Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

770

Vragen van de leden **Kathmann**, **Lahlah** en **Mutluer** (allen GroenLinks-PvdA) aan de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie en Veiligheid en de Staatssecretarissen van Justitie en Veiligheid en van Binnenlandse Zaken en Koninkrijksrelaties over *gezichtsherkenning bij de politie* (ingezonden 23 oktober 2024).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 9 december 2024).

Vraag 1
Bent u bekend met de briefing «In beeld bij de politie: camerasurveillance bij vreedzaam protest in Nederland» van Amnesty International?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u dit rapport zo spoedig mogelijk voorzien van een appreciatie? Kunt u daarbij expliciet reageren op de afzonderlijke aanbevelingen?

Antwoord 2
Mijn reactie op de aanbevelingen van Amnesty International volgt in het eerstvolgende halfjaarbericht politie van december 2024.

Vraag 3
Bent u het eens met de mening dat u uiterst terughoudend dient te zijn met de inzet van camerasurveillance en gezichtsherkenning bij vreedzame demonstraties?

[1] Amnesty International, 16 oktober 2024, «Camerasurveillance door politie moet aan banden worden gelegd» (https://www.amnesty.nl/actueel/camera-surveillance-door-politie-moet-aan-banden-worden-gelegd).

ah-tk-20242025-770
ISSN 0921 - 7398
's-Gravenhage 2024

Antwoord 3
Allereerst wil ik benadrukken dat de politie geen realtime gezichtsherkenningstechnologie inzet bij demonstraties om demonstranten te identificeren. Enkel wanneer sprake is van strafbare feiten kan door de politie achteraf gezichtsherkenningstechnologie worden ingezet om verdachten te identificeren.
Ik ben me er goed van bewust dat het gebruik van camera's een inbreuk vormt op de privacy van de burger en dus voorzien moet zijn bij wet, een legitiem doel moet dienen en noodzakelijk moet zijn in een democratische samenleving. Gelet op die inbreuk wordt de inzet goed overwogen. Voorafgaand aan een demonstratie wordt in de lokale driehoek een risicoafweging gemaakt op basis waarvan de politie-inzet wordt bepaald. Daarin wordt onder andere gekeken naar de complexiteit van een demonstratie en het risico op ongeregeldheden.
Cameratoezicht wordt ingezet om voldoende zicht te hebben op de demonstratie om zo te kunnen zorgen voor een ordelijk en veilig verloop ervan. Denk aan het voorkomen van onveilige (verkeers)situaties en het tijdig in kunnen grijpen als een groep/groepen de demonstratie willen verstoren. De inzet van camera's is zeker niet standaard en vindt bij een klein deel van alle demonstraties plaats. Voor de goede orde: de politie doet niet aan biometrische surveillance.

Vraag 4
Deelt u de mening dat het inzetten van camerasurveillance bij vreedzame demonstraties een onwenselijk afschrikkend effect kan hebben voor het uitoefenen van dit grondrecht?

Antwoord 4
Ik ben me ervan bewust dat mensen het niet prettig kunnen vinden om gefilmd te worden. Mogelijk passen zij zelfs hun gedrag aan, bijvoorbeeld door af te zien van deelname aan een demonstratie. Dit zogenaamde «chilling effect» wordt niet licht bezien, en wordt meegewogen in het besluit om camera's al dan niet in te zetten. Voor de goede orde: de politie doet niet aan biometrische surveillance.

Vraag 5
Vindt u ook dat adequaat toezicht op het gebruik van camerasurveillance en gezichtsherkenningstechnologie een randvoorwaarde is om het te mogen gebruiken? Kunt u onderbouwen dat de Autoriteit Persoonsgegevens voldoende is uitgerust om hierop toe te zien?

Antwoord 5
In de brief van 30 september jl. naar aanleiding van de motie van het lid Kathmann over het gebruik van gezichtsherkenningstechnologie heeft het kabinet de onderliggende zorgen van de motie onderschreven en aangegeven dat er heldere wettelijke kaders noodzakelijk zijn bij de inzet van gezichtsherkenning, toezicht en controle daarop.[2]
De Autoriteit Persoonsgegevens (AP) heeft voldoende expertise en middelen om toezicht te houden op het gebruik van cameratoezicht en gezichtsherkenningstechnologie. De wijze waarop de AP de middelen die hen ter beschikking worden gesteld verdeelt over de afzonderlijke taken is uitsluitend aan de AP, als onafhankelijke toezichthouder.

