Juridisch kader

Deze bijlage schetst de voornaamste aspecten van het juridisch kader bij de inzet van de in het bericht in de Volkskrant genoemde systemen, welke als doel hebben burgers te categoriseren en/of herkennen aan de hand van hun persoonsgegevens.

Verbod op discriminatie

Artikel 1 van de Nederlandse Grondwet verbiedt discriminatie wegens godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht of op welke grond dan ook. Eenzelfde verbod is neergelegd in artikel 21 van het Handvest van de Grondrechten van de Europese Unie, dat eveneens discriminatie verbiedt, zij het op grond van geslacht, ras, kleur, etnische of sociale afkomst, genetische kenmerken, taal, godsdienst of overtuiging, politieke of andere denkbeelden, het behoren tot een nationale minderheid, vermogen, geboorte, een handicap, leeftijd of seksuele gerichtheid. Non-discriminatie is een pijler onder onze rechtsstaat.

In verticale verhoudingen – de verhouding tussen de overheid en burgers – kan zowel directe als indirecte discriminatie geoorloofd zijn, als het gemaakte onderscheid maar objectief gerechtvaardigd kan worden. Dit betekent dat er sprake moet zijn van een legitieme reden om het onderscheid te maken, dat het maken van onderscheid proportioneel is en dat er geen minder ingrijpende middelen ter beschikking staan om hetzelfde doel te bereiken.

Voor horizontale rechtsverhoudingen – de verhouding tussen private partijen onderling – is artikel 1 Grondwet uitgewerkt in verschillende wetten waaronder de Algemene Wet Gelijke Behandeling (AWGB).[1] De AWGB verbiedt direct en indirect onderscheid op grond van onder meer godsdienst, ras en geslacht in de sfeer van de arbeid en het aanbieden van of verlenen van toegang tot goederen en diensten. Direct onderscheid, waarbij rechtstreeks wordt verwezen naar een wettelijk beschermd persoonskenmerk, is verboden, tenzij sprake is van een wettelijke uitzondering. Indirect onderscheid, waarbij een ogenschijnlijk neutrale bepaling, maatstaf of handelwijze personen vanwege een beschermd persoonskenmerk bijzonder treft, is niet verboden indien het onderscheid objectief gerechtvaardigd is door een legitiem doel en de middelen voor het bereiken van dat doel passend en noodzakelijk zijn. Een voorbeeld van een casus die kan worden getoetst aan de AWGB is de inzet van algoritmische besluitvorming in een selectieprocedure. Als sollicitanten met een 'gat' in hun curriculum vitae automatisch worden uitgefilterd, dan vindt uitsluiting plaats op basis van een criterium dat niet direct verwijst naar een beschermd persoonskenmerk. Van direct onderscheid is daarom geen sprake. Wel kan dergelijke besluitvorming leiden tot indirect onderscheid. Het zijn immers vaak vrouwen die hun carrière tijdelijk onderbreken in verband met zwangerschap, bevalling en het verrichten van zorgtaken.

De inzet van een systeem om onderscheid te maken op basis van de bij wet beschermde categorieën is derhalve niet per definitie verboden. Per casus moet worden beoordeeld of wordt voldaan aan de eisen uit het anti-discriminatierecht. In de praktijk betekent dit dat (biometrische) systemen niet snel kunnen worden ingezet om daarmee onderscheid te maken.

Bescherming persoonlijke levenssfeer en gegevensbescherming

Het recht op eerbiediging van de persoonlijke levenssfeer is onder meer vastgelegd in artikel 10 van de Grondwet en artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM). De bescherming van persoonsgegevens en de eerbiediging van het privéleven zijn bovendien Europese grondrechten, neergelegd in artikelen 7 en 8 van het EU-Handvest van de grondrechten. De Grondwet maakt het mogelijk om bij of

[1] https://wetten.overheid.nl/BWBR0006502/2020-01-01

krachtens een wet in formele zin een inbreuk op dit grondrecht toe te staan. Deze wettelijke grondslag moet voldoende specifiek zijn. Daarnaast moet de inbreuk noodzakelijk zijn (relevant om het beoogde doel te bereiken) en voldoen aan de eisen van proportionaliteit (staat het belang in verhouding tot de inbreuk) en subsidiariteit (kan het doel ook met een minder ingrijpend middel worden bereikt). Elk voornemen om mensen op afstand te herkennen en in te delen in categorieën moet aan deze eisen worden getoetst. Concreet betekent dit dat er doorgaans een wettelijke grondslag moet bestaan om de verwerking rechtmatig uit te voeren.

