26643 Informatie- en communicatietechnologie (ICT)

Nr. 1223 Brief van de staatssecretaris van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 9 oktober 2024

Tijdens het ordedebat van 21 mei jl. heeft uw Kamer verzocht om een brief over de motie van het lid Kathmann over het gebruik van gezichtsherkenningssoftware.[1] De motie Kathmann verzoekt de regering om het gebruik van gezichtsherkenningssoftware bij publieke en private organisaties in kaart te brengen en toepassingen waarbij het gebruik niet expliciet is toegestaan door wetgeving maar wel gewenst is, zo snel mogelijk van een grondslag te voorzien en anders te doen beëindigen. Ook verzoekt de motie Kathmann om een vergunningplicht voor het gebruik van gezichtsherkenning in de publieke ruimte te onderzoeken en uw Kamer voor het kerstreces over de vorderingen te informeren.

Het kabinet onderschrijft de onderliggende zorgen van de motie, nu de inzet van gezichtsherkenningstechnologie naar zijn aard gepaard gaat met risico's voor grondrechten zoals privacy en gegevensbescherming. Heldere wettelijke kaders bij de inzet van gezichtsherkenning, toezicht en controle daarop zijn noodzakelijk. Daarom gelden er zowel in Europese Unie (EU)- als nationaal verband strenge regels die ervoor moeten zorgen dat op een terughoudende wijze wordt omgegaan met deze technologie. De noodzaak daarvan neemt alleen maar toe nu gezichtsherkenningstechnologie steeds toegankelijker wordt en het gebruik ervan toeneemt, zoals ook de Autoriteit Persoonsgegevens (AP) ziet en de motie benadrukt.[2]

Hieronder start ik met een korte uiteenzetting van het juridisch kader voor de inzet van gezichtsherkenning. Vervolgens ga ik in op uw verzoek tot het in kaart brengen van de toepassingen, het toezicht en de handhaving. Gezichtsherkenning is een belangrijk aandachtspunt voor de toezichthouder. Ook ga ik in op uw verzoek tot het invoeren van een vergunningsplicht

Juridisch kader

[1] *Kamerstukken II* 2021/22, 26 643, nr. 1171.
[2] *AP jaarverslag 2023,* Autoriteitpersoonsgegevens.nl/documenten/ap-jaarverslag-2023, 1 juli 2024.

Er zijn vele vormen van de inzet van gezichtsherkenningssoftware denkbaar die in meer of mindere mate maatschappelijk gezien wenselijk kunnen worden geacht. De Algemene verordening gegevensbescherming (AVG) is het primaire juridische instrument bij de regulering van gezichtsherkenningstechnologie. Dit kader stelt strenge eisen aan het verwerken van biometrische gegevens voor het identificeren van een persoon. Bij gezichtsherkenning wordt gebruik gemaakt van biometrische persoonsgegevens, die zien op unieke lichaamskenmerken die tijdens het leven (bijna) niet veranderen. De AP heeft in een “handreiking” de meest gestelde vragen beantwoord over de inzet van gezichtsherkenning.[3] Daarin wordt bevestigd dat het verwerken van biometrische persoonsgegevens op grond van de AVG is verboden (artikel 9 AVG) behoudens strikte uitzonderingssituaties.[4] Zo kunnen onder omstandigheden uitzonderingen van toepassing zijn bij de inzet van gezichtsherkenning.[5] Hieronder bespreek ik deze uitzonderingen.

Een eerste uitzondering geldt als de betrokkene vooraf uitdrukkelijk toestemming heeft gegeven voor het verwerken van biometrische persoonsgegevens (artikel 9, tweede lid, sub a, AVG). Deze toestemming dient niet alleen uitdrukkelijk, maar – in lijn met de richtsnoeren inzake toestemming van het Europees comité voor gegevensbescherming (EDPB) – ook vrij, ondubbelzinnig, geïnformeerd en specifiek te zijn (artikel 4, sub 11, AVG).[6] Vrije toestemming betekent bijvoorbeeld dat een betrokkene die ervoor kiest geen toestemming te geven, daarvan geen nadelige gevolgen mag ondervinden. Bij een nadelig gevolg kan bijvoorbeeld worden gedacht aan het hypothetische geval waarin via toegangspoortjes toegang wordt verkregen tot een evenement, en de verhouding tussen het aantal toegangspoortjes voor identificatie door gezichtsherkenning en analoge identificatie er voorzienbaar toe leidt dat betrokkenen die geen toestemming geven voor het verwerken van hun biometrische gegevens aanzienlijk langer moeten wachten en daardoor een deel van het evenement zullen moeten missen.[7]