Vraag 6
In wat voor situaties vindt u het gerechtvaardigd dat de politie gezichtsherkenning gebruikt om demonstranten te identificeren? Binnen welke wettelijke kaders is dit toegestaan?

Antwoord 6
Enkel wanneer er strafbare feiten zijn gepleegd door demonstranten kan de politie achteraf proberen de identiteit van de verdachten te achterhalen door middel van gezichtsherkenningstechnologie. Dit doet de politie door afbeeldingen van de verdachten geautomatiseerd te vergelijken met

[2] Kamerstuk 26 643, nr. 1223

afbeeldingen van veroordeelden en aangehouden verdachten van een strafbaar feit waar minimaal 4 jaar gevangenisstraf voor staat.
De gelaatsafbeelding van een verdachte kan afkomstig zijn van een tijdelijke politiecamera of een bodycam (beide op grond van artikel 3 Politiewet 2012), een gemeentelijke camera (artikel 151c Gemeentewet) of van een particuliere camera (gevorderd op grond van artikel 126nd Wetboek van Strafvordering). Ook kan het zo zijn dat beeldmateriaal door burgers of bedrijven aan de politie wordt verstrekt op grond van de AVG.
De gegevens worden gelet op artikel 3 Wet Politiegegevens (Wpg) slechts verwerkt voor zover dit noodzakelijk is voor de bij of krachtens de Wpg geformuleerde doeleinden. Het omzetten van een gelaatsafbeelding in biometrische kenmerken moet dan ook altijd noodzakelijk zijn voor een van de doeleinden in de Wpg. Bijvoorbeeld voor de uitvoering van de dagelijkse politietaak (artikel 8 Wpg). Met het extraheren van biometrische kenmerken uit een gelaatsafbeelding worden gegevens gecreëerd die die moeten worden aangemerkt als een bijzondere categorie van politiegegevens in de zin van artikel 5 van de Wpg. Dergelijke politiegegevens mogen alleen worden verwerkt voor zover dat onvermijdelijk is voor het doel van de verwerking en in aanvulling op andere politiegegevens. Dit vereist dan ook een extra zware noodzakelijkheidstoets. Ook moeten de gegevens afdoende worden beveiligd. Politiegegevens kunnen geautomatiseerd vergeleken worden op grond van artikel 8, lid 2 en artikel 11, lid 1 en 2 Wpg. Vergelijking van gelaatsafbeeldingen aan de hand van biometrische kenmerken is daarvan niet uitgesloten.
Er is geen sprake van inzet van gezichtsherkenningstechnologie voor het identificeren van demonstranten. Daarnaast wordt geen gebruik gemaakt van realtime gezichtsherkenningstechnologie.

Vraag 7
Kunt u alle relevante interne protocollen en afwegingskaders voor het inzetten van gezichtsherkenning door de overheid delen met de Kamer?

Antwoord 7
In februari 2023 is de Kamer geïnformeerd over het inzetkader gezichtsherkenningstechnologie dat de politie heeft ontwikkeld.[3] In het tweede halfjaarbericht politie 2023 is de Kamer geïnformeerd over de eerste ervaringen met dit inzetkader.[4]

Vraag 8 en 9
Op welke termijn verwacht u moderne wet- en regelgeving aan de Kamer aan te bieden over de strikte inzet van gezichtsherkenning en geautomatiseerde besluitvorming van de overheid, zoals aangekondigd in het regeerprogramma?[5]
Op welke manieren moet de aangekondigde wet- en regelgeving de bestaande praktijk aanvullen? Waarin schiet wet- en regelgeving momenteel tekort en hoe gaat u deze gebreken nader invullen?

Antwoord 8 en 9
Het voornemen in het regeerprogramma om te zorgen voor passende, moderne wet- en regelgeving op het gebied van gezichtsherkenning wordt uitgewerkt in het kader van de implementatie van de Europese Verordening Kunstmatige Intelligentie (AI-verordening).
De AI-verordening is in augustus 2024 van kracht geworden. Deze verordening verbiedt de inzet van realtime gezichtsherkenningstechnologie in de openbare ruimte met het oog op de rechtshandhaving. Uitzonderingen op dat verbod zijn mogelijk als daar nationale wetgeving voor wordt gecreëerd. Het Ministerie van Justitie en Veiligheid onderzoekt nu of dat wenselijk en noodzakelijk is. Als onderdeel van dat traject wordt ook gekeken naar het steviger wettelijk borgen van de huidige toepassing van deze technologie (niet real time) door de politie. Dit traject bevindt zich in een verkennende fase.