De Algemene Verordening Gegevensbescherming (AVG) biedt het basiskader voor de verwerking van persoonsgegevens. De verordening bevat onder meer de beginselen inzake de verwerking van persoonsgegevens, welke zijn neergelegd in artikel 5 AVG. Deze vereisen onder meer dat gegevens ten aanzien van betrokkene rechtmatig, transparant en op behoorlijke wijze worden verwerkt (artikel 5 lid 1 sub a). Een discriminerende verwerking van persoonsgegevens kan derhalve ook onder de AVG nooit rechtmatig zijn. Ook het principe van dataminimalisaties is relevant ten aanzien van onderhavige systemen. Dit schrijft voor dat gegevens toereikend en ter zake dienend moeten zijn, alsook dat alleen de gegevens die noodzakelijk zijn om het doel te bereiken mogen worden verwerkt (artikel 5 lid 1 sub c). In samenloop met het principe van doelbinding (artikel 5 lid 1 sub b) dat voorschrijft dat gegevens alleen voor het welbepaalde en specifiek omschreven doelen mogen worden verwerkt, leidt het principe van dataminimalisatie ertoe dat altijd moet worden gekozen voor het minst-ingrijpende systeem waarvoor zo min mogelijk gegevens worden verwerkt. Voorts is van belang dat iedere verwerking van persoonsgegevens moet berusten op een rechtsgrondslag uit artikel 6 AVG. Voor de overheid zal dit doorgaans betekenen dat er een wettelijke basis aan de verwerking ten grondslag moet liggen. Wanneer er bij een verwerking hoge risico's voor de rechten en vrijheden van betrokkenen bestaan – en dus niet alleen risico's ten aanzien van privacy – schrijft de AVG voor dat er een zogeheten Gegevensbeschermingseffectenbeoordeling (ook wel 'DPIA') moet worden uitgevoerd.[2] Indien hieruit blijkt dat bepaalde risico's voor de privacy en gegevensbescherming van burgers niet zelf kunnen worden geadresseerd moet de DPIA aan de AP worden voorgelegd.[3] Een AI-systeem kan ingevolge de AVG dus niet zomaar worden ingezet.

De inzet van bepaalde AI-systemen is onder de AVG niet zomaar toegestaan. Zo verbiedt artikel 22 volledig geautomatiseerde besluitvorming waaraan rechtsgevolgen of anderzijds gevolgen verbonden zijn die een betrokkene in aanmerkelijke mate treffen. In dat geval gelden er aanvullende waarborgen, waaronder in voorkomend geval het recht om menselijke tussenkomst te eisen (artikel 22 lid 3 AVG). AI-systemen kunnen echter ook stuiten op het verbod op de verwerking van bijzondere persoonsgegevens uit artikel 9 lid 1 AVG. Bijzondere persoonsgegevens zijn onder meer gegevens over ras, etnische afkomst, politieke voorkeur of seksueel gedrag, maar ook 'biometrische gegevens' vallen onder deze noemer. Biometrische gegevens zijn gegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot fysieke, fysiologische of gedragsgerelateerde kenmerken op grond waarvan eenduidige identificatie van een natuurlijk persoon mogelijk is.[4] Hierbij kan worden gedacht aan identificatie aan de hand van gezichtsafbeeldingen of vingerafdrukken. Wanneer gegevens over iemands gezicht worden verwerkt teneinde deze persoon te identificeren, worden biometrische en dus bijzondere persoonsgegevens verwerkt, Daarom kan niemand zomaar aan de slag met dergelijke systemen; het verbod is het uitgangspunt.

