Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

32 761 Verwerking en bescherming persoonsgegevens

30 821 Nationale Veiligheid

Nr. 206

BRIEF VAN DE MINISTERS VAN JUSTITIE EN VEILIGHEID EN VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 december 2021

In het commissiedebat van 24 november jl. (Kamerstuk 21 501-33, nr. 898) over de aankomende EU TELECOM-Raad van 3 december 2021 zijn door uw Kamer vragen gesteld over gezichtsherkenning in de openbare ruimte. Dit betreft vragen van het lid van Ginneken (D66) over de inzet van gezichtsherkenning door de politie en vragen van het lid Dassen (VOLT) over wenselijke toepassingen van gezichtsherkenning in de publieke ruimte. De Minister van Economische Zaken en Klimaat heeft uw Kamer toegezegd dat hier schriftelijk op terug zou worden gekomen. Met deze brief wordt deze toezegging gestand gedaan.

Wettelijke waarborgen bij gezichtsherkenningstechnologie

Aan het toepassen van gezichtsherkenningstechnologie kleven risico's op ongerechtvaardigde inbreuken op fundamentele rechten. Daarom zijn er zowel in EU als nationaal verband strikte regels vastgesteld, die ertoe nopen dat er zeer terughoudend en met inachtneming van de noodzakelijke waarborgen wordt omgegaan met de inzet van deze technologie.[1] Dit geldt zowel voor politie en justitie, als voor bedrijven en burgers. Het kabinet is hier in de kabinetsreactie op het bericht in de Volkskrant over de EDPB/EDPS Opinie betreffende de AI-verordening[2] op ingegaan. Als bijlage bij die kabinetsreactie is een juridisch kader opgenomen waarin wordt toegelicht in welke gevallen gezichtsherkenningstechnologie zou kunnen worden ingezet en met welke waarborgen.

[1] Bij deze waarborgen kunt u denken aan het vooraf uitvoeren van een Data Protection Impact Assessment (artikel 35 Algemene Verordening Gegevensbescherming (AVG) respectievelijk artikel 4c van de Wet politiegegevens (Wpg).

[2] Kamerstukken 32 761 en 22 112, nr. 198

kst-32761-206
ISSN 0921 - 7371
's-Gravenhage 2021

De Minister van Justitie en Veiligheid heeft uw Kamer in 2019 geïnformeerd over «Waarborgen en kaders bij gebruik gezichtsherkenningstechnologie».[3] In die brief wordt uitgelegd hoe en waarvoor de politie gezichtsherkenningstechnologie inzet en wordt nader ingegaan op het juridisch kader daaromtrent. In de met deze brief gelijktijdig aan uw Kamer verstuurde beantwoording van de Kamervragen van het lid Van Ginneken (D66) wordt voorts toegelicht dat de politie alleen gebruik maakt van het systeem CATCH (Aanhangsel Handelingen II 2021/22, nr. 1053). Hiermee kan alleen achteraf – niet «realtime» – worden gekeken of de onbekende mensen op beelden van misdaden al bij de politie bekend zijn en dus in de CATCH-database staan.

De politie past geen real-time gezichtsherkenningstechnologie in de openbare ruimte toe. De inzet van gezichtsherkenningstechnologie bij de politie moet altijd een juridisch-ethische toets doorstaan. De politie hanteert een interne beleidslijn dat daarna ook nog toestemming moet worden gegeven door de portefeuillehouders »Ethiek en Privacy» en »Digitalisering» van de politie. Het juridische aspect van voornoemde toets ziet onder meer toe op of de inzet past binnen de bevoegdheden van de politie en of er wordt voldaan aan de eisen die de wet Politiegegevens stelt aan het verwerken van gegevens, zoals onder meer dat bijzondere persoonsgegevens (waaronder biometrische gegevens) alleen mogen worden verwerkt voor zover dit voor het doel van de verwerking noodzakelijk is en slechts in aanvulling gebeurt op de verwerking van andere politiegegevens.[4] Zoals ik uw Kamer eerder heb laten weten, heeft dit nog niet geleid tot goedkeuring van een ander gebruik van biometrische gezichtsherkenningstechnologie dan CATCH.[5] Indien hier verandering in zou komen wordt uw Kamer hierover geïnformeerd.
Hier komt bovenop dat de voorliggende concept AI-verordening real-time gezichtsherkenningstechnologie in de openbare ruimte ten behoeve van de rechtshandhaving in beginsel verbiedt. Hierop zijn een aantal uitzonderingssituaties geformuleerd, zoals bijvoorbeeld ten behoeve van het voorkomen van terroristische aanslagen.[6] Het kabinet heeft aangegeven dat het deze uitzonderingsgronden in beginsel passend vindt.[7] Dit standpunt is mede bepaald door de belangrijke waarborgen die in artikel 5 verder worden geïntroduceerd.[8] Zo regelt het tweede lid dat er waarborgen moeten worden gesteld die het gebruik van real-time gezichtsherkenningstechnologie beperken in tijd, ruimte en met betrekking tot het aantal personen. Het derde lid stelt dat het gebruik van real-time gezichtsherkenningstechnologie door een bevoegde autoriteit vooraf moet worden getoetst. En als laatste schrijft het vierde lid voor dat lidstaten in nationale wetgeving moeten vastleggen in welke gevallen en onder geleide van welke waarborgen een bevoegde autoriteit het gebruik van real-time gezichtsherkenningstechnologie toe mag staan. Hiermee wordt uw Kamer dus in gelegenheid gebracht om te bepalen óf en zo ja voor welke uitzonderingsgronden er in Nederland real-time gezichtsherkenningstechnologie zou mogen worden ingezet in het kader van de rechtshandhaving. Als laatste is van belang op te merken dat de concept