---

[3] *Gezichtsherkenning. Antwoord op vragen over verwerkingen van persoonsgegevens bij de inzet van gezichtsherkenning*, Autoriteitpersoonsgegevens.nl/documenten/juridisch-kader-gezichtsherkenning, 2 mei 2024.

[4] De verwerking van biometrische gegevens valt onder het verwerkingsverbod van artikel 9 van de AVG.

[5] De voormalige Kamerleden Kerseboom en Leijten hebben vragen gesteld over het gebruik van gezichtsherkenningstechnologie bij de toegang tot evenementen en festivals. Die vragen zijn beantwoord in *Aanhangsel Handelingen* 2021/22, nrs. 789, 974 en 975

[6] Richtsnoeren 05/2020 van 4 mei 2020 van de EDPB inzake toestemming overeenkomstig Verordening 2016/679.

[7] *Kamerstukken II* 2020/21, 34926, nr. 11.

Een tweede uitzondering geldt op grond van artikel 29 Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), indien het verwerken van biometrische gegevens noodzakelijk is voor redenen van zwaarwegend algemeen belang voor beveiligings- of authenticatiedoeleinden. In het wetsvoorstel “Verzamelwet gegevensbescherming”, dat aanhangig is bij uw Kamer, wordt in

artikel 29 UAVG verduidelijkt dat per voorkomend geval dient te worden getoetst of sprake is van een zwaarwegend algemeen belang.[8] Dat resulteert in een dubbele noodzakelijkheidstoets; de verwerking moet noodzakelijk zijn om redenen van zwaarwegend algemeen belang én voor authenticatie- of beveiligingsdoeleinden.[9] In de toelichting bij het wetsvoorstel zijn ten behoeve van de rechtszekerheid situaties omschreven waarin van zwaarwegend algemeen belang sprake is. Het gaat bijvoorbeeld om processen binnen bedrijven of sectoren, waarvan de verstoring schade kan toebrengen aan de volksgezondheid, het milieu of de voedselvoorziening. Veiligheid in het algemeen of belangen zoals efficiëntie of kostenbesparing vallen er niet onder. Met het expliciet opnemen van de dubbele noodzakelijkheidstoets sluit artikel 29 UAVG nog beter aan bij artikel 9, tweede lid, sub g van de AVG, waarvan artikel 29 UAVG een uitwerking is. De gegevensbescherming bij de toepassing van gezichtsherkenning wordt daarmee versterkt.

Indien één van de hierboven beschreven uitzonderingsgronden van toepassing is, is nog niet meteen de inzet van gezichtsherkenning toegestaan. De gebruikelijke vereisten voor de verwerking van persoonsgegevens uit de AVG blijven onverminderd van toepassing. Er dient bijvoorbeeld een verwerkingsgrondslag te zijn voor de verwerking van persoonsgegevens, zoals toestemming van de betrokkene of gerechtvaardigd belang (artikel 6 AVG).[10] Daarnaast dient er te worden voldaan aan de beginselen van gegevensbescherming (artikel 5 AVG). Het beginsel van dataminimalisatie vereist bijvoorbeeld dat niet meer gegevens worden verwerkt dan noodzakelijk is voor het doel van de

---

[8] De Verzamelwet gegevensbescherming is een wijziging van de UAVG en enkele andere wetten in verband met het stroomlijnen en actualiseren van het gegevensbeschermingsrecht (Verzamelwet gegevensbescherming), *Kamerstukken II* 2022/23, 36264.

[9] Authenticatie kan worden onderscheiden van identificatie: authenticatie gaat over het bevestigen van identiteit, identificatie over het vaststellen daarvan.

