Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022 **Aanhangsel van de Handelingen**

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

974

Vragen van het lid **Leijten** (SP) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het gebruik van gezichtsherkenning bij toegang tot evenementen* (ingezonden 28 oktober 2021).

Antwoord van Minister **Dekker** (Rechtsbescherming) (ontvangen 6 december 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 789.

Vraag 1
Is er een overzicht van het aantal evenementen dat gebruik heeft gemaakt van gezichtsherkenning om gasten of personeel toegang te verlenen? Zo ja, kunt u dit aan de Kamer doen toekomen?[1]

Antwoord 1
Een dergelijk overzicht is er niet.

Vraag 2
Bent u het met mij eens dat gezichtsherkenning grote risico's kent, zoals een groot verlies aan privacy, het ongeoorloofd gebruik van persoonlijke data en buitensluiting? Zo nee, waarom niet?

Antwoord 2
Dat ben ik met u eens.

Vraag 3
Vindt u het wenselijk dat evenementen gebruik maken van gezichtsherkenningstechnologie van private aanbieders, terwijl er ook minder ingrijpende alternatieven voorhanden zijn? Zo ja, waarom?

Antwoord 3
Aan het toepassen van gezichtsherkenning kleven risico's. Dat is ook onderkend door de wetgever. Zowel in EU als nationaal verband zijn er strikte regels, die ertoe moeten leiden dat er terughoudend wordt omgegaan met de inzet van deze technologie. Ik vind het belangrijk dat de inzet van gezichtsherkenning rechtmatig is en voldoet aan dit strikte juridisch kader dat daarvoor

[1] NRC, 25 oktober 2021, «Gezichtsherkenning als identificatiemiddel naast de coronacheck voor festivals», https://www.nrc.nl/nieuws/2021/10/25/gezichtsherkenning-als-identificatiemiddel-naast-de-coronacheck-om-een-festival-binnen-te-komen-a4063069

ah-tk-20212022-974
ISSN 0921 - 7398
's-Gravenhage 2021

geldt. Er geldt in deze gevallen een «nee, tenzij» regime en op grond daarvan is er weinig ruimte voor gezichtsherkenning. Bij deze evenementen zal de inzet hooguit denkbaar kunnen zijn op basis van uitdrukkelijke toestemming van de betrokkene zelf, die vrijelijk moet kunnen worden gegeven. De verwerkingsverantwoordelijke, in deze casus de organisator van een evenement, moet burgers dus echt de keuze bieden of zij toestemming willen geven voor gezichtsherkenning, ook door minder ingrijpende alternatieven aan te bieden. Op basis van de informatie uit het NRC-artikel heb ik geen reden om aan te nemen dat bij genoemde evenementen niet aan de wettelijke vereisten is voldaan.
Ik verwijs verder naar de antwoorden op de vragen 2 en 3 van het lid Kerseboom (FVD) aan de Minister voor Rechtsbescherming over de inzet van gezichtsherkenningstechnologie die ik tegelijkertijd aan uw Kamer heb aangeboden. Hierin is onder meer tot uiting gebracht dat, ook al is er vrijelijk uitdrukkelijke toestemming door betrokkenen verstrekt, gezichtsherkenning alleen mag worden toegepast als aan alle voorwaarden uit de AVG is gedaan. Hierbij wordt onder meer gewezen op het beginsel van data minimalisatie.

Vraag 4
Zijn er richtlijnen voor veiligheidsregio's als zij een verzoek krijgen voor een evenement met gezichtsherkenning? Zo ja, wat behelzen deze en is er overeenstemming tussen veiligheidsregio's over de inzet van gezichtsherkenning?

Antwoord 4
Uit navraag onder de veiligheidsregio's is gebleken dat er geen specifieke richtlijnen bekend zijn voor evenementen met gezichtsherkenning in de veiligheidsregio's.

Vraag 5
In hoeverre vindt u dat er wordt voldaan aan de eis dat gebruik van gezichtsherkenningssoftware vrijwillig moet zijn, als er bijvoorbeeld evenementen georganiseerd zouden worden waarbij negen toegangspoorten werken met gezichtsherkenning en één reguliere toegangspoort voor bezoekers is? Bent u het met mij eens dat de grens tussen vrijwillig en drang of zelfs praktische dwang niet altijd eenduidig is? Bent u het met mij eens dat deze beslissingen binnen een wettelijk kader horen?

