



College voor
de Rechten
van de Mens

Grondrechtenbescherming in de AI-verordening

**College voor de
Rechten van de Mens**

Postbus 16001
3500 DA Utrecht

bezoekadres:
Kleinesingel 1-3
3572 CG Utrecht

030 888 38 88
info@mensenrechten.nl
www.mensenrechten.nl

Voor vragen kun je een e-mail sturen en
op werkdagen bellen van 10.00 - 16.00 uur.

Ontwerp
Enof creatieve communicatie

December 2025

Inhoud

Samenvatting	4
1. Inleiding: grondrechten centraal in de AI-verordening	5
1.1 Doel van de publicatie	5
1.2 Waarom een overzicht van de grondrechtendimensie?	5
1.3 Opzet van de publicatie	6
2. Basisoverzicht van grondrechten	7
2.1 De complexiteit van AI toetsen op grondrechten	7
2.2 Geen <i>one size fits all</i> bij grondrechtentoetsing	8
3. Artikelsgewijze bespreking van grondrechten in de AI-verordening	9
3.1 Algemeen geldende verplichtingen (hoofdstuk I en II)	9
3.2 AI-systemen met een hoog risico (hoofdstuk III)	11
3.3 Transparantieplichtingen en AI-testomgevingen (hoofdstuk IV en VI)	16
4. Grondrechtenrisico's van Bijlage III hoog-risico AI-systemen	18
4.1 Biometrische AI-systemen	18
4.2 AI-systemen in kritieke infrastructuur	19
4.3 Onderwijs en beroepsopleiding	19
4.4 Werkgelegenheid	20
4.5 Essentiële diensten	21
4.6 Rechtshandhaving	21
4.7 Migratie, asiel en grensbeheer	23
4.8 Rechtsbedeling en democratische processen	23
5. Grondrechtentoezicht in de AI-verordening	25
5.1 Toezichtstructuur en integratie van grondrechten	25
5.2 Rol van grondrechtenautoriteiten	25
5.3 De markttoezichthouder als cruciale schakel in grondrechtentoezicht	26
5.4 Uitvoering van grondrechtentoezicht in Nederland	26
6. Conclusie: toezicht op AI betekent het beschermen van grondrechten	28

Samenvatting

De Europese AI-verordening heeft als doel om de marktwerking van kunstmatige intelligentie te verbeteren en innovatie te ondersteunen, en tegelijkertijd hierbij de veiligheid, gezondheid en grondrechten (met inbegrip van de democratie, de rechtsstaat en de bescherming van het milieu) te beschermen tegen de schadelijke gevolgen van AI.

Deze publicatie bevat een overzicht van de grondrechtenbescherming in de AI-verordening. Als één van de grondrechtenautoriteiten voor AI-systemen in Nederland biedt het College voor de Rechten van de Mens hiermee een praktisch overzicht voor toezichthouders, beleidsmakers en andere betrokken partijen die verantwoordelijk zijn voor de handhaving van deze wetgeving.

Grondrechtenbescherming is cruciaal in AI-toezicht
AI-systemen worden breed ingezet in de samenleving en kunnen vrijwel alle grondrechten raken. De bescherming van grondrechten vormt daarom een rode draad door de gehele AI-verordening. Daarnaast is grondrechtenbescherming een nieuwe toevoeging aan de bestaande markttoezichtsstructuren.

Dit document geeft in vier inhoudelijke hoofdstukken een overzicht van hoe de AI-verordening concreet grondrechten beschermt:

Hoofdstuk 2: basisoverzicht van grondrechten
Grondrechtenbescherming bij AI kan niet in een checklist gevat worden. Toetsing moet altijd plaatsvinden in de context van een concreet systeem en de impact op mensen of groepen.

Hoofdstuk 3: artikelsgewijze bespreking van grondrechten in de AI-verordening
Overzicht van de meest relevante bepalingen voor grondrechtenbescherming: AI-geletterdheid (artikel 4), verboden AI (hoofdstuk II),

verplichtingen voor AI-systemen met een hoog risico (hoofdstuk III), verplichtingen voor gebruiksverantwoordelijken, transparantieplichtingen (hoofdstuk IV) en de AI-testomgevingen (hoofdstuk VI).