[10] Als er sprake is van een uitzonderingsgrond “uitdrukkelijke toestemming” of “zwaarwegend algemeen belang” zal er doorgaans ook een verwerkingsgrondslag zijn, nu toestemming en zwaarwegend belang beide verwerkingsgrondslagen zijn op grond van artikel 6, eerste lid, sub a en sub e, AVG.

verwerking. Daarnaast dient te zijn voldaan aan de vereisten voor het beveiligen van biometrische gegevens.[11]

De verwerkingsverantwoordelijke die gezichtsherkenning wil toepassen, dient steeds te zorgen dat wordt voldaan aan de wettelijke vereisten en fundamentele rechten afdoende worden beschermd. Van belang is daarbij de getrapte en risico-gebaseerde toezichtstructuur in de AVG. 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 voor gegevensbescherming (FG) aanstellen (artikel 37, eerste lid, AVG). De positie en taken van de FG zijn grotendeels vastgelegd in artikel 38 en 39 AVG. De FG houdt binnen een organisatie toezicht op de toepassing en naleving van de AVG en vormt het schakelpunt met de AP.

Vanwege de sleutelpositie van de FG zet ik er op in om de positie van de FG verder te versterken. Door deze wettelijke functie verder te professionaliseren en de kwaliteit ervan te borgen, wordt een belangrijke stap gezet in het versterken van die positie. Uit een verkenning in opdracht van het ministerie van Justitie en Veiligheid is gebleken dat een openbaar (kwaliteits)register voor FG's kan bijdragen aan die kwalitatieve impuls.[12] Daarom werk ik aan de oprichting van een Nationaal Register voor FG's (NRFG) met kwaliteitseisen, voorwaarden voor toelating tot het register en adequate bescherming van de persoonsgegevens in het register. Belanghebbenden worden hier (pro)actief bij betrokken. Tegelijkertijd met de oprichting van het NRFG worden gesprekken gevoerd met *stakeholders* zoals de AP om te bezien hoe de positie van de FG nog verder kan worden versterkt.

Om een verantwoorde verwerking van persoonsgegevens bij gezichtsherkenning te borgen, dient een verwerkingsverantwoordelijke voorafgaand aan de inzet ervan een gegevensbeschermingseffectenbeoordeling, ofwel een Data Protection Impact Assessment ('DPIA'), toe te passen.[13] Een DPIA is verplicht bij gegevensverwerkingen die gelet op de aard en de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. [14] Bij cameratoezicht, profilering, observatie en de inzet van biometrie, zoals bij de inzet van gezichtsherkenningstechnologie, is het uitvoeren van een DPIA in

---

[11] Advies 11/2024 van 24 mei 2024 van de EDPB over het gebruik van gezichtsherkenning bij het stroomlijnen van luchthavenpassagiers.
[12] *Kamerstukken II* 2023/24, 32761, nr. 304.
[13] Artikel 35 van de AVG.
[14] Artikel 35 van de AVG.

ieder geval verplicht.[15] De DPIA brengt de gegevensbeschermingsrisico's van een voorgenomen verwerking in kaart, en laat zien welke maatregelen moeten worden genomen om het risico op een inbreuk op de privacy te voorkomen of te minimaliseren. Een DPIA beoordeelt ook of het doel waarmee gezichtsherkenning wordt ingezet op een minder intrusieve wijze kan worden bereikt. De FG toetst deze DPIA in diens onafhankelijke rol en voorziet van een advies. Indien uit een DPIA blijkt dat een voorgenomen gegevensverwerking – bijvoorbeeld bij de inzet van gezichtsherkenning – ook na de nodige maatregelen een hoog risico zou blijven opleveren, is de een "voorafgaande raadpleging" verplicht: de verwerkingsverantwoordelijke moet dan de AP raadplegen vóórdat met de verwerking wordt begonnen. Als de toezichthoudende autoriteit ziet dat de voorgenomen verwerking in strijd is met de AVG, kan zij een verwerkingsverbod opleggen.[16] Bij het wijzigen van de met de verwerking gepaarde risico's dient opnieuw te worden beoordeeld of de verwerking overeenkomstig de DPIA wordt uitgevoerd.