---

[3] Kamerstukken II, vergaderjaar 2022-2023, 29 629, 32 761, nr. 1156
[4] Kamerstukken II, vergaderjaar 2023-2024, 29 628, nr. 1193
[5] Regeerprogramma. Uitwerking van het hoofdlijnenakkoord door het kabinet, 13 september 2024, pagina 88.

In het kader van geautomatiseerde besluitvorming door de overheid is een reflectiedocument «Algoritmische besluitvorming en de Awb» in internetconsultatie gegeven waarop tot en met 31 juli jl. 53 openbare reacties zijn ontvangen. Tijdens de plenaire behandeling van de begroting van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is toegezegd dat de Kamer uiterlijk in het eerste kwartaal van 2025 een brief ontvangt waarin een analyse is opgenomen van de consultatiereacties op het reflectiedocument. In die brief zal nader worden ingegaan op de vraag waarin de wet- en regelgeving momenteel tekortschiet en binnen welke termijn een wetsvoorstel kan worden verwacht.

Vraag 10
Welke technologie(ën) gebruikt Nederland momenteel voor gezichtsherkenning? Kunt u per toepassing aangeven of deze gebruikmaken van een algoritme of kunstmatige intelligentie (AI)? In het geval van AI-toepassingen: kunt u aangeven op welke datasets de modellen getraind zijn?

Antwoord 10
Ik lees uw vraag in de context van het rapport van Amnesty International. Ik beperk me in mijn antwoord tot het gebruik van gezichtsherkenningstechnologie door de politie.
De politie maakt gebruikt van het systeem CATCH. Daarnaast zijn er twee databases: CATCH-strafrecht en CATCH-vreemdelingen. De laatste is de Vreemdelingendatabase die onder de verantwoordelijkheid van de Minister van Asiel en Migratie valt. In de Kamerbrief van november 2019 worden de juridische kaders en waarborgen rondom het gebruik van gezichtsherkenningstechnologie door de politie beschreven en wordt er dieper ingegaan op het gebruik van CATCH-strafrecht.5 In maart 2023 is in antwoord op schriftelijke vragen over CATCH-vreemdelingen uitleg gegeven over de wettelijke grondslag.[6] De algoritmes die CATCH gebruikt zijn niet door de politie getraind. Ze zijn getraind aangekocht.
Momenteel is de politie bezig met het inrichten van een nadere kwaliteitstoets op algoritmen. De aanleiding hiervoor is de AI-verordening. In artikel 6 van deze verordening zijn verplichtingen opgenomen voor hoog-risico AI-systemen. CATCH is in het huidige gebruik door de politie zeer waarschijnlijk aan te merken als een hoog-risico systeem. De verplichtingen en verantwoordelijkheden die hier mee samenhangen treden op 1 augustus 2026 in werking. Dit behelst, ten behoeve van de verscherping en nadere toetsing op de juridische en technische kwaliteit, ook een uitvoeriger bestudering van de initiële datasets waar het model op is gerealiseerd.

Vraag 11
Met welke toepassingen van gezichtsherkenning wordt er momenteel geëxperimenteerd, zoals aangegeven door de vorige Minister van Justitie en Veiligheid in haar antwoorden op vragen van het lid Sneller?[7]

Antwoord 11
In haar antwoord op vragen van het lid Sneller geeft mijn ambtsvoorganger aan dat eventuele experimenten plaats vinden binnen de daarvoor geldende wettelijke bepalingen. Bij het Centrum voor Biometrie van de politie vinden geen experimenten plaats. Bij de toetsingscommissie gezichtsherkenningstechnologie van de politie is geen experiment bekend.

Vraag 12
Deelt u de mening van uw ambtsvoorganger dat nieuwe experimenten met gezichtsherkenning zonder expliciete wettelijke grondslag moeten worden toegestaan? Acht u dit in lijn met de aangenomen motie-Kathmann (Kamerstuk 26 643, nr. 1172), die vraagt om toepassingen altijd van een expliciete grondslag te voorzien en anders te beëindigen?