Hoofdstuk 4: grondrechtenrisico's van Bijlage III hoog-risico AI-systemen

Bespreking van de AI-systemen met een hoog risico (Bijlage III) en de concrete grondrechtelijke risico's per categorie.

Hoofdstuk 5: grondrechtentoezicht in de AI-verordening

Markttoezichthouders spelen een sleutelrol in de grondrechtenbescherming: als centrale actor in het producttoezicht betrekken zij op het juiste moment de grondrechtenautoriteiten. De grondrechtenautoriteiten dragen bij aan zowel de monitoring en signalering, als ook aan de evaluatie van specifieke AI-systemen met een hoog risico.

Voorwaarden voor succesvolle grondrechtenbescherming

De effectiviteit van de grondrechtenbescherming in de AI-verordening hangt mede af van hoe de abstracte verplichtingen worden geconcretiseerd in technische standaarden, richtsnoeren en sjablonen. Bovenal is succes afhankelijk van de vaardigheden en capaciteiten van alle betrokken partijen. Aanbieders, gebruiksverantwoordelijken én toezichthouders moeten grondrechtenrisico's adequaat kunnen inschatten.

1. Inleiding: grondrechten centraal in de AI-verordening

1.1 Doel van de publicatie

Het beschermen van grondrechten is één van de hoofddoelen van de Europese AI-verordening.¹ Het College voor de Rechten van de Mens (hierna: het College) fungeert als één van de grondrechtenautoriteiten voor AI-systemen in Nederland. Met deze publicatie biedt het College een overzicht van hoe de AI-verordening praktisch grondrechten beschermt.

We richten ons in deze publicatie primair tot (markt) toezichthouders en beleidsmakers.² Deze partijen dragen namelijk actief bij aan toezicht op en uitvoering van grondrechtenbescherming bij AI-systemen. In deze publicatie zetten we op hoofdlijnen uiteen wat deze grondrechtenbescherming in de praktijk inhoudt en hoe het toezicht daarop vormgegeven is.

1.2 Waarom een overzicht van de grondrechtendimensie?

De AI-verordening wil een evenwicht vinden tussen enerzijds het stimuleren van AI-innovatie en het bijdragen aan de werking van de interne markt, en anderzijds het verzekeren dat AI grondrechten respecteert. De bescherming van grondrechten staat daarmee aan de basis van de verordening. Dit is onder andere zichtbaar in de mantra die als rode

draad door de verordening loopt over mogelijke “risico’s voor de gezondheid, veiligheid, of grondrechten”.³ Deze rode draad beoogt te verzekeren dat alle partijen een helder beeld hebben van welke risico’s een AI-systeem met zich meebrengt en hoe deze beheerst kunnen worden.

Het risico op grondrechtenschendingen vormt een complexe categorie voor betrokkenen om grip op te krijgen, waardoor de grondrechtendimensie van de AI-verordening specifieke aandacht behoeft. AI-systemen worden immers door de gehele samenleving heen ingezet, beïnvloeden bijna elk aspect van het dagelijks leven en raken bijna alle grondrechten, zoals het recht op non-discriminatie, recht op een eerlijk proces, recht op onderwijs, recht op sociale zekerheid en recht op privacy.⁴

De grondrechtendimensie vormt bovendien een nieuwe toevoeging aan het bestaande productveiligheidstoezicht. De AI-verordening volgt het ‘Nieuwe Wetgevingskader’, waarin grondrechten normaal geen expliciet onderdeel vormen.⁵ De grondrechtenbescherming in de AI-verordening is daarmee een nieuwe taak voor toezichthouders, waardoor het waardevol is deze nieuwe dimensie uit te lichten.

1 Artikel 1 Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (AI-verordening).

2 Markttoezichtautoriteiten zijn de nationale toezichthouders (Artikel 3(26) AI-verordening). Andere relevante actoren in het toezicht zijn de grondrechtenautoriteiten (artikel 77 AI-verordening) en de anmeldende autoriteit (artikel 3(19) AI-verordening). Dit overzicht kan ook relevant zijn voor aanbieders, degene die AI-systemen ontwikkelen of in de handel brengen, en voor gebruiksverantwoordelijken, diegene die een AI-systeem gebruiken buiten de persoonlijke sfeer (artikel 3(3) en (4) AI-verordening).

