, en de invloed op onze vrije samenleving. Ik begrijp die zorgen. We kennen, met name uit het buitenland, de zorgwekkende berichtgeving over het gebruik van gezichtsherkenningstechnologie door overheden voor doeleinden die in strijd lijken te zijn met onze normen van recht en vrijheid van burgers. Ik benadruk nogmaals dat de wijze waarop in Nederland gezichtsherkenning wordt ingezet ten behoeve van de taakuitvoering van de Nederlandse politie altijd in overeenstemming moet zijn met onze rechtsstaat.

Tijdens het AO Nationale Veiligheid van 14 november jl. wees mevrouw Buitenweg mij er op dat ik in de beantwoording van de Kamervragen over de gezichtsherkenning heb vermeld dat de politie gebruik maakt van het gezichtsherkenningssysteem CATCH, terwijl ik tijdens het AO Nationale Veiligheid van 20 juni verklaarde dat dergelijke techniek op dit moment nog niet door onze diensten wordt gebruikt. Hier is sprake van een misverstand. In de discussie op 20 juni ging het niet om een systeem als CATCH, maar – zoals in de voorgaande alinea ook staat - over 'live' gezichtsherkenning die gekoppeld is aan een breed netwerk van camera's die mensen zonder aanleiding op de openbare weg filmen, identificeren of 'taggen' en vervolgens voor opsporing of handhaving gebruikt kan worden. Dergelijke systemen worden niet door onze diensten gebruikt.

Toekomstige inzet van gezichtsherkenningstechnologie
Ik sta open voor een verdere ontwikkeling van deze technologie. Om de kennis en reeds aanwezige ervaring te bundelen is dan ook al enige tijd geleden aan de politie opdracht gegeven te komen tot de vorming van een Centrum voor Biometrie ten behoeve van het hele ministerie van Justitie en Veiligheid. Bij de toekomstige inzet van gezichtsherkenningstechnologie zal veel afhangen van de wijze van inzet. Het gaat dan niet om het enkele feit dat er gezichtsherkenningstechnologie wordt ingezet, maar om hoe dat wordt gedaan en welke waarborgen worden ingebouwd om op een zorgvuldige wijze om te gaan met de inzet en de analyse.

In mijn antwoord op de Kamervragen over gezichtsherkenning heb ik uw Kamer geïnformeerd over de onderzoeken van de politie naar een bredere inzet van gezichtsherkenningstechnologie bij de uitvoering van de politietaak[3]. Het is op zich gebruikelijk dat de politie bij de start van experimenten voor zichzelf inzichtelijk maakt wat de wettelijke waarborgen zijn, welke juridische mogelijkheden en beperkingen er zijn en wat de praktische bruikbaarheid is.

Specifiek voor de experimenten met gezichtsherkenningstechnologie, waar door het gebruiken van biometrische gegevens, in beginsel inbreuk wordt gemaakt op de grondrechten van de betrokken personen, vind ik het belangrijk dat er geen twijfel is over het wettelijke kader dat van toepassing is en dat alle noodzakelijke (technische en organisatorische) waarborgen zijn getroffen. Ik vind het ook belangrijk dat er - voordat een nieuwe toepassing van gezichtsherkenningstechnologie bij de politie operationeel wordt ingezet - goed is nagedacht over vragen van juridisch-ethische aard.

De politie heeft voor het operationele gezichtsherkenningssysteem CATCH al voldoende waarborgen getroffen om de persoonlijke levenssfeer van de betrokkenen te beschermen. Ik heb de politie opdracht gegeven om ten aanzien van de toekomstige, andere inzet van gezichtsherkenningstechnologie samen met betrokken partijen inzichtelijk te maken wat het wettelijk kader is, welke waarborgen er zijn getroffen en wat de uitkomst is van de juridisch-ethische toets. Zolang daar geen opgave van is gedaan, mag een desbetreffende experiment niet operationeel worden ingezet.

Nationale veiligheid

Er is specifiek beleid om ook nationale veiligheidsbelangen in het algemeen te borgen. In deze paragraaf zal ik daarop ingaan.

Veel camerabeelden zijn kwetsbaar voor digitale spionage. Bij misbruik van camerabeelden door kwaadwillende (statelijke) actoren kunnen zich, naast privacyrisico's, ook nationale veiligheidsrisico's voordoen. Informatie zoals de biometrische gegevens van medewerkers of bestuurders van overheidsinstellingen of vitale bedrijven is gevoelig. Zolang camerasystemen kwetsbaar zijn voor digitale spionage, is de dreiging voor een belangrijk deel gerelateerd aan alle statelijke actoren met een offensief cyberprogramma tegen Nederland. De kans op dergelijk misbruik wordt groter wanneer beelden op systemen worden opgeslagen die aan het internet zijn gekoppeld. Risico's voor de nationale veiligheid manifesteren zich met name op plekken die overeenkomen met gekende inlichtingenbehoeften zoals bijvoorbeeld gebouwen van de Rijksoverheid en overheidsinstituten.