---

[6] Aanhangsel Handelingen, vergaderjaar 2022-2023, nr. 1943
[7] Aanhangsel Handelingen II, vergaderjaar 2023–2024, nr. 1198.

Antwoord 12
Ik hecht eraan om de mening van mijn ambtsvoorganger in context te lezen. Het ontbreken van een expliciete wettelijke grondslag betekent niet dat er geen wettelijke grondslag bestaat voor de toepassing van een technologie door de politie. Voor de uitleg van die wettelijke grondslag verwijs ik naar mijn antwoord op vraag 6. Als de politie binnen de kaders van onze wetgeving handelt en de voorgeschreven waarborgen treft, zoals het uitvoeren van een gegevensbeschermingseffeceoordeling, dan zie ik geen bezwaren. In dat opzicht deel ik de mening van mijn ambtsvoorganger.
De motie waar u naar verwijst is op verzoek van de indiener aangehouden.[8]
Ik verwijs u voor een reactie op de aangenomen motie 1171 naar de brief van de Staatssecretaris van Justitie en Veiligheid van 9 oktober 2024.[9]

Vraag 13 en 14
Klopt het dat er momenteel geen centraal overzicht is van de plekken en manieren waarop de overheid gezichtsherkenning toepast? Waarom is dit nog niet inzichtelijk gemaakt?[10]
Kunt u met een tijdlijn aangeven hoe u zo snel mogelijk gaat voldoen aan de registratieverplichting van hoogrisico AI-systemen, die per 2026 geldt? Deelt u de mening dat Nederland transparant dient te zijn en hierin vooruit moet lopen op de deadline uit de Europese AI-verordening?

Antwoord 13 en 14
De AI-verordening verplicht de registratie van hoog risico AI-systemen door aanbieders en gebruiksverantwoordelijken van deze systemen in een EU-databank. Deze verplichting geldt per 2 augustus 2026 voor nieuwe hoog risico AI-systemen. Voor hoog risico AI-systemen op het gebied van rechtshandhaving, migratie, asiel en grenstoezichtbeheer vindt registratie plaats in een niet openbaar gedeelte van de databank, die wel toegankelijk is voor toezichthouders. Het kabinet onderschrijft de noodzaak van transparantie over het gebruik van AI-systemen door de overheid. Op nationaal niveau wordt daarom aanvullend invulling gegeven aan deze transparantie middels het algoritmeregister. Met uw Kamer is afgesproken dat voor zover het de Rijksoverheid betreft, ten minste alle hoog risico AI-systemen eind 2025 in het register zijn gepubliceerd. Voor registratie in het algoritmeregister geldt dat publicatie in het register begrensd kan worden door wettelijke of gerechtvaardigde uitzonderingen die van toepassing zijn in het kader van bijvoorbeeld opsporing, rechtshandhaving, defensie of inlichtingenverzameling.

Vraag 15
Welke toetsen gaan vooraf aan het besluit om camerasurveillance bij vreedzame demonstraties in te zetten? Met welke organisaties moeten deze gedeeld worden?

Antwoord 15
Ik wil hier benadrukken dat iedere demonstratie uniek is en een unieke afweging vraagt. Voorafgaand aan een demonstratie wordt binnen de lokale driehoek een risicoafweging gemaakt op basis waarvan de politie-inzet wordt bepaald. Daarin wordt onder andere gekeken naar de complexiteit van een demonstratie en het risico op ongeregeldheden.
Onderdeel van die afweging is dat er geen onnodige inbreuk op de privacy van burgers wordt gemaakt en dat de veiligheid van demonstranten en omstanders wordt gewaarborgd. Cameratoezicht wordt ingezet om voldoende zicht te hebben op de demonstratie om zo te kunnen zorgen voor een ordelijk en veilig verloop ervan. Denk aan het voorkomen van onveilige (verkeers)situaties en het tijdig in kunnen grijpen als een groep/groepen de demonstratie willen verstoren. De inzet van camera's is zeker niet standaard en vindt bij een klein deel van alle demonstraties plaats. Er wordt niet geregistreerd hoe vaak cameratoezicht wordt toegewezen.

---

[8] Handelingen, vergaderjaar 2023-2024, nr. 74, item 15
[9] Kamerstukken II, vergaderjaar 2024-2025, 26 643, nr. 1223
[10] Zoals ook blijkt uit uw Kamerbrief (Kamerstuk 26 643, nr. 1223) over het uitvoeren van de motie-Kathmann (Kamerstuk 26 643, nr. 1172), waarin slechts verwezen wordt naar toekomstige verplichtingen uit de AI-verordening en naar de EU-databank die in 2026 af is.