Vanwege de impact voor gegevensbescherming is gezichtsherkenning een belangrijk aandachtspunt voor de AP. Hiervoor is in 2023 een speciaal team opgericht binnen de AP, en van start gegaan met een aantal actiepunten: naast een externe consultatie van een door de AP opgesteld juridisch kader voor gezichtsherkenning, en werkbezoeken aan diverse wetenschappelijke partijen, heeft een rondetafelgesprek over gezichtsherkenning plaatsgehad met verschillende Europese gegevensbeschermingstoezichthouders. In 2024 is de AP hiermee verder gegaan en staat het jaarplan van de AP in het teken van het beschermen van burgers in een digitale wereld.[17]

In aanvulling op het hierboven geschetste wettelijke kader van de AVG treedt per 1 augustus 2024 de Europese AI-verordening in werking. De AI-verordening roept verplichtingen in het leven voor AI-systemen, waaronder AI-systemen voor gezichtsherkenning. Deze verplichtingen kunnen – in lijn met het doel van de motie – bijdragen aan goed toezicht op de naleving van bestaande wetgeving, waaronder de AVG. De vereisten uit de AI-verordening treden stapsgewijs in werking.

Allereerst verbiedt de AI-verordening vanaf 2 februari 2025 het op de markt brengen of in gebruik nemen van *real time* biometrische identificatie – bijvoorbeeld door de inzet van gezichtsherkenning –

---

[15] Besluit van de AP van 27 november 2019, Stcrt. 2019, nr. 64418.
[16] Artikel 36, tweede lid, in samenhang met artikel 58 AVG.
[17] *AP jaarplan 2024,* Autoriteitpersoonsgegevens.nl/documenten/ap-jaarplan-2024,
21 december 2023; *AP jaarverslag 2023*, Autoriteitpersoonsgegevens.nl/documenten/ap-jaarverslag-2023, 1 juli 2024.

op afstand in de openbare ruimte met het oog op de rechtshandhaving (artikel 5, eerste lid, sub d).[18] Door te voorkomen dat systemen die naar hun aard onrechtmatig of ongewenst zijn op de markt worden aangeboden of in gebruik worden genomen, wordt het *ex ante* toezicht op deze systemen versterkt. Handhaving kan plaatsvinden voordat de inzet van een systeem leidt tot een inbreuk op grondrechten of schade veroorzaakt.[19] Voor de rechtshandhaving kan er door het maken van een nationale wettelijke grondslag een beperkte uitzondering gecreëerd worden op het hiervoor genoemde verbod, waar in uitzonderlijke situaties gebruik van gemaakt kan worden. In het halfjaarbericht van de politie van juni 2024 is uw Kamer door de minister van Justitie en Veiligheid geïnformeerd over het traject dat op mijn departement in gang is gezet om te onderzoeken of, en zo ja in welke gevallen, er in nationale wetgeving uitzonderingen op dit verbod zouden moeten worden opgenomen.[20] Hierbij merk ik op dat bij de verwerking van politiegegevens door een bevoegde autoriteit niet de AVG maar de Richtlijn gegevensbescherming bij rechtshandhaving (RGR) van toepassing is. In Nederland is deze richtlijn geïmplementeerd in onder andere de Wet politiegegevens (Wpg).[21]

In aanvulling op de hierboven genoemde verboden in de AI-verordening, gelden vanaf 2 augustus 2026 de regels voor het op de markt brengen en gebruiken van bepaalde “hoog risico” AI-systemen (artikel 6, tweede lid e.v. AI-verordening). Onder deze categorie vallen (ook) AI-systemen die gebruik maken van biometrische gegevens zoals systemen voor biometrische identificatie (gezichtsherkenning) op afstand.[22] Deze AI-systemen worden “hoog risico” geacht omdat zij – anders dan bijvoorbeeld systemen voor verificatie of authenticatie die alleen zijn bedoeld

---

[18] In de context van de AI-verordening betekent *real time* toepassing van biometrie, dat de vergelijking en de identificatie ogenblikkelijk, bijna ogenblikkelijk of in ieder geval zonder noemenswaardige vertraging plaatsvinden.
[19] Vgl. *Kamerstukken II* 2021/22, 32761, nr. 198, p. 4.
[20] *Kamerstukken II* 2023/24, 29 628, nr. 1217 (bijlage nummer 2). Daarmee is de motie Kathmann (*Kamerstukken II* 2023/24, 26 643, nr. 1172) afgedaan. Dit betreft een andere motie dan de motie Kathmann (*Kamerstukken II* 2023/24, 26 643, nr. 1171) die de aanleiding is voor de voorliggende Kamerbrief.
[21] Een politiegegeven is volgens artikel 1, onder a, van de Wet politiegegevens elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012, met uitzondering van de uitvoering van wettelijke voorschriften van de wet administratieve handhaving verkeersvoorschriften, en de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1 en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012.
[22] Artikel 6 AI-verordening in samenhang met Annex III, eerste lid, sub a.