---

[2] Artikel 35 AVG. Zie hierover tevens de site van de Autoriteit Persoonsgegevens: https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

[3] Artikel 36 AVG

[4] Artikel 4 lid 14 AVG

In artikel 9 lid 2 AVG wordt een aantal uitzonderingen op het verbod op de verwerking van bijzondere persoonsgegevens neergelegd. Voorbeelden zijn de uitdrukkelijke toestemming van betrokkene (in sub a) of het vitale belang van de betrokkene of een ander natuurlijke persoons als deze niet in staat is toestemming te geven (sub c). Verder zijn er een aantal doeleinden waarvoor bij wet kan worden bepaald dat in dat kader bijzondere persoonsgegevens verwerkt kunnen worden, bijvoorbeeld wanneer dit nodig is om redenen van ´zwaarwegend algemeen belang´ (sub g).

Wat betreft de uitzonderingen die van toepassing kunnen zijn kan onderscheid gemaakt worden tussen verschillende organisaties die gegevens verwerken.[5] In hoofdzaak zijn er drie situaties te onderscheiden: private organisaties en personen, publieke organisaties wier verwerking onder de AVG valt, en publieke organisaties wier verwerking(en) onder het speciale regime voor gegevensverwerking neergelegd in de Wet Politiegegevens (Wpg) en Wet justitiële en strafvorderlijke gegevens (Wsjg) vallen.[6]

1. *Private organisaties en personen wier verwerkingen onder de AVG vallen*
   In reactie het rapport ´Op het eerste gezicht´ van 5 februari jl. heeft de minister voor Rechtsbescherming het juridisch kader voor het gebruik van biometrische gegevens in ´horizontale relaties´ uiteengezet.[7] Conclusie daarvan is dat er weinig ruimte bestaat om biometrie in private relaties toe te passen. Kort gezegd bestaat die ruimte nagenoeg alleen in die gevallen waarin onomwonden toestemming wordt verleend of wanneer er redenen van zwaarwegend algemeen belang zijn om gezichtsherkenning toe te passen voor authenticatie of beveiligingsdoeleinden. Hierbij kan worden gedacht aan het beveiligen van vitale processen of de volksgezondheid. Biometrische gegevens mogen in horizontale relaties dus alleen in zeer uitzonderlijke gevallen worden verwerkt.

2. *Overheidsorganisaties wier verwerkingen onder de AVG vallen*
   Van verwerking van biometrische gegevens door overheidsorganisaties kan doorgaans alleen sprake zijn op grond van een expliciet wettelijk vastgelegde bevoegdheid.[8] Ook hier geldt dus dat het gebruik van biometrie de uitzondering is. Het gebruik van biometrie door de overheid dient dus tot uitzonderlijke, wettelijk vastgelegde situaties beperkt te blijven.[9]

3. *Overheidsorganisaties wier verwerkingen onder de Wet politiegegevens vallen*
   In zijn brief van 20 november 2019 is de Minister van Justitie en Veiligheid nader ingegaan op de inzet van gezichtsherkenningstechnologie ten behoeve van de opsporing. In deze

[5] Hierbij worden overheidsdiensten die buiten de reikwijdte van het EU-acquis vallen buiten beschouwing gelaten aangezien deze noch door de AVG noch door de conceptverordening worden gereguleerd. Hierbij kan worden gedacht aan de inlichtingendiensten.
[6] In het onderstaande wordt geen uitputtende opsomming van mogelijke uitzonderingsgronden weergeven, maar wel de meest voorkomende en realistische scenario´s voor de verwerking van biometrische gegevens.
[7] Dit betreft de relatie tussen burgers en bedrijven als mede de relatie tussen burgers onderling.
[8] De AVG schrijft niet expliciet voor op welk niveau van regelgeving uitzonderingen op het verwerkingsverbod moeten worden vastgesteld. Bij gegevens van bijzondere aard geldt – gelet op de inbreuk op grondrechten die hiermee is gemoeid – dat de grondslag (ook al betreft dit een delegatiegrondslag) expliciet in de wet moet worden vermeld.
[9] Andere voorbeeld van dergelijke wettelijk vastgelegde situaties is de hierboven benoemde situatie in welke een verwerking noodzakelijk is het vitaal belang van een betrokkene of ander natuurlijke persoon te beschermen. Van de onder artikel 9 lid 2 sub a omschreven uitzonderingssituatie in welke de betrokkene uitdrukkelijke toestemming verleend zal, gelet op de machtsrelatie tussen de overheid en burger, niet vaak sprake zijn omdat de burger toestemming niet 'vrijelijk' kan verlenen.