Vraag 16
Worden alle relevante rapportages en stukken die de toezichthouders nodig hebben om de inzet van gezichtsherkenning te toetsen altijd in volledigheid met hen gedeeld? Kunt u deze vraag ter bevestiging aan de relevante toezichthouder(s) voorleggen en, indien hier niet aan wordt voldaan, alsnog alle stukken met hen delen?

Antwoord 16
Ja. Uit de terugkoppeling die ik heb ontvangen van de politie blijkt niets anders dan volledige medewerking.

Vraag 17
In hoeveel gevallen is de inzet van camerasurveillance bij vreedzame demonstraties, al dan niet in combinatie met gezichtsherkenning, vooraf óf achteraf afgekeurd? Om welke redenen is dit gebeurd?

Antwoord 17
De politie inzet bij demonstraties wordt bepaald door een risicoafweging in de lokale driehoek. Zoals uiteengezet wordt de inzet van cameratoezicht niet licht bezien gelet op die potentiële inbreuk op de privacy van burgers of het zogenaamde «chilling effect» dat kan optreden. Vanzelfsprekend kan een risicoafweging ook leiden tot een negatief besluit over de inzet van camera's. Bijvoorbeeld omdat het voorziene veiligheidsrisico niet opweegt tegen de beschreven inbreuk. Bij de meeste demonstraties wordt dan ook geen gebruik gemaakt van cameratoezicht. Daarnaast kan gezichtsherkenningstechnologie enkel achteraf toegepast worden voor de identificatie van verdachten van strafbare feiten. Bij een vreedzame demonstratie zal dit in de regel niet aan de orde zijn.
Er wordt niet geregistreerd hoe vaak cameratoezicht wordt toe- of afgewezen.

Vraag 18
Welke toetsen gaan vooraf aan het besluit om gezichtsherkenning ter identificatie in te zetten in politieonderzoek? Met welke organisaties moeten deze gedeeld worden?

Antwoord 18
De politie maakt op dit moment alleen gebruik van het systeem CATCH. Ieder voornemen voor een andere toepassing van gezichtsherkenningstechnologie dan CATCH moet worden getoetst door de toetsingscommissie gezichtsherkenningstechnologie van de politie. Die commissie doet dit aan de hand van het inzetkader gezichtsherkenning. Een positief advies van de toetsingscommissie moet voorafgaand aan de operationele inzet worden bekrachtigd door de korpschef.
Indien de politie in het kader van een opsporingszaak beschikt over een gelaatsafbeelding van de verdachte, dan kan de politie trachten de identiteit te achterhalen met behulp van gezichtsherkenningstechnologie. Voor zowel de verkrijging van de verdachtenfoto als voor de verdere verwerking is een wettelijke grondslag nodig. Voor de toepassing van CATCH-Strafrecht voert de betrokken opsporingsambtenaar deze toets uit. In bijzondere gevallen kan als laatste redmiddel gebruik worden gemaakt van de Vreemdelingendatabase (CATCH-vreemdelingen) in het kader van de opsporing. Hiervoor moet de officier van justitie een schriftelijke machtiging van de rechter-commissaris hebben alvorens hij deze informatie kan vorderen, zie voor de eisen artikel 107 zesde lid, Vreemdelingenwet 2000.

Vraag 19
Hoeveel verdachten worden jaarlijks succesvol herkend door het gebruik van gezichtsherkenning? Hoeveel mensen worden jaarlijks aangehouden of ondervraagd op basis van een foutieve match?

Antwoord 19
In 2023 zijn er 1693 gezichtsafbeeldingen van Nederlandse opsporingsonderzoeken aangeboden voor vergelijking. Hiervan bleken 660 gezichtsafbeeldingen niet geschikt voor verdere verwerking. Van de 1033 geschikt bevonden gezichtsafbeeldingen, leidden 424 gezichtsafbeeldingen tot een herkenning. De overige 609 werden niet herkend.

Een herkenning door middel van de inzet van deze technologie én de beoordeling van biometrie-experts levert ondersteunend bewijs op in het onderzoek naar verdachten.

