Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Aanhangsel van de Handelingen

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

3932

Vragen van het lid **Verhoeven** (D66) aan de Minister van Justitie en Veiligheid over *het bericht «Gezichtendatabase van politie bevat foto's van 1,3 miljoen mensen»* (ingezonden 25 juli 2019).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Minister voor Rechtsbescherming (ontvangen 11 september 2019) Zie ook Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3606.

Vraag 1
Kent u het bericht «Gezichtendatabase van politie bevat foto's van 1,3 miljoen mensen»?[1]

Antwoord 1
Ja.

Vraag 2 en 4
Wat is de wettelijke grondslag op basis waarvan deze foto's worden bewaard?
Hoe heeft de politie deze foto's verworven? Gebruikt de politie «scraping»-technieken teneinde foto's van onschuldige Nederlanders te vergaren?

Antwoorden 2 en 4
Het genoemde artikel gaat over gelaatsvergelijking met het systeem Catch Strafrecht Verdachte en Veroordeelde (hierna te noemen Catch).
Veel politiebureaus beschikken over een zogenaamde identificatiezuil[2] waarmee onder andere een (frontale) foto van het gezicht en een kopie van het identiteitsbewijs worden gemaakt. De bevoegdheid om deze gelaatsfoto's te nemen van verdachten is neergelegd in artikel 55c, tweede lid, van het Wetboek van Strafvordering (WvSv), dat op 1 oktober 2010 in werking is getreden. Een deel van de bij de politie aanwezige foto's is genomen vóór de inwerkingtreding van artikel 55c WvSv. De bevoegdheid tot het nemen van die (gelaats)foto's was destijds neergelegd in artikel 61a WvSv. De politie maakt geen gebruik van scraping technieken om foto's te vergaren voor Catch.

[1] https://www.nu.nl/tech/5967571/gezichtendatabase-van-politie-bevat-fotos-van-13-miljoen-mensen.html
[2] Staat ook bekend als Basis Voorziening Identiteitvaststelling (BVID) of Progis-zuil.

ah-tk-20182019-3932
ISSN 0921 - 7398
's-Gravenhage 2019

De bij de identificatiezuil gemaakte foto en vingerafdrukken worden automatisch (gelijktijdig) zowel naar de Justitiële Informatiedienst (hierna: Justid) als naar de relevante politiesystemen gestuurd (HAVANK, Catch). De Foto Confrontatie Module (FCM) wordt gebruikt om slachtoffers en getuigen te confronteren met gelaatsfoto's van verdachten. De FCM is al langer in gebruik dan de identificatiezuilen.
In het Besluit identiteitsvaststelling verdachten en veroordeelden (Bivv) zijn de bewaartermijnen voor foto's die worden bewaard in de SKDB vastgelegd. De termijn varieert van 20 tot 80 jaar. De termijn voor het bewaren van politiegegevens is geregeld in de Wet politiegegevens (Wpg) Er zijn dus meerdere bewaartermijnen van toepassing op dezelfde foto. Dit leidt in de praktijk tot onduidelijkheid.
De onduidelijkheid over bewaartermijnen vind ik onwenselijk. Op dit moment is het beter om deze onvolkomenheid in de naleving van de wet te accepteren en genoegen te nemen met de maatregelen van de korpschef om de toegang tot de data te beperken tot het strikt noodzakelijke. Het alsnog voldoen aan de letter van de wet zou alleen kunnen via een grove selectiemethode waardoor ook gegevens worden vernietigd die kunnen bijdragen aan de opsporing in cold case zaken. Het oplossen van deze zaken zal hierdoor ernstig worden belemmerd. Wel hecht ik er belang aan dat er in de praktijk passende waarborgen zijn getroffen om de persoonlijke levenssfeer van betrokkenen te waarborgen[3]. Ik ga hier in het antwoord op vraag 11 nader op in.
Uit de evaluatie[4] van de Wpg en de Wjsg in 2014 bleek al dat politie en justitie op onderdelen niet (kunnen) voldoen aan de wetgeving. Eén van de toentertijd geconstateerde gebreken was dat gegevens in de digitale tijd niet altijd tijdig kunnen worden vernietigd. In mijn aanbiedingsbrief bij die wetsevaluatie heeft mijn ambtsvoorganger al gemeld dat de Wpg (en ook de Wet justitiële en strafvorderlijke gegevens (Wjsg)) zal worden gemoderniseerd. Ik ben momenteel bezig met beleidsvorming ten aanzien van de integrale herziening van deze wetten. Minister Dekker en ik verwachten uw Kamer in het voorjaar van 2020 een brief te sturen met onze beleidsvoornemens op dit punt. Daarin wordt dit onderwerp meegenomen.