3 Zie bijvoorbeeld als eerst overweging 7 AI-verordening.

4 Fundamental Rights Agency, *Getting the Future Right. Artificial Intelligence and Fundamental Rights*, 2021.

5 Mededeling van de Commissie, De Blauwe Gids van 2022: richtlijnen voor de uitvoering van de productvoorschriften van de EU, 2022/C 247/01. Voor een verdere bespreking zie Hoofdstuk 5.

Omdat de grondrechtelijke dimensie veelzijdig is, door de gehele verordening heenloopt én een nieuw aspect voor het reguliere markttoezicht vormt, is een overzicht van hoe deze concreet terugkomt in de verschillende verplichtingen nuttig. Vanaf augustus 2026 treedt de AI-verordening vrijwel volledig in werking.⁶ Alle betrokken organisaties, van overheden en onderwijsinstellingen tot bedrijven en toezichthouders, moeten dan de verplichtingen implementeren. Met deze publicatie wil het College betrokkenen helpen om de grondrechtenbescherming effectief uit te voeren.

1.3 Opzet van de publicatie

Deze publicatie beschrijft op hoofdlijnen hoe de AI-verordening grondrechten beschermt. Het is geen diepgaande mensenrechtelijke analyse van de verordening en beoogt ook geen normuitleg, maar biedt een overzicht van hoe de verschillende verplichtingen concreet beogen grondrechten te beschermen.

We richten ons op hoofdstukken I, II, III, IV, VI en IX van de AI-verordening, voor zover deze relevant zijn vanuit een grondrechtelijk perspectief. Niet alle onderdelen van de verordening komen aan bod. Bijvoorbeeld: certificering en conformiteit (hoofdstuk III, afdeling 5), *governance* (hoofdstuk VII), de EU-databank (hoofdstuk VIII) en sancties (hoofdstuk XII) worden buiten beschouwing gelaten. AI-modellen voor algemene doeleinden (hoofdstuk V), gedragscodes (hoofdstuk X) en Bijlage I behandelen we alleen op hoofdlijnen in tekstboxen. We richten ons vooral op de rol van gebruiksverantwoordelijken, aanbieders en toezichthouders. Distributeurs, importeurs en de bredere waardeketen blijven buiten beeld.

De opzet van deze publicatie is als volgt:

- **Hoofdstuk 2: basisoverzicht van grondrechten**
De complexiteit van grondrechtentoetsing en waarom nagenoeg alle grondrechten relevant zijn in de context van AI.
- **Hoofdstuk 3: artikelsgewijze bespreking van grondrechten in de AI-verordening**
Overzicht van bepalingen waarin grondrechtenbescherming het meest naar voren komt: AI-geletterdheid (artikel 4), verboden AI (hoofdstuk II), verplichtingen voor AI-systemen met een hoog risico (hoofdstuk III), verplichtingen gebruiksverantwoordelijken, transparantieplichtingen (hoofdstuk IV) en de AI-testomgevingen voor regelgeving (*sandbox*) (hoofdstuk VI)
- **Hoofdstuk 4: grondrechtenrisico's van Bijlage III hoog-risico AI-systemen**
Concrete AI-systemen met een hoog risico (Bijlage III) en de grondrechtelijke risico's per categorie.
- **Hoofdstuk 5: grondrechtentoezicht in de AI-verordening**
Hoe toezicht op grondrechtenbescherming vormgegeven is en de rol van het College als grondrechtenautoriteit in Nederland.

Tot slot bespreken we in de **Conclusie** de belangrijkste aandachtspunten voor grondrechtenbescherming.

⁶ Zie artikel 113 AI-verordening. De EU bespreekt momenteel aanpassingen aan de tijdslijn en verplichtingen van de AI-verordening in het digitale omnibus pakket, zie: [Simpler EU digital rules and new digital wallets to save billions for businesses](#). Deze publicatie houdt de geldige versie van de AI-verordening in november 2025 aan.