brief heeft hij uitgelegd hoe – en met welke waarborgen – dergelijke technologie wordt ingezet en welk juridisch kader daarop van toepassing is.[10] In artikel 5 van de Wpg is vastgelegd dat de politie biometrische gegevens alleen mag verwerken als dit onvermijdelijk is voor het doel van de verwerking en in aanvulling is op het verwerken van andere politiegegevens over die persoon. Het is ingevolge artikel 7a lid 2 van de Wpg ook niet toegestaan om op geautomatiseerde besluiten te baseren op de verwerking van bijzondere persoonsgegevens, tenzij de Autoriteit Persoonsgegevens daar van tevoren over is geraadpleegd. De politie zet gezichtsherkenning dan ook niet in op een wijze waaraan daar geautomatiseerde gevolgen worden verbonden: meerdere identificatie-experts voeren een menselijke toets uit op een mogelijke ´match´ die wordt gevonden door gezichtsherkenningssoftware. De mogelijkheden voor de inzet van gezichtsherkenningstechnologie zijn dus ook voor de politie beperkt en met waarborgen omkleed.[11]

Toelichting op relevante bepalingen uit de conceptverordening

In april 2021 heeft de Commissie de verordening tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie gepresenteerd (Hierna: "de conceptverordening"). Het doel van dit instrument is dat AI-systemen die op de Europese markt worden gebracht en gebruikt, veilig en in overeenstemming zijn met fundamentele rechten en waarden binnen de EU, zoals onder andere neergelegd in de Europese verdragen en internationale mensenrechtenverdragen en in wet- en regelgeving. De verordening geldt dus expliciet als aanvulling op het reeds bestaande juridisch kader.[12]

Artikel 5 van de conceptverordening betreft de door de Europese Commissie voorgestelde verboden AI-praktijken. Gelet op de in het bericht in de Volkskrant aangehaalde voorstellen voor verboden zijn met name de bepalingen vanaf lid 1 sub d relevant. Artikel 5 lid 1 sub d betreft namelijk ´remote biometric identification systems´ (Hierna: ¨RBIS¨).[13] Gezichtsherkenningssystemen vallen binnen de voorgestelde definitie omdat zij op afstand op basis van biometrische gegevens iemands identiteit vaststellen. Genoemde bepaling verbiedt de inzet van ´real-time´ biometrische identificatiesystemen[14] in publiek toegankelijke ruimten ten behoeve van rechtshandhaving, tenzij een uitzonderingsgrond van toepassing is. Daarvan kan sprake zijn wanneer de inzet ´strikt noodzakelijk´ is voor één van de volgende doelen: het gericht zoeken naar slachtoffers van mogelijke slachtoffers van criminaliteit (inclusief vermiste kinderen), het voorkomen van specifieke, substantiële, naderende dreigingen ten aanzien van het leven of de fysieke veiligheid van natuurlijk personen of een terroristische aanval, of als laatste voor het bestrijden (opsporen, lokaliseren, identificeren of vervolgen) van zware criminaliteit.

---

[10] Kamerstukken II 2019/2020, 32761, nr. 152

[11] Uitgebreider beschrijving van de inzet en waarborgen omtrent gezichtsherkenning bij de politie is opgenomen in de brief van de Minister van Justitie en Veiligheid over 'Waarborgen en kaders bij gebruik gezichtsherkenningstechnologie'. Kamerstukken II 2019/2020, 32 761 / 30 821, nr. 152.