Antwoord 5
Ik ben het met u eens dat dergelijke beslissingen binnen een wettelijk kader horen. Dit is ook het geval. Hoe de wet in de praktijk uitpakt is altijd afhankelijk van de specifieke omstandigheden van het geval. Toestemming door de betrokkene, zoals beschreven in artikel 7 van de Algemene verordening gegevensbescherming (AVG), moet vrijelijk en uitdrukkelijk zijn gegeven. Het onthouden van toestemming mag er niet toe leiden dat betrokkene als gevolg daarvan nadelige gevolgen ondervindt.[2] In het hypothetische geval dat de door de organisator van het evenement voorziene indeling van het aantal toegangspoortjes tussen «identificatie door gezichtsherkenning» versus «analoge identificatie» ertoe leidt dat betrokkenen die geen toestemming verlenen voor het verwerken van hun biometrische gegevens bijvoorbeeld substantieel langer moeten wachten en een deel van het evenement missen waarvoor zij hebben betaald, kan worden aangenomen dat dit als nadelig gevolg kwalificeert. Het is aan de Autoriteit Persoonsgegevens (AP), of in voorkomend geval aan de rechter, om in het specifieke geval te beoordelen of deze toestemming daadwerkelijk vrijelijk is gegeven. Op basis van de informatie in het aangedragen NRC-artikel heb ik geen reden om aan te nemen dat bezoekers hun toestemming niet vrijelijk hebben kunnen verlenen. Evenementen moeten er vanuit hun rol als verwerkingsverantwoordelijke van deze bijzondere persoonsgegevens zorg voor dragen dat aan de wet wordt voldaan en dat zij rechtmatig gegeven toestemming van betrokkenen verkrijgen voor de verwerking van biometrische gegevens. Eén van die vereisten is dat het evenement – gelet op de risico's die dergelijke grootschalige monitoring van biometrische gegevens meebrengt – een Data Protection

[2] Artikel 7 AVG, zie ook overweging 42 bij de AVG.

Impact Assessment (DPIA) uit moet voeren.[3] In zo'n beoordeling zal de vraag over het rechtmatig geven van toestemming en de consequenties daarvan voor de manier waarop de toegang tot het evenement wordt ingericht een centrale rol moeten vervullen. Vervolgens is het aan de organisatie om maatregelen te nemen zodat toestemming wél vrijelijk kan worden gegeven, bijvoorbeeld door de indeling van de toegangspoortjes aan te passen, en er zorg voor te dragen dat aan alle bepalingen en beginselen van de AVG wordt voldaan.

Vraag 6
Welke instanties houden toezicht bij evenementen of deelname niet alleen in theorie vrijwillig is maar er ook daadwerkelijk een afdoende alternatief geboden wordt? Heeft onder andere de Autoriteit Persoonsgegevens, die nu al kampt met tekorten en grote uitdagingen, hier wel voldoende capaciteit voor volgens u?

Antwoord 6
De AVG kent een getrapte en risico-gebaseerde toezichtstructuur. De AP is de toezichthouder op de verwerking van persoonsgegevens en daarmee de centrale figuur in het toezichtstelsel. Daarnaast moeten organisaties in bij wet bepaalde gevallen waar de risico's van gegevensverwerkingen voor betrokkenen groter worden een Functionaris Gegevensbescherming (FG) aanstellen.[4] Deze FG fungeert als interne controleur en als verlengstuk van de AP binnen organisaties. De positie en taken van de FG zijn ook in de wet vastgelegd.[5] Daarnaast moeten organisaties zoals eerder genoemd een DPIA uitvoeren als de verwerking een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen, om vervolgens maatregelen te nemen om die risico's te mitigeren. De FG toetst deze DPIA in diens onafhankelijke rol.
Wat betreft de capaciteit van de AP verwijs ik naar de brief van 19 november 2020 waarin uw Kamer is geïnformeerd over de taken en middelen van de AP.[6] Vanaf 2022 ontvangt de AP structureel 6 miljoen extra.

Vraag 7
Wordt er volgens u bij het inzetten of op grotere schaal gebruiken van nieuwe technologieën in voldoende mate tijdig onderkend welke maatschappelijke gevolgen uit het gebruik (kunnen) voortvloeien? Zo ja, waar baseert u dit op? Zo nee, bent u bereid hier onderzoek naar te laten doen?