om te bevestigen wie de persoon is – kunnen worden gebruikt voor een groot aantal personen zonder hun actieve betrokkenheid.[23] Ook AI-systemen die personen op basis van biometrische kenmerken indelen in beschermde categorieën en emotieherkenning zijn hoog risico.[24] [25] De aanbieder[26] van deze systemen dient te zorgen dat het systeem veilig en accuraat is, en gecontroleerd wordt op vooringenomenheid zodat discriminatie wordt voorkomen (afdeling 2 en artikel 16, AI-verordening). Een gebruiksverantwoordelijke dient de inzet vervolgens te monitoren en te zorgen voor menselijke controle op de toepassing ervan (artikel 26, AI-verordening). Ook dient de gebruiksverantwoordelijke te zorgen dat de aan biometrische categorisatie en emotieherkenning blootgestelde personen worden geïnformeerd over de werking van het systeem (artikel 50, derde lid, AI-verordening). Ten slotte dienen deze systemen door de aanbieders verplicht te worden geregistreerd in een Europese database. Deze eisen uit de AI-verordening die grotendeels *ex ante*, dus voorafgaand aan het op de markt brengen en in gebruik nemen van het systeem, worden gesteld, dragen bij aan de rechtmatige en verantwoorde inzet van AI-systemen, waaronder AI-systemen voor biometrische identificatie. Aangezien documentatie en transparantie onderdeel zijn van deze vereisten, biedt dit extra handvatten om te controleren op onder andere de rechtmatigheid van het gebruik en de verwerking van persoonsgegevens.

De AI-verordening vereist tevens – in lijn met het verzoek in motie Kathmann om het gebruik van gezichtsherkenning in kaart te brengen – de registratie van hoog risico AI-systemen waaronder bepaalde systemen die gebruik maken van biometrische identificatie (artikel 49 en

artikel 71 AI-verordening). De aanbieder van een dergelijk systeem dient dit systeem voordat hij of zij dat systeem op de markt brengt of in gebruik stelt onder eigen naam te registreren in een door de Europese Commissie nog op te zetten EU-Database (artikel 16, sub i, AI-verordening). Deze verplichting geldt voor zowel de private als

---

[23] Overweging 8 van de AI-verordening.
[24] Biometrische categorisering is het in bepaalde (beschermde) categorieën indelen van personen op basis van biometrische gegevens. Denk aan het op basis van gezichtskenmerken indelen naar geslacht. Emotieherkenning is het op basis van biometrische gegevens, bijvoorbeeld aan de hand van gezichtsuitdrukkingen of bewegingen, identificeren van getoonde emoties.
[25] Artikel 6 AI-verordening in samenhang met Annex III, eerste lid, sub b, sub c. NB. De toepassing van emotieherkenning vereist niet (noodzakelijk) de verwerking van bijzondere, biometrische, persoonsgegevens.
[26] De aanbieder is, zoals bepaald in artikel 3, tweede lid, AI-verordening, diegene die een AI-systeem ontwikkelt of laat ontwikkelen en dat systeem in de handel brengt of het AI-systeem in gebruik stelt onder eigen naam. De aanbieder kan dus zowel een private als een publieke organisatie zijn.

de publieke sector en leidt tot duidelijkheid over welke AI-systemen op de markt zijn. Ook is er een registratieverplichting voor gebruiksverantwoordelijke overheidsinstanties (en organisaties die namens deze instanties opereren) (artikel 26, achtste lid, AI-verordening).[27] Deze verplichting leidt tot inzicht in welke AI-systemen worden gebruikt door of namens overheidsinstanties. Systemen die worden gebruikt voor rechtshandhaving, migratie, asiel en grenstoezichtsbeheer worden geregistreerd in een niet-publiek deel van deze EU-Database (artikel 49, vierde lid, AI-verordening). De informatie van deze registraties is toegankelijk voor de toezichthouder (artikel 49, vierde lid, AI-verordening). Deze nieuwe verplichtingen uit de AI-verordening dragen bij aan het versterken van het toezicht op gezichtsherkenningstoepassingen.

