Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

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

584

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 18 september 2019).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) (ontvangen 31 oktober 2019). Zie ook Aanhangsel Handelingen, vergaderjaar 2019–2020, nr. 338.

Vraag 1, 2
Zijn er naast het systeem Catch Strafrecht Verdachte en Veroordeelde (Catch) nog andere gezichtsherkenningssystemen die door de politie gebruikt worden?[1]
Worden gezichtsherkenningssystemen ook toegepast in de openbare ruimte? Zo ja, kunt u beschrijven hoe dit in de praktijk vormgegeven is?

Antwoord 1, 2
Naast Catch Strafrecht Verdachte en Veroordeelde maakt de politie ook gebruik van het systeem Catch in de uitvoering van de vreemdelingentaak. Het gaat hierbij om dezelfde applicatie als Catch Strafrecht Verdachte en Veroordeelde, maar in dit geval wordt gebruik gemaakt van gelaatsfoto's die zijn opgenomen in de Basisvoorziening Vreemdelingen (BVV). De BVV bevat persoons- en statusgegevens van vreemdelingen. Naast de identificatie van vreemdelingen, mag dit systeem ook worden geraadpleegd ten behoeve van de opsporing en vervolging van strafbare feiten indien er een redelijk vermoeden bestaat dat de verdachte een vreemdeling is, of in het belang van het onderzoek en het opsporingsonderzoek op een dood spoor is beland, dan wel snel resultaat geboden is bij de opheldering van het misdrijf. Raadpleging is alleen toegestaan in geval van een misdrijf waarvoor voorlopige hechtenis is toegestaan en na schriftelijke machtiging van de rechter-commissaris op vordering van de officier van justitie.[2]
Naast deze toepassingen onderzoekt de politie of gezichtsherkenning breder kan worden ingezet bij de uitvoering van de politietaak. Zo worden opsporingsfoto's (en dat kunnen ook «stills» van bewegende beelden zijn) afkomstig van camera's in de openbare ruimte aangeboden voor gelaatsvergelijking in Catch. In alle gevallen wordt daarbij gekeken naar de wettelijke

[1] Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3932
[2] Artikel 107, zesde lid Vreemdelingenwet 2000

ah-tk-20192020-584
ISSN 0921 - 7398
's-Gravenhage 2019

waarborgen, juridische mogelijkheden en beperkingen en de praktische bruikbaarheid.

Vraag 3
Gebruikt de politie scraping technieken voor andere doeleinden, specifiek voor doeleinden ten behoeve van gezichtsherkenning of anderszins? Zo ja, welke?

Antwoord 3
In algemene zin kan gesteld worden dat de politie te allen tijde de mogelijke toepasbaarheid beziet van methoden en technieken die van belang zouden kunnen zijn voor taakuitvoering (zoals in beperkte mate web crawling en scraping). Het (laten) doen van onderzoek, het kennisnemen van of opbouwen van kennis, en het kennis nemen van of zelf uitvoeren van experimenten zijn daarbij onderdeel van de inzet.

Vraag 4
Wat is de reden dat tijdens een audit zoals bedoeld in artikel 33 Wet politiegegevens (Wpg) niet wordt gekeken naar specifieke werkwijzen of systemen? Is toetsing aan de praktijk niet juist noodzakelijk voor een effectieve audit? Bent u bereid toe te zeggen dat volgende audits (art. 33 Wpg) worden uitgebreid zodat ook gekeken wordt naar de feitelijke situatie bij specifieke werkwijzen en systemen?

Antwoord 4
De audit (hierna: privacy audit) zoals bedoeld in artikel 33 Wet politiegegevens (hierna: Wpg) is gericht op de werking van het stelsel van gegevensbescherming. Bij de uitvoering van de privacy audit toetst een onafhankelijke auditor primair of de organisatie adequaat is ingericht om in voldoende mate tegemoet te komen aan de wettelijke bepalingen. Tijdens deze audit wordt niet gekeken naar specifieke werkwijzen of systemen.[3]
Voor de toetsing van specifieke werkwijzen en systemen hecht ik waarde aan de verplichte gegevensbeschermingseffectbeoordeling zoals opgenomen in artikel 4c van de Wpg. Het systeem Catch dateert van voor de inwerkingtreding van dit artikel (1 januari 2019). Er wordt bij de vernieuwing van het systeem Catch – die momenteel door de politie wordt uitgevoerd – een gegevensbeschermingseffectbeoordeling[4] uitgevoerd die het gehele systeem Catch omvat.

Vraag 5
Ziet u het overschrijven van de wettelijke bewaartermijnen als een inbreuk op de beveiliging (art. 33a Wpg) en de onrechtmatige verwerking na de wettelijke bewaartermijn als een risico voor de rechten en vrijheden van de betrokkenen? Zo ja, worden deze overschrijdingen aan de Autoriteit Persoonsgegevens en aan de betrokkenen gemeld?

Antwoord 5
Artikel 1q Wpg geeft een definitie van inbreuk op de beveiliging. Volgens deze definitie is het overschrijden van wettelijke bewaartermijnen dan wel het raadplegen van te lang bewaarde data geen inbreuk op de beveiliging in de zin van art. 33a van de Wpg. Er is daarom geen sprake van een datalek waarvoor een meldplicht geldt.
Het overschrijden van de wettelijke bewaartermijn en de verwerking van te lang bewaarde gegevens levert echter wel een risico op voor de rechten en vrijheden van de betrokkenen. Tegenover dat risico staat het maatschappelijke belang van de opsporing van zware misdrijven, die soms lang onopgelost blijven. Zoals ik in de brief over de aanpak van cold cases[5] heb geschetst, streef ik ernaar om bij de herziening van de Wpg/Wjsg een beter evenwicht te vinden tussen beide belangen. Daarbij moet ook goed gekeken worden naar de uitvoerbaarheid.

---

[3] Kamerstuk 30 327, nr. 3, p. 89
[4] Zie artikel 4c lid 1 Wpg
[5] Kamerstuk 29 268, nr. 859

De (beleids)voorbereidingen voor de herziening van de Wpg en de Wjsg zijn inmiddels gestart. Dit gaat om een algehele herziening en modernisering van beide wetten die de informatiehuishouding van zowel de politie, bijzondere opsporingsdiensten, boa-werkgevers als het justitiële domein regelen. Ik verwacht de contourennota over deze herziening in het voorjaar van 2020 naar uw Kamer te kunnen sturen. Terwijl ik werk aan een structurele oplossing, heb ik de korpschef gevraagd tijdelijke maatregelen te nemen om de risico's te beperken. In dit kader verwijs ik kortheidshalve naar mijn antwoord op vraag 11 van de eerder gestelde Kamervragen over de gezichtsdatabase[6].

[6] Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3932