2. Basisoverzicht van grondrechten

Grondrechten beschermen iedereen tegen de overheid en garanderen het recht op een menswaardig bestaan. Ze zijn onvervreemdbaar, ondeelbaar en universeel, en vormen zo de fundamentele pijler van de democratische rechtsstaat. Hoewel grondrechten soms abstract klinken of algemeen geformuleerd zijn, zoals vrijheid van meningsuiting of respect voor het privéleven, krijgen ze concrete betekenis in specifieke situaties. Het recht op onderwijs betekent in de praktijk bijvoorbeeld dat een AI-systeem niet zomaar mag bepalen welk schooladvies een kind ontvangt.

2.1 De complexiteit van AI toetsen op grondrechten

De bescherming van grondrechten bij de ontwikkeling en inzet van AI-systemen valt niet samen te vatten in één algemene checklist. Grondrechten zijn daarvoor te breed en de toepassing te contextafhankelijk. Toezichthouders, gebruiksverantwoordelijken en aanbieders moeten daarom altijd blijven beoordelen hoe mensen in de praktijk nadeel kunnen ondervinden van een AI-systeem.

Eén van de redenen voor dit brede bereik is dat relevante grondrechten zijn vastgelegd in een breed scala aan internationale verdragen en wetgeving. Omdat de AI-verordening EU-recht is, staat het Handvest van de Grondrechten van de Europese Unie centraal.⁷ Vervolgens is deze intern ook verbonden aan het Europees Verdrag voor de Rechten van de Mens.⁸ Daarnaast zijn nationale grondrechtenbepalingen van lidstaten zoals grondwetten en gelijkebehandelingswetgeving relevant. Ook zijn de mensenrechten beschermd in internationale verdragen waar die landen zich aan gebonden hebben aan de orde. In het kader van AI-systemen kunnen onder andere het

Internationaal Verdrag inzake burgerrechten en politieke rechten, het Internationaal Verdrag inzake economische, sociale en culturele rechten en het VN-kinderrechtenverdrag een rol spelen. In al deze verdragen committeren staten zich aan het respecteren, beschermen en vervullen van grondrechten om een menswaardig bestaan te garanderen.

Een zeer breed palet aan grondrechten uit deze verschillende documenten kan bij AI-gebruik in beeld komen. AI-systemen worden namelijk in veel sectoren ingezet waardoor praktisch elk grondrecht geraakt kan worden. Denk bijvoorbeeld aan overheidsdiensten, onderwijs, rechtshandhaving of grensbeheer. Welk grondrecht concreet geraakt kan worden, hangt vervolgens af van de context waarin het AI-systeem gebruikt wordt. Een AI-systeem gebruikt door rechters zal bijvoorbeeld snel kunnen raken aan het recht op een eerlijk proces, terwijl dat recht minder relevant zal zijn bij een systeem dat bepaalt of je een hypotheek krijgt of niet.

Staten zijn op diverse manieren gebonden aan grondrechten. De meeste grondrechten beschermen burgers in de eerste plaats tegen de

⁷ Zie bijvoorbeeld overweging 1 en artikel 1 AI-verordening.

⁸ Artikel 52(3) Handvest van de Grondrechten van de Europese Unie.

overheid.⁹ Zo bepaalt vrijheid van meningsuiting bijvoorbeeld dat de overheid alleen onder strenge voorwaarden grenzen mag stellen aan leuzen die tijdens een demonstratie geroepen worden. Dit is een verplichting voor de overheid om het recht op de vrijheid van meningsuiting te respecteren. Een ander type verplichting is om een grondrecht te beschermen of zelfs te vervullen. Dit houdt in dat de overheid wetten en beleid moet maken om mensen te beschermen. Verdragen over discriminatie verplichten bijvoorbeeld maatregelen tegen discriminatie op de werkvloer of in het onderwijs. In deze situaties creëren grondrechten indirect ook verplichtingen voor burgers onderling. In de context van de AI-verordening betekent dit dat grondrechten in sommige sectoren meer direct aan bod komen, zoals bij overheidsdienstverlening. In andere sectoren werken grondrechten vooral indirect door, zoals bij slimme zonnepanelen.