Motie Kathmann

De motie Kathmann verzoekt de regering om het gebruik van gezichtsherkenningssoftware bij publieke en private organisaties in kaart te brengen, en toepassingen waarbij het gebruik van gezichtsherkenningstechnologie niet expliciet is toegestaan door wetgeving, maar wel gewenst is, zo snel mogelijk van een grondslag te voorzien en anders te doen beëindigen. De motie Kathmann verzoekt tevens om een vergunningsplicht voor het gebruik van gezichtsherkenning in de publieke ruimte te onderzoeken.

Zoals hiervoor is uiteengezet, is gezichtsherkenningstechnologie in EU-verband en nationaal strikt gereguleerd. Voor het in kaart brengen van systemen wijs ik op de eerdergenoemde nieuwe registratieverplichting voor AI-systemen die “hoog risico” zijn en waarin biometrische gegevens worden verwerkt. Daarmee wordt komende tijd een steeds completer overzicht gegeven van deze systemen.

Met betrekking tot de voorgestelde vergunningplicht ziet het kabinet dat de inzet van gezichtsherkenning op basis van de AVG reeds onder het verwerkingsverbod voor biometrische persoonsgegevens valt. Voor de gevallen waarin een uitzondering op het verwerkingsverbod voor biometrische persoonsgegevens denkbaar is, gelden de waarborgen van de bij de inzet van gezichtsherkenning verplichte DPIA in combinatie met een eventuele verplichte voorafgaande raadpleging bij de AP als ook met de nodige maatregelen een hoog risico voor grondrechten blijft bestaan. Daarmee biedt het stelsel van de AVG naar mijn oordeel de nodige waarborgen voor een verantwoorde inzet van gezichtsherkenning.

---

[27] De gebruiksverantwoordelijke is diegene die het AI-systeem onder eigen verantwoordelijkheid gebruikt.

Het verdient in dit verband opmerking dat degene die gezichtsherkenning wil inzetten, dat wil zeggen de verwerkingsverantwoordelijke in het kader van de AVG, een eigen verantwoordingsplicht heeft (artikel 5, tweede lid, AVG). Het stelsel van de AVG regelt daarbij een toetsing achteraf door de AP dan wel door de rechter. De verwerkingsverantwoordelijke dient te zorgen dat wordt voldaan aan de wettelijke vereisten. Uiteindelijk is het aan de AP om *in concreto* te beoordelen of bijvoorbeeld de door een betrokkene gegeven toestemming voldoet aan de daarvoor geldende maatstaven. Een systeem van formele vergunningenverlening door een derde partij voorafgaand aan de inzet van gezichtsherkenning zou zich niet goed verhouden tot dit Unierechtelijke systeem voor de bescherming van persoonsgegevens.

In aanvulling op de waarborgen uit de AVG gelden de regels uit de AI-verordening voor biometrische AI-systemen, waaronder het verbod op de inzet van real-time biometrische identificatie in de publieke ruimte door de rechtshandhaving en de waarborgen die gelden voor hoog risicosystemen. Het geheel van waarborgen uit de AVG en de AI-verordening zoals in deze brief beschreven, strekt er mede toe om voorafgaand aan de inzet en het op de markt brengen van gezichtsherkenning, de rechtmatigheid ervan te waarborgen.

Concluderend merk ik op dat het kabinet in grote lijnen de zorgen uit de motie onderschrijft. Het ik kabinet is voorstander van strenge regels, strikte voorwaarden en effectieve handhaving bij de inzet van gezichtsherkenningstechnologie, die naar haar aard gemakkelijk inbreuk kan maken op grondrechten. Met het hierboven geschetste juridische kader, de recent in werking getreden aanvullende regulering en aangekondigde versterkingsmaatregelen is het kabinet van oordeel dat aan deze zorgen afdoende tegemoet is gekomen.

De staatssecretaris van Justitie en Veiligheid,
T.H.D. Struycken