[3] Kamerstukken 32 761 en 30 821, nr. 152.
[4] Artikel 5, Wet politiegegevens
[5] Aanhangsel van de Handelingen II 2021/22, nr. 105 «Antwoord van Minister Dekker (Rechtsbescherming), mede namens de Minister van Justitie en Veiligheid, ontvangen op 28 september 2021»
[6] Artikel 5, eerste lid, van het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op artificiële intelligentie) en tot wijziging van de bepaalde wetgevingshandelingen van de Unie
[7] Beantwoording schriftelijk overleg BNC-Fiches AI en reactie brief Rathenau instituut
[8] Artikel 5, concept AI-verordening, te raadplegen via https://eur-lex.europa.eu/

AI-verordening geen grondslag biedt om gezichtsherkenningstechnologie wél toe te passen. De beperkingen en eisen uit de conceptverordening zouden in aanvulling gelden op de reeds bestaande regels uit de Wpg en deze niet vervangen.

De toepassing van gezichtsherkenningstechnologie in de openbare ruimte anders dan door de politie

Op basis van het bestaand juridisch kader kan gezichtsherkenningstechnologie, in het bijzonder in openbare ruimten, alleen in een beperkt aantal gevallen worden ingezet.[9]

Als dit overheidsorganisaties betreft zou dit doorgaans alleen kunnen op grond van een expliciet wettelijk vastgelegde bevoegdheid. Dit vereist in de regel een wet in formele zin, waarbij het parlementair proces uiteraard doorlopen wordt. Hiermee voert de wetgever regie over in welke uitzonderingssituaties een inbreuk op het recht op privéleven, bijvoorbeeld door de inzet van gezichtsherkenningstechnologie, noodzakelijk is en aan de eisen van proportionaliteit en subsidiariteit voldoet.[10] Anderzijds zijn er situaties waarin onomwonden en vrijelijk toestemming is verleend door alle betrokkenen. Hierbij kan worden gedacht aan het verlenen van toegang tot bepaalde ruimten. In die gevallen, waarin de verwerking berust op het geven van toestemming, moet mensen dus een echte keuze worden geboden. Denk bijvoorbeeld aan de »poortjes» op Schiphol.

De inzet van gezichtsherkenningstechnologie door burgers en bedrijven kan in beginsel alleen in twee gevallen. Ten eerste op grond van artikel 29 UAVG, dat bepaalt dat biometrische gegevens mogen worden verwerkt om redenen van zwaarwegend algemeen belang voor authenticatie of beveiligingsdoeleinden. Daarbij kan gedacht worden aan de beveiliging van vitale infrastructuur, zoals bijvoorbeeld om de toegang tot energiecentrales alleen voor bevoegden mogelijk te maken.

Ten tweede kan gezichtsherkenningstechnologie worden ingezet als daar onomwonden toestemming is verleend door álle betrokkenen die daaraan onderworpen zijn. Een voorbeeld is het ontgrendelen van eigen apparaten, maar het kan ook gaan om het krijgen van toegang tot bepaalde ruimten. De European Data Protection Board geeft dit laatste tevens als voorbeeld: *«Voorbeeld: Een verwerkingsverantwoordelijke beheert de toegang tot zijn gebouw met behulp van gezichtsherkenningstechnologie. Mensen kunnen van deze manier van toegang alleen gebruikmaken als zij daarvoor van tevoren uitdrukkelijk geïnformeerde toestemming hebben gegeven (overeenkomstig artikel 9, lid 2, onder a)). Om te voorkomen dat opnamen worden gemaakt van iemand die hiervoor geen toestemming heeft gegeven, mag de gezichtsherkenning pas worden toegepast wanneer de betrokkene deze zelf activeert, bijvoorbeeld door op een knop te drukken. Om de rechtmatigheid van de verwerking te waarborgen, moet de verwerkingsverantwoordelijke altijd een alternatieve toegangswijze bieden om in het gebouw te komen waarbij geen biometrische gegevens worden verwerkt, bijvoorbeeld met badges of sleutels.»*[11]

Een ander voorbeeld is dat gezichtsherkenningstechnologie ingezet zou kunnen worden in een «gecontroleerde omgeving», welke weliswaar

---

[9] Zie bijlage 1 (juridisch kader) bij Kamerstukken 32 761 en 22 112, nr. 198, pp. 3–4

[10] Kamerstukken 32 761 en 22 112, nr. 198, p. 3

[11] EDPB Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door midden van videoapparatuur, p. 20.

behoort tot de openbare ruimte, maar waarbinnen alle betrokken onomwonden en geïnformeerd toestemming hebben gegeven. Deze toestemming moet natuurlijk wel »vrijelijk» zijn gegeven, wat betekent dat mensen geen nadelige consequenties mogen ondervinden van het niet verlenen van toestemming.[12]

Conclusie

Gezichtsherkenningstechnologie mag alleen in een zeer beperkt aantal gevallen en onder geleide van strikte waarborgen in de openbare ruimte worden ingezet. De concept AI-verordening breidt de bestaande mogelijkheden voor gezichtsherkenningstechnologie niet uit, maar stelt verdere beperkingen aan de inzet van real-time gezichtsherkenningstechnologie in het kader van rechtshandhaving en draagt eraan bij dat het beperkt aantal biometrische systemen dat wél mag worden ingezet grondig wordt gecontroleerd alvorens deze in gebruik worden genomen. Hiermee voorkomen we dat er fouten worden gemaakt en stimuleren we een rechtsstatelijke inzet van gezichtsherkenningstechnologie.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

De Minister voor Rechtsbescherming,
S. Dekker

[12] Zie voor meer voorbeelden van rechtmatige en onrechtmatige inzet van gezichtsherkenning de EDPB Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevensdoor middelen van videoapparatuur, vanaf p. 18.