Ten slotte creëren sommige grondrechten een directe inroepbare verplichting bij de overheid, terwijl andere de overheid niet verplichten tot een resultaat maar alleen een inspanning. Het recht op respect voor het privéleven geeft bijvoorbeeld

iemand het recht om te eisen dat de overheid niet zonder toestemming diens woning betreedt. Het recht op huisvesting legt de overheid daarentegen slechts een inspanningsverplichting op.

2.2 Geen *one size fits all* bij grondrechtentoetsing

Het is onmogelijk om in algemene zin vast te stellen hoe AI-systemen getoetst moeten worden of wanneer ze ‘voldoen’ aan grondrechten. AI-systemen kunnen vrijwel alle grondrechten raken en de impact kan erg contextafhankelijk zijn. Toetsing moet dus altijd plaatsvinden in de context van een concreet systeem, kijkend naar de impact op mensen of groepen.

Dit document inventariseert daarom hoe de AI-verordening de bescherming van grondrechten vormgeeft. Zo kunnen toezichthouders, aanbieders en gebruiksverantwoordelijken beter inschatten op welke punten zij scherp moeten zijn over grondrechtenrisico's.

9 Zie bijvoorbeeld E. Frantziou, ‘[The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality](#),’ *European Law Journal* 2015/21, p. 657–679.

3. Artikelsgewijze bespreking van grondrechten in de AI-verordening

Dit hoofdstuk biedt een overzicht van de bepalingen waarmee de AI-verordening grondrechten beschermt. Het behandelt eerst AI-geletterdheid en de verboden AI-praktijken (onderdeel 3.1). Daarna bespreekt het de vereisten voor AI-systemen met een hoog risico (onderdeel 3.2). Tot slot behandelt het de transparantieverplichtingen voor specifieke AI-systemen en de AI-testomgeving voor regelgeving (onderdeel 3.3).

3.1 Algemeen geldende verplichtingen (hoofdstuk I en II)

AI-geletterdheid (artikel 4)

De verplichting tot AI-geletterdheid vormt de eerste materiële bepaling van de AI-verordening en neemt een bijzondere positie in omdat zij geldt voor alle typen AI-systemen, ongeacht het risiconiveau.¹⁰ Samengevat moeten aanbieders en gebruiksverantwoordelijken ervoor zorgen dat hun personeel voldoende kennis en vaardigheden hebben om verantwoord met AI-systemen om te gaan. Personeel moet bewust zijn van de risico's van de AI-systemen waar ze mee werken, waaronder de impact op grondrechten.¹¹ Veel van deze risico's gaan over hoe een AI-systeem de grondrechten van mensen kan raken. Dat betekent dat AI-geletterdheid verder gaat dan technische kennis. Het vereist dat medewerkers voorzien en in kaart kunnen brengen hoe hun specifieke AI-systemen grondrechten in de praktijk kunnen raken.

Het concrete niveau van kennis dat nodig is en de maatregelen die een organisatie moet nemen om dat niveau te verzekeren zijn contextafhankelijk. Het hangt onder andere af van de positie van de medewerkers, het type AI-systemen waar ze mee werken, de ernst van de mogelijke risico's, en de personen of groepen die geraakt worden door de systemen. Hierdoor vereist de AI-gelettertheidsverplichting maatwerk en moeten organisaties het structureel en beleidsmatig verankeren.¹² Hiertoe biedt de Europese Commissie handvatten via een informatiepagina en een openbare database met voorbeelden van organisatorische implementatie.¹³

10 'AI-verordening: waarom de nieuwe verplichting tot 'AI-geletterdheid' ook 'mensenrechtengeletterdheid' betekent', *College voor de Rechten van de Mens*, 1 augustus 2025.

11 Deze verplichting gaat ook op ten aanzien van mensen die in opdracht van een organisatie werken.

12 Zie ook de Autoriteit Persoonsgegevens, *Aan de slag met AI-geletterdheid*, februari 2025.

13 Informatiepagina van de Europese Commissie over AI-geletterdheid: digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers. Databank met strategieën voor AI-geletterdheid: digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy.