[12] *Explanatory memorandum* bij de conceptverordening, p. 4, te raadplegen via: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[13] Deze worden in artikel 4 sub 36 van de conceptverordening gedefinieerd als: *an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified*.

[14] De definitie van 'real-time' in de conceptverordening omvat mede systemen waarbij wordt gewerkt met een lichte vertraging.

In artikel 5 leden 2 en 3 van deze conceptverordening worden nadere beperkingen en voorwaarden gesteld aan het inroepen van deze uitzonderingen op het verbod. Lid 2 bepaalt dat rekening moet worden gehouden met de aard van de situatie en de waarschijnlijkheid en zwaarte van de gevolgen indien het systeem niet wordt ingezet, en de consequenties van de inzet van het systeem voor de vrijheid van alle personen die daardoor worden geraakt. Daarom wordt er in lid 2 ook vastgesteld dat er waarborgen moeten worden geïntroduceerd wanneer een systeem wordt gebruikt.[15] In lid 3 wordt bepaald dat de doelen uit lid 1 en de voorwaarden uit lid 2 moeten worden getoetst door een bevoegde autoriteit. In principe moet deze toets worden uitgevoerd voordat het systeem wordt ingezet, alleen in noodgevallen mag (eventuele) autorisatie achteraf plaatsvinden.

Indien een lidstaat in afwijking van het verbod uit artikel 5 lid 1 en met inachtneming van de aan een afwijking gestelde beperkingen en voorwaarden RBIS ten behoeve van de rechtshandhaving wil toepassen, kan het in nationaal recht gedetailleerde regels vastleggen met betrekking tot het voldoen aan de voorwaarden uit artikel 5 leden 2 en 3. Hierbij wordt ook vastgelegd voor welke van de in artikel 5 lid 1 geformuleerde doelen afwijking van het verbod mogelijk is.[16]

Voorts is van belang op een aantal andere artikelen van de verordening in te gaan. Wanneer een bepaald systeem in de verordening niet wordt verboden betekent dit immers niet dat er geen nadere regels aan worden gesteld. Artikel 6 bepaalt welke systemen worden geclassificeerd als zijnde een 'hoog risico systeem'. Indien een systeem binnen deze categorie valt gelden daarvoor de additionele vereisten voor hoog-risico systemen in hoofdstuk 2 van de conceptverordening. Deze zien onder meer toe op het inrichten van risicomanagementsystemen, de accuraatheid van systemen en de inrichting van menselijk toezicht.[17]

Ingevolge artikel 6 lid 2 van de conceptverordening worden de in Annex III opgenomen toepassingen gekwalificeerd als zijnde 'hoog risico'. In sub 1 van deze Annex worden AI systemen bedoeld voor zowel 'realtime' als 'post' biometrische identificatie van natuurlijke personen als 'hoog risico' aangemerkt. Ook systemen die bedoeld zijn voor de vaststelling van de emotionele toestand van een natuurlijk persoon die worden ingezet in het kader van de rechtshandhaving of migratie, asiel en beheer van grenscontroles worden als 'hoog risico' geclassificeerd. Daarnaast kan nog worden gewezen op artikel 52 van de conceptverordening waarin aanvullende transparantievereisten worden gesteld aan het gebruik van emotieherkenningssystemen[18] en biometrische categorisatiesystemen.[19] De gebruiker van een dergelijk op basis van biometrische gegevens werkend systeem is verplicht natuurlijke personen die door het systeem worden blootgesteld over het gebruik hiervan te informeren. Dit logischerwijs in aanvulling op de daarvoor reeds geldende verplichtingen die voortvloeien uit de AVG.[20]

---

[15] Meer specifiek stelt artikel 5 lid 2 van de conceptverordening hierover: ¨…. *In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.*¨

[16] Zie het voorgestelde artikel 5 lid 4 van de conceptverordening

[17] Artikels 8 tot en met 15 van de conceptverordening.

[18] Artikel 3 sub (34): *an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data*;

[19] Artikel 3 sub (35): *an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data;*

[20] Artikel 5 lid 1 sub a AVG jo. artikel 12 tot en met 14 AVG