Antwoord 7
Ik vind het van groot belang dat hier voldoende aandacht is voor. Het kabinet heeft dan ook meerdere onderzoeken laten verrichten naar de ethische en juridische consequenties van technologie. Naar aanleiding daarvan heeft het kabinet maatregelen genomen om te borgen dat die risico's worden beperkt.[7] Ook in de Nederlandse Digitaliseringsstrategie (NDS) wordt aandacht gegeven aan de risico's van digitalisering, bijvoorbeeld als het gaat om de bescherming van persoonsgegevens.[8] Ik vind het belangrijk dat komende overheidsstrategieën alle gevolgen van technologische ontwikkelingen, dus zowel positief als negatief, voldoende in ogenschouw nemen.
Mijn indruk is daarnaast dat erin de wetenschap, maar ook in het politieke debat en het openbaar bestuur volop aandacht wordt besteed aan de gevolgen van technologische ontwikkeling. Dit baseer ik op de veelheid aan artikelen, rapporten en aanbevelingen over de maatschappelijke, economi-

---

[3] Artikel 35 AVG. Zie ook het besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectenbeoordeling (DPIA) verplicht is van de Autoriteit Persoonsgegevens. Te raadplegen via de website van de Autoriteit Persoonsgegevens.
[4] Zie artikel 37 lid 1 AVG.
[5] Artikels 38 en 39 AVG.
[6] Kamerstuk 25 268, nr. 197
[7] Zie bijvoorbeeld drietal de «kabinetsreactie op drietal algoritmeonderzoeken» (Kamerstuk 26 643, nr. 726); of de kabinetsreactie op drie onderzoeken naar respectievelijk gezichtsherkenning in horizontale relaties, drones en spyware (Kamerstuk 34 926, nr. 11)
[8] Kamerstuk 26 643, nr. 755 https://www.rijksoverheid.nl/documenten/kamerstukken/2021/04/26/nederlandse-digitaliseringsstrategie-2021

sche en juridische consequenties van nieuwe technologie.[9] Ik ga er vanuit dat de aandacht voor dit belangrijke onderwerp de komende jaren alleen nog maar verder toe zal nemen.

Vraag 8
Vindt u dat er voldoende geborgd is dat werknemers in bijvoorbeeld voetbalstadions niet verplicht mogen worden, of anderzijds onder druk mogen worden gezet, om gebruik te maken van toegang tot hun werk door dit soort software? Zo ja, hoe? Zo nee, kunt u met voorstellen komen zodat dit wel voldoende geborgd zal zijn?

Antwoord 8
Ja. De Algemene verordening gegevensbescherming (AVG) biedt zoals in antwoord op vraag 2, 3 en 5 weergeven, als mede in de hiervoor genoemde kabinetsbrieven uitgebreider beschreven, een uitgebreid kader dat de verwerking van biometrische gegevens reguleert. Verplichte biometrische identificatie om toegang tot de werkomgeving te verkrijgen zal doorgaans niet rechtmatig zijn, omdat toestemming in relaties tussen werkgevers en werknemers niet vrijelijk kan worden gegeven.[10] Dit behoudens uitzonderingssituaties waar het gebruik van biometrische gegevens noodzakelijk is om redenen van zwaarwegende algemeen belang voor beveiligings- of authenticatiedoeleinden; zoals het identificeren van werknemers bij een energiecentrale. Deze laatste eis bevat dus een dubbele en cumulatief werkende noodzakelijkheidstoets: noodzakelijk voor een zwaarwegend algemeen belang én noodzakelijk voor beveiligings- of authenticatiedoeleinden. Deze dubbele noodzakelijkheidstoets zal in de aanstaande wijziging van de UAVG worden vastgelegd.

[9] Recente voorbeelden zijn bijvoorbeeld: de ROB over gegevens en algoritmes in het openbaar bestuur «Sturen of gestuurd worden» (te raadplegen via: https://www.raadopenbaarbestuur.nl/documenten/publicaties/2021/05/25/advies-sturen-of-gestuurd-worden); het adviestraject van de Wetenschappelijke Raad voor het Regeringsbeleid over AI: https://www.wrr.nl/adviesprojecten/artificiele-intelligentie; of rapporten van het Rathenau instituut als bijvoorbeeld: https://www.rathenau.nl/nl/digitale-samenleving/de-stand-van-digitaal-nederland

[10] Zie de richtsnoeren 05/2020 van de EDPB inzake «toestemming overeenkomstig Verordening 2016/679», pp. 9–10, te raadplegen