Verboden AI (hoofdstuk II, artikel 5)

De rest van de AI-verordening volgt een risico gebaseerde structuur waarbij de verplichtingen afhangen van het risiconiveau.¹⁴ De verboden AI-praktijken uit artikel 5 vormen de top van deze risicopiramide.

Concreet verbiedt artikel 5 acht specifieke AI-systemen,¹⁵ expliciet vanwege hun onacceptabele grondrechtenrisico. De verordening beschrijft in overweging 28 dat deze systemen gemakkelijk kunnen worden misbruikt en een instrument kunnen vormen voor manipulatie, uitbuiting en sociale controle:

“Dergelijke praktijken zijn bijzonder schadelijk en abusief en moeten worden verboden omdat zij in strijd zijn met de waarden van de Unie, namelijk eerbied voor de menselijke waardigheid, vrijheid, gelijkheid, democratie en de rechtsstaat, en met de grondrechten van de Unie die zijn vastgelegd in het Handvest”, waaronder het recht op non-discriminatie, gegevensbescherming en privacy, en de rechten van het kind.”

De Europese Commissie wijst daarnaast in het richtsnoer voor verboden AI-systemen ook op risico's voor vrijheid van meningsuiting, het recht op een eerlijk proces en de onschuldpresumptie.¹⁶

Samengevat zijn dit de acht verboden systemen (op volgorde van artikel 5(1)):

- **Sub a: manipulatieve of misleidende AI**
AI-systemen mogen niet doelbewust manipuleren of misleiden om iemands gedrag wezenlijk te verstoren op een manier die aanzienlijke schade veroorzaakt. Bijvoorbeeld: een systeem dat de stem van een familielid nabootst om iemand intieme gegevens te laten prijsgeven.

- **Sub b: AI-systemen die kwetsbaarheden uitbuiten**

AI mag geen gedrag veranderen door kwetsbaarheden uit te buiten die voortkomen uit leeftijd, handicap of specifieke sociale of economische omstandigheden op een manier die aanzienlijke schade veroorzaakt. Bijvoorbeeld: een spel dat kinderen verslaafd maakt of een therapeutische *chatbot* die mensen overtuigt onnodig dure medicatie te kopen.

- **Sub c: social scoring AI**

AI-systemen mogen mensen niet beoordelen op basis van hun sociale gedrag of persoonlijke kenmerken, als dit leidt tot onevenredig nadelige behandeling of als de nadelige behandeling niet gerelateerd is aan het gedrag. Bijvoorbeeld: systemen die toegang tot sociale zekerheidsvoorzieningen koppelen aan irrelevante gegevens zoals afval verkeerd buiten zetten, gedrag op sociale media, of het te laat terugbrengen van bibliotheekboeken.

- **Sub d: risicobeoordeling voor strafbare feiten**

AI-systemen mogen niet voor een individu beoordelen wat het risico is dat die een strafbaar feit pleegt op basis van profilering en persoonlijkheidseigenschappen en -kenmerken. Bijvoorbeeld: politie-systemen die voorspellen of iemand een terroristisch misdrijf zal plegen enkel op basis van kenmerken als leeftijd, nationaliteit of adresgegevens.

- **Sub e: ongerichte scraping voor gezichtsherkenning**

AI-systemen mogen geen databanken aanleggen met ongericht verzamelde gezichtsafbeeldingen van internet of CCTV-beelden voor de ontwikkeling van gezichtsherkenningssystemen.

14 Voor meer uitleg zie digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai en artificialintelligenceact.eu/high-level-summary/.

15 Dit verbod geldt alleen binnen het toepassingsbereik van de AI-verordening uit artikel 1 en 2. Door de scope van de AI-verordening mogen deze systemen dus nog wél gebruikt worden in het kader van nationale veiligheid, defensie- en militaire doeleinden, justitiële samenwerking, onderzoek en ontwikkeling, persoonlijke en niet-professionele activiteit.