Vraag 20
Welke foutmarges kennen de systemen voor gezichtsherkenning die nu in gebruik zijn? Zijn deze gelijk voor alle huidskleuren en geslachten? Kunt u in een percentage uitdrukken welke foutmarge volgens u acceptabel is?

Antwoord 20
De gebruikte gezichtsherkenningstechnologie genereert een «shortlist» van personen die een zekere mate van gelijkenis vertonen met de persoon op de verdachtenfoto. De uiteindelijke beoordeling wordt uitgevoerd door meerdere, onafhankelijk van elkaar werkende, biometrie-experts. Door dit principe van «human-in-the-loop» is er altijd sprake van menselijke interactie.
De politie is bezig een intern proces op te zetten om, naast de staande processen, een aanvullende kwaliteitstoets op algoritmen te implementeren. Nu kan er nog geen uitspraak worden gedaan naar wat acceptabel is. Rondom de initiële inzet van CATCH is gekeken naar de daartoe beschikbare externe kwaliteitsrapportages. In dit geval van het Amerikaanse National Institute of Standards and Technology (NIST). CATCH is gebaseerd op een model van IDEMIA waar het NIST een evaluatie op heeft uitgevoerd.[11]

Vraag 21
Welke middelen, zoals bodycams en videosurveillanceauto's, mag de politie gebruiken voor camerasurveillance? Met welke regelmaat worden de beelden gebruikt om met gezichtsherkenningstechnologie mensen te identificeren?

Antwoord 21
Camerasurveillance, of cameratoezicht in het Nederlands, is een breed begrip. Daaronder vallen o.a. de volgende vormen: bodycams, drones en helikopters die zijn uitgerust met een camera, videosurveillancewagens, tijdelijke camera's, of vast bevestigde tijdelijke camera's (om tijdelijk een bepaald gebied of bepaalde locatie te monitoren). Ook kan de politie beschikken over de beelden van Openbare orde camera's (op grond van artikel 151c Gemeentewet). ANPR-camera's zijn, hoewel specifiek gericht op het herkennen van voertuigen, ook een vorm van cameratoezicht.
Voor het tweede deel van deze vraag verwijs ik naar mijn antwoord op vraag 19.

Vraag 22
Welke eisen stelt u aan de camera's die voor opsporing en handhaving worden ingezet? Kunt u garanderen dat Nederland geen gebruik maakt van hardware of software die ontwikkeld is in landen met offensieve cyberprogramma's tegen ons land?

Antwoord 22
De politie is bij de aanschaf van technologische middelen gehouden aan de Europese en nationale aanbestedingsregels, zoals de Aanbestedingswet 2012. Het uitgangspunt is dat het gebruik van apparatuur en programmatuur veilig moet zijn en dat eventuele risico's beperkt en/of gemonitord worden. Het risicobeleid ten aanzien van nationale veiligheid bij inkoop en aanbesteding is constant in ontwikkeling en heeft blijvende aandacht van de politie.
Bij de aanschaf en implementatie van apparatuur of programmatuur waarbij risico's optreden voor de nationale veiligheid wordt geanticipeerd op zowel algemene risico's in relatie tot leveranciers, als op specifiekere risico's met betrekking tot het concrete gebruik van de systemen, bijvoorbeeld als het gaat om fysieke of digitale toegang door derden. Per praktijksituatie moet worden bezien of en zo ja, hoe eventuele risico's voor de nationale veiligheid beheersbaar kunnen worden gemaakt. Een belangrijk uitgangspunt hierbij is dat maatregelen die hiertoe genomen worden proportioneel zijn. Er kunnen bijvoorbeeld technische beveiligings- of organisatorische maatregelen worden getroffen binnen de eigen organisatie. Ook kunnen strenge eisen

[11] Online toegankelijk via https://pages.nist.gov/frvt/reportcards/1N/idemia_1.pdf

gesteld worden aan de beveiliging van producten en diensten en kunnen ondernemers gevestigd in bepaalde landen uitgesloten worden van aanbestedingsprocedures.
De politie kan niet garanderen dat er geen gebruik wordt gemaakt van hardware of software die ontwikkeld is in landen met offensieve cyberprogramma's tegen ons land. Dat komt deels omdat de politie niet alle camera's zelf aanschaft. Deels stond de Aanbestedingswet 2012 tot voor kort het niet toe om bepaalde aanbieders uit te sluiten.