Vraag 3
Is er een privacy audit uitgevoerd op de verwerking van deze foto's conform artikel 33 van de wet politiegegevens? Zo ja, bent u bereid deze naar de Kamer te sturen?

Antwoord 3
Bij een audit zoals bedoeld in artikel 33 Wpg wordt gecontroleerd of de politie de Wpg uitvoert overeenkomstig de bij of krachtens deze wet gegeven regels. Tijdens zo'n audit wordt niet gekeken naar specifieke werkwijzen of systemen. De politie laat deze privacyaudit elke vier jaar uitvoeren door een externe onafhankelijke instantie, de Auditdienst Rijk (ADR). De uitkomst van de laatste afgeronde audit is in december 2015 aangeboden aan uw Kamer[5]. Ik verwacht dat ik de uitkomsten van de externe audit 2019 dit najaar aan uw Kamer kan aanbieden.

Vraag 5
Kunt u nader ingaan op het feit dat er van 1,3 miljoen Nederlanders foto's worden bewaard door de politie? Klopt het, dat dit alleen foto's zijn van mensen die zijn verdacht van een misdrijf waar minimaal 4 jaar celstraf op staat? Hoeveel van de 1,3 miljoen mensen zijn daadwerkelijk veroordeeld? Klopt het voorts dat er tussen deze 1,3 miljoen Nederlanders onschuldige mensen zitten die geen misdrijf hebben gepleegd? Om hoeveel onschuldige Nederlanders gaat het?

---

[3] Zie ook mijn brief over aanpak van cold cases, dd. 4 januari 2019 Kamerstuk 29 268, nr. 859.
[4] Kamerstuk 33 842, nr. 2.
[5] Bijlage bij Kamerstuk 33 842, nr. 4.

Antwoord 5
Er zijn foto's opgenomen van 1,3 miljoen personen van verschillende nationaliteiten. Voor de wijze waarop de politie deze verkrijgt en opslaat, verwijs ik naar het antwoord op vraag 4.
De systemen bevatten in hoofdzaak foto's van personen die – op het moment dat de foto werd genomen – werden verdacht van een misdrijf waarvoor voorlopige hechtenis mogelijk is. Een uitzondering hierop doet zich voor als er twijfel bestaat over de identiteit van een verdachte. Op bevel van de (hulp)officier van justitie mogen er dan ook voor lichtere vergrijpen vingerafdrukken en foto's worden genomen. Een tweede uitzondering hierop betreft de foto's die zijn genomen vóór 2010. Die foto's zijn destijds genomen op grond van artikel 61a WvSv. In tegenstelling tot artikel 55c WvSv noemt artikel 61a WvSv niet de voorwaarde dat de persoon minimaal moet worden verdacht van een misdrijf waarvoor voorlopige hechtenis mogelijk is.

Vraag 6
Waarom worden foto's van verdachten die onschuldig blijken, niet verwijderd?

Antwoord 6
Zie mijn antwoord op vraag 2.

Vraag 7
Staan er Nederlanders in de database die nog nooit zijn verdacht van een misdrijf? Zo ja, wat is hier de reden voor?

Antwoord 7
Nee, op grond van artikel 55c WvSv (en vóór de inwerkingtreding van artikel 55c WvSv in 2010 op grond van artikel 61a WvSv) mogen alleen foto's worden gemaakt van verdachten.

Vraag 8
Kunt u een statistisch onderbouwde analyse naar de Kamer sturen over nut en noodzaak van deze database van miljoenen foto's?

Antwoord 8
In het verleden zijn er vele maatregelen getroffen om identiteitsvaststelling in de strafrechtsketen te verbeteren. De Wet identiteitsvaststelling verdachten, veroordeelden en getuigen (Wivv) is daar een voorbeeld van. Uit de wetshistorie blijkt de noodzaak van het instellen van een centrale databank. In de memorie van toelichting[6] wordt de noodzaak onderbouwd aan de hand van de toen beschikbare cijfers[7]. Uit cijfers van de politie blijkt dat onderzoek met Catch in 2018 in ruim 8% van de zaken een herkenning opleverde die heeft geleid tot een aanknopingspunt voor vervolgonderzoek.

Vraag 9
Acht u het proportioneel om van onschuldige Nederlanders een database met foto's aan te leggen?

Antwoord 9
De foto's die worden gemaakt op grond van artikel 55c WvSv (en vóór de inwerkingtreding van artikel 55c WvSv in 2010 op grond van artikel 61a WvSv), worden alleen gemaakt omdat de persoon in kwestie wordt verdacht van een strafbaar feit.