16 Zie Europese Commissie, 'Richtsnoeren van de Commissie betreffende verboden artificiële-intelligentiepraktijken zoals vastgesteld bij Verordening (EU) 2024/1689 (AI-verordening)' C(2025) 5052 final, 4 februari 2025, alinea (8).

■ **Sub f: emotieherkenning op het werk en in het onderwijs**

AI mag werknemers of leerlingen niet continu surveilleren om hun emoties af te leiden, bijvoorbeeld om hun engagement of verveling te meten.

■ **Sub g: biometrische categorisering op verboden gronden**

AI-systemen mogen mensen niet categoriseren op basis van biometrische gegevens om gevoelige eigenschappen zoals etniciteit,¹⁷ politieke opvattingen, vakbondslidmaatschap, seksuele gerichtheid of religie af te leiden. Bijvoorbeeld: sociale media die advertenties tonen op basis van door AI gedetecteerde seksuele gerichtheid of religie.

■ **Sub h: biometrische identificatie op afstand in real time**

De politie mag geen AI-systemen gebruiken om in openbare ruimtes mensen in *real time* te identificeren en te volgen.

Het is belangrijk te benadrukken dat deze verboden strikt zijn gedefinieerd en de meeste ook specifieke uitzonderingen hebben. Daarom kunnen systemen die intuïtief onder een verbod vallen, in de praktijk kwalificeren als AI-systemen met een hoog risico of zelfs een laag risico. De Europese Commissie heeft uitgebreide richtsnoeren met uitleg over deze nuances voor de toepassing van deze verboden gepubliceerd.¹⁸

Noemenswaardig is het verbod op *real time* biometrische identificatie op afstand in openbare ruimte. Het kent een beladen wetgevingstraject waar bezwaren over de zware grondrechtelijke impact en over het beschermen van de veiligheid en openbare orde tegenover elkaar stonden.¹⁹ Het resultaat is een algemeen verbod, met een uitgebreid en complex stelsel van uitzonderingen op basis waarvan rechtshandhaving deze AI-systemen juist wel mag inzetten.²⁰

3.2 AI-systemen met een hoog risico (hoofdstuk III)

Net als bij de verboden systemen classificeert de Europese Unie AI-systemen als ‘hoog risico’;²¹ (de tweede laag van de risicopiramide) vanwege de grote kans op grondrechtenschendingen. Concreet geldt:

“Een bijzonder relevante factor voor de classificering van een AI-systeem als AI-systeem met een hoog risico, is de omvang van de door het AI-systeem veroorzaakte nadelige effecten op de grondrechten die door het Handvest worden beschermd.”²²

De twee risicocategorieën hangen nauw met elkaar samen. Dit komt enerzijds doordat de specifieke systemen die binnen deze categorieën vallen, in elkaars verlengde liggen. Zo is emotieherkenning in onderwijs- en werkomgevingen verboden, terwijl vergelijkbare toepassingen in andere sectoren worden aangemerkt als AI-systemen met een hoog risico. Anderzijds bestaat er samenhang omdat AI-systemen met een hoog risico die niet voldoen aan de vereisten van de verordening, niet in gebruik mogen worden genomen of op de markt mogen worden gebracht, en daarmee verboden zijn.

Hoofdstuk III van de AI-verordening bevat concrete vereisten en verplichtingen voor AI-systemen met een hoog risico. Deze vereisten zijn nagenoeg alle expliciet te koppelen aan de bescherming van grondrechten en vormen het merendeel van de materiële verplichtingen van de AI-verordening. In dit onderdeel worden de meest relevante daarvan uitgelicht. Een bespreking van welke specifieke systemen zijn aangewezen als ‘hoog risico’ in Bijlage III van de verordening volgt in hoofdstuk 4.

Voor de eerste zes bepalingen die hier worden besproken, geldt dat het vereisten zijn waar de

17 Het artikel zelf refereert aan ‘ras’ in de zin van de juridische discriminatiegrond.

18 Zie voetnoot 16.

19 Zie bijvoorbeeld [Joint civil society recommendations for an EU Artificial Intelligence Act for Fundamental Rights](#).