Vraag 23
Welke databronnen worden gebruikt als referentiemateriaal bij gezichtsherkenning? Kunt u expliciet maken welke open en gesloten bronnen hiervoor gebruikt mogen worden of mogen worden opgevraagd?

Antwoord 23
De politie maakt voor gezichtsherkenning gebruik van het eerder genoemde systeem CATCH. CATCH kan een gezichtsvergelijking uitvoeren door een verdachtenfoto te vergelijken met referentiemateriaal. Dat referentiemateriaal is opgeslagen in twee bestanden: één met gelaatsafbeeldingen van aangehouden verdachten van een strafbaar feit waarvoor minimaal 4 jaar celstraf staat en van veroordeelden (CATCH Strafrecht) en één met gelaatsafbeeldingen van vreemdelingen (CATCH Vreemdelingen). Slechts in zeer uitzonderlijke gevallen (enkele keren per jaar) kan er worden gekeken of de verdachte voorkomt in de Vreemdelingendatabank. Zie hiervoor ook mijn antwoord op vraag 18.
De grondslag voor het verkrijgen van het referentiemateriaal is artikel 55c Wetboek van strafrecht voor de afbeeldingen van verdachten en veroordeelden. En artikel 107, vijfde lid, van de Vreemdelingenwet 2000 voor de gelaatsafbeeldingen van vreemdelingen.
De politie maakt geen gebruik van open of andere gesloten bronnen bij de operationele inzet van de genoemde CATCH varianten.

Vraag 24
Worden opgeslagen beelden van vreedzame demonstraties gebruikt als referentiemateriaal om verdachten op te sporen, ook als hun vermeende misdrijf niks met de demonstratie te maken heeft?

Antwoord 24
Zoals omschreven in reactie op vraag 23 wordt in de huidige toepassing van gezichtsherkenningstechnologie door de politie geen gebruik gemaakt van beelden van vreedzame demonstraties als referentiemateriaal. Wel kan het voorkomen dat op beeldmateriaal van een demonstratie een strafbaar feit zichtbaar is. In dat geval kan dat beeldmateriaal worden gebruikt als bewijsmateriaal en voor de identificatie van de verdachte. Het maakt hierbij geen verschil of de verdachte wel of niet als demonstrant wordt aangemerkt.

Vraag 25
Welke bewaartermijn hanteert de politie voor beelden van vreedzame demonstraties? Hoe wordt erop toegezien dat de beelden na deze termijn daadwerkelijk worden verwijderd? Heeft de politie op dit moment beelden van vreedzame demonstraties bewaard die reeds vernietigd hadden moeten worden?

Antwoord 25
De Wet politiegegevens (Wpg) en de Gemeentewet regelen de bewaartermijnen. Afgeleid van artikel 151c Gemeentewet bewaart de politie camerabeelden maximaal 28 dagen. Beelden waarop een strafbaar feit zichtbaar is, mogen worden bewaard zolang het opsporingsonderzoek loopt.
Jaarlijks wordt er een interne privacyaudit uitgevoerd (de zogenaamde Wpg-audit). Eens in de 4 jaar wordt er een externe privacyaudit uitgevoerd. Op uw vraag of de politie op dit moment beelden van vreedzame demonstraties bewaart die reeds vernietigd hadden moeten worden, kan de politie in zijn algemeenheid geen uitspraak doen. De procedure is zodanig dat de camerabeelden binnen 28 moeten zijn beoordeeld en er een besluit moet zijn genomen.

Vraag 26
Worden politiebeelden waarvan blijkt dat ze achteraf onrechtmatig verkregen zijn altijd op tijd verwijderd? Waaruit blijkt dit?

Antwoord 26
De betrokken officier van justitie maakt de afweging welk belang het zwaarst weegt: het belang van waarheidsvinding of het belang van de rechten van de op de politiebeelden zichtbare personen. Als blijkt dat de politiebeelden onrechtmatig zijn verkregen, dan kan een rechter besluiten dit niet als bewijs toe te laten. Bij een onrechtmatige inbreuk op de persoonlijke levenssfeer kan dit worden meegewogen in de strafmaat.

Vraag 27
Kunt u deze vragen afzonderlijk van elkaar en zo snel mogelijk beantwoorden?

Antwoord 27
Deze vragen zijn zo goed mogelijk beantwoord, waarvoor het in gevallen wenselijk is ze gezamenlijk te behandelen.