Vraag 10
Waarom is gekozen voor een bewaartermijn van 20 tot 80 jaar? Acht u deze bewaartermijn proportioneel?

Antwoord 10
De bewaartermijn van 20 tot 80 jaar zijn geregeld in het Bivv en gelden voor de foto's die zijn opgenomen in de SKDB.

---

[6] Kamerstuk 31 436, nr. 3
[7] Kamerstuk 31 436, nr. 3, par. 3.

Bij het bewaren van strafrechtelijke gegevens moet er een balans zijn tussen het profijt dat de opsporing en vervolging heeft van deze bewaring en het recht op bescherming van de persoonlijke levenssfeer zoals geregeld in art. 8 EVRM. Hierbij gelden de beginselen van proportionaliteit en subsidiariteit. Ik verwijs kortheidshalve naar de memorie van toelichting bij het wetsvoorstel identiteitsvaststelling verdachten, veroordeelden en getuigen voor een nadere toelichting[8].

Vraag 11
Welke risico's ziet u met betrekking tot de beveiliging van deze database? Wat voor gevolgen voorziet u bij het uitlekken van de database? Wat voor maatregelen zijn er getroffen teneinde dit te voorkomen?

Antwoord 11
Op grond van artikel 4a en artikel 5 Wpg is de politie verplicht om technische en organisatorische maatregelen te treffen om de gegevens te beschermen. De database is beveiligd volgens de gebruikelijke werkwijze van de politie. Een van de reeds getroffen maatregelen betreft de toegankelijkheid van het systeem Catch. Alleen de 30 geautoriseerde experts van het Centrum voor biometrie (onderdeel van het Landelijk Forensisch Service Centrum van de Landelijke eenheid van politie) hebben toegang tot het systeem Catch. Iedere aanvraag wordt in een registratiesysteem bijgehouden. Verder zijn de foto's die de experts beoordelen geanonimiseerd. Omwille van vertrouwelijkheid kan ik geen specifieke uitspraken doen over de getroffen maatregelen.

Vraag 12
Kunt u toelichten op welke manier Nederlandse opsporingsdiensten gezichtsherkenningssoftware gebruiken? Heeft de politie zelf software ontwikkeld of koopt de politie deze software in bij een bedrijf? Zo ja, welk bedrijf levert gezichtsherkenningssoftware aan de politie?

Antwoord 12
De politie en de bijzondere opsporingsdiensten kunnen een aanvraag doen voor het zoeken naar de identiteit van een onbekende persoon door middel van Catch. Catch zoekt op basis van een biometrisch profiel van de kenmerken van het gezicht naar overeenkomsten en genereert een kandidatenlijst van gezichten die technisch het meest op de gezochte afbeelding lijken. Een expert kijkt naar dit resultaat. Als deze expert er van overtuigd is dat er sprake is van voldoende overeenkomst met één van de kandidaten uit de lijst, wordt de match voorgelegd aan twee andere experts die de overeenkomst onafhankelijk van elkaar beoordelen. Als beide experts tot dezelfde conclusie komen, dan wordt die gezamenlijke conclusie als eindconclusie gerapporteerd. Bij een ongelijke conclusie wordt de meest conservatieve conclusie gerapporteerd. Deze rapportage wordt door de politie als aanknopingspunt gebruikt voor vervolgonderzoek.
De politie maakt gebruik van software van het bedrijf IDEMIA. IDEMIA publiceert regelmatig over de doorontwikkeling van deze software. De testresultaten zijn openbaar.

Vraag 13
Hoe vaak wordt deze technologie toegepast? Hoe vindt goedkeuring van het gebruik van deze technologie plaats? Moet een rechter-commissaris toestemming geven voor het gebruik?

Antwoord 13
De politie heeft mij laten weten dat in 2018 door opsporingsinstanties ruim 1300 afbeeldingen ter vergelijking werden aangeboden. De aanvragen betreffen onderzoeken variërend van woninginbraken, overvallen, liquidatie-onderzoeken tot aan terreurzaken. Een deel van de foto's was ongeschikt. Bijvoorbeeld doordat de afbeelding onvoldoende scherp was of het gezicht niet goed in beeld was. De resterende afbeeldingen konden door de gelaatsvergelijkingssoftware worden gebruikt om te zoeken naar een match in de database. In het antwoord op vraag 12 gaf ik al aan dat de experts

[8] Kamerstuk 31 436, nr.3

uiteindelijk tot een match komen, niet de software. Voor het gebruik is geen toestemming nodig van de rechter-commissaris.
De eisen waaraan de software moet voldoen betreffen onder andere functionaliteit, betrouwbaarheid, accuratesse en veiligheid.