Zoals ik in deze brief al benadrukte staat gezichtsherkenningstechnologie vaak los van de camera die de beelden opneemt. Wanneer beelden worden vergaard die voldoende kwaliteit hebben om biometrische kenmerken te onderscheiden, kan een derde dus ook eigen gezichtsherkenningstechnologie gebruiken.

De infrastructuur van camerabewaking en aanverwante gezichtsherkennings-technologie zorgt - vanwege de frequente koppeling aan internet - ervoor dat de risico's niet noodzakelijkerwijs beperkt zijn tot een bepaalde leverancier. Slecht beveiligde en beheerde camerabewakingssystemen kunnen, zelfs zonder kennis van 'backdoors', door statelijke actoren gecompromitteerd worden. Dat maakt de huidige kwetsbaarheid dus voor een aanzienlijk deel leverancier neutraal.

Worden maatregelen genomen tegen digitale spionage op afstand, dan komt daar bovenop dat leveranciers uit bepaalde landen via nationale wet- en regelgeving gedwongen kunnen worden tot medewerking aan inlichtingenactiviteiten. De risico's voor de nationale veiligheid worden verder vergroot als het landen betreft die een offensief cyberprogramma voeren tegen de Nederlandse belangen en wanneer technische mogelijkheden om de veiligheidsrisico's te beschermen niet voorhanden zijn.

Het kabinet monitort risico's voor de nationale veiligheid en intervenieert waar nodig om deze risico's beheersbaar te maken. Met betrekking tot dit vraagstuk is het overheidsbeleid dat bij de aanschaf en installatie van beveiligingsapparatuur nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van beveiligingsproducten en hieraan gerelateerde diensten. Bij de aanschaf van gevoelige apparatuur zal volgens dit beleid bij aanschaf en implementatie rekening worden gehouden met zowel eventuele risico's in relatie tot de leverancier als met het concrete gebruik van de systemen, bijvoorbeeld waar het gaat om de controle op toegang tot het systeem door derden. Eind vorig jaar heeft het Kabinet een verscherpt inkoop en aanbestedingsbeleid ten aanzien van nationale veiligheidsrisico's geïmplementeerd alsmede een instrumentarium om dit beleid te ondersteunen. Dit instrumentarium wordt ook ter beschikking gesteld aan bedrijven en organisaties uit vitale sectoren en medeoverheden.

Ten aanzien van beveiligingssystemen bij de Rijksoverheid geldt daarnaast ook het Normenkader Beveiliging Rijkskantoren (NKBR). Hieruit volgt dat de beveiligingssystemen logisch en fysiek gescheiden in het netwerk opgenomen dienen te zijn ten opzichte van andere ICT-voorzieningen. In principe is er een aparte techniekruimte beveiliging waarin de beveiligingssystemen worden geplaatst. Daarnaast kan het noodzakelijk zijn om elders in het gebouw onderdelen van een beveiligingssysteem in een beveiligde ruimte te plaatsen.

Verder gelden voor het gebruik van deze diensten en producten in algemene zin, de reguliere regels ten aanzien van privacybescherming zoals ik eerder in deze brief reeds heb aangegeven.

Afweging kosten en veiligheid
In het AO heeft uw Kamer ook vragen gesteld over de wijze waarop de afweging tussen kosten en veiligheid wordt gemaakt. Bij elke casus wordt bezien hoe risico's voor de nationale veiligheid beheersbaar kunnen worden gemaakt. Hierbij wordt gezocht naar een proportionele aanpak, waarin de financiële en economische impact van de verschillende beheersmaatregelen wordt meegewogen. Uitgangspunt blijft dat nationale veiligheidsrisico's beheersbaar zijn. Het implementeren van maatregelen kan betekenen dat er meer kosten moeten worden gemaakt. Per casus kan deze afweging anders uitvallen. In het genoemde inkoop- en aanbestedingsbeleid en het bijbehorende instrumentarium worden nationale veiligheidsoverwegingen integraal meegenomen.

Toepassing in acute veiligheidssituaties
In zeer ernstige gevallen, zoals in het tijdens het VAO van 25 juni 2019 geschetste voorbeeld van een vluchtende terrorist die via onze binnengrenzen reist, zou wellicht een mobiel camerasysteem met gezichtsherkenningstechnologie aan de Nederlands-Belgische of Nederlands-Duitse grens kunnen worden geplaatst. Met de huidige stand van de techniek is het nodig dat voertuigen die de grens passeren worden gestopt, waarna er van de inzittenden een gelaatsafbeelding wordt gemaakt. De gezichtsherkenningstechnologie wordt dan gebruikt om snel vast te stellen of er een mogelijke match is. Technisch is een dergelijke toepassing dus mogelijk. En zodra de techniek een stap verder is, is het waarschijnlijk niet meer nodig om de voertuigen te laten stoppen. Juridisch is het op dit moment niet mogelijk. Bovendien meldde ik eerder in deze brief dat een structurele inzet van een breed vertakt, realtime gezichtsherkenningstechnologie,

waarbij mensen continu en overal in kaart worden gebracht, niet past bij de samenleving die ik voor sta.

De Minister van Justitie en Veiligheid

Datum
20 november 2019

Ons kenmerk
2747528

Ferd Grapperhaus