20 Voor een uitleg en bespreking van dit uitzonderingssysteem zie bijvoorbeeld: A. Giannini en S. Tas, ‘[AI Act and the Prohibition of Real-Time Biometric Identification](#)’, *Verfassungsblog*, 10 december 2024.

21 Artikel 6 AI-verordening. Zie pagina 18 voor een uitgebreidere bespreking van de specifieke voorwaarden van Artikel 6 AI-verordening.

22 Overweging 48 AI-verordening.

AI-systemen aan moeten voldoen en waar de aanbieders in de eerste plaats verantwoordelijkheid voor dragen.²³ Dit zijn de bepalingen over:

- Risicobeheer (artikel 9),
- *Datagovernance* (artikel 10),
- Documentatie en registratie (artikel 11 en 12),
- Transparantie (artikel 13)
- Menselijk toezicht (artikel 14)

De laatste bepalingen die in dit onderdeel besproken worden (artikel 26 en 27) gaan juist over de verplichtingen van organisaties die de AI-systemen gaan gebruiken: de gebruiksverantwoordelijken.²⁴

Systemen voor risicobeheer (artikel 9)

Aanbieders moeten een risicobeheersysteem opzetten. Dit risicobeheersysteem moet bestaan uit een “doorlopend en gepland iteratief proces” met “periodieke en systematische toetsing en actualisering”.²⁵ Dit is een belangrijke vereiste nu het de verantwoordelijkheid om grondrechten-risico's in kaart te brengen en te minimaliseren meteen bij de ontwikkeling van een AI-systemen introduceert. Ook maakt het duidelijk dat deze verantwoordelijkheid door de gehele productieketen blijft bestaan. Aanbieders kunnen zich hierdoor niet verschuilen achter een gebrek aan kennis.

De eerste stap bij het opzetten en beheren van een risicobeheersysteem is het in kaart brengen van de risico's. Dit betreft expliciet risico's die kunnen worden gemitigeerd door ontwerpkeuzes of door duidelijke informatieverstrekking.²⁶ Vervolgens bepalen aanbieders welke gerichte en passende maatregelen deze risico's kunnen beperken.²⁷ Om dit te ondersteunen, moeten de AI-systemen technisch worden getest.²⁸ De mogelijke maatregelen bestrijken zowel risico's bij correct gebruik als risico's bij voor de hand liggend misbruik van het systeem.²⁹

Het is daarbij van belang de risico's voor kinderen en, waar relevant, andere kwetsbare groepen expliciet mee te nemen.³⁰ Concreet moeten alle bekende en redelijkerwijs te voorziene risico's worden geïdentificeerd.³¹ Hoewel dit voor ieder systeem en iedere context anders is, zijn voor de hand liggende risico's bij de meeste AI-systemen onder meer het risico op discriminatie of schendingen van het recht op privacy en gegevensbescherming.

Ten slotte vereist artikel 9 dat aanbieders rekening houden met wie de waarschijnlijke gebruiksverantwoordelijke is en welke kennis- en ervaringsniveau deze partij heeft. Op basis hiervan stellen zij aanvullende gebruiksinstructies op, zodat kennis en verantwoordelijkheid voor de bescherming van grondrechten correct worden doorgegeven binnen de keten.

23 Artikel 16 AI-verordening.

24 Artikel 3(4) AI-verordening.

25 Artikel 9(2) AI-verordening. Voor uitleg en context zie J. Schuett, '[Risk Management in the Artificial Intelligence Act](#)', *European Journal of Risk Regulation* 2024/15(2), p. 367-385.

26 Artikel 9(3) AI-verordening.

27 Zie bijvoorbeeld *Committee on Artificial Intelligence, Methodology For The Risk And Impact Assessment Of Artificial Intelligence Systems From The Point Of View Of Human Rights, Democracy And The Rule Of Law (Huderia Methodology)*, Raad van Europa, CAI(2024)16rev2, 28 November 2024

28 Artikel 9(6) AI-verordening, mogelijk in een reële testomgeving op basis van artikel 60 AI-verordening in Artikel 9(7).

29 Artikel 9(2) a en b AI-verordening.

30 Artikel 9(9) AI-verordening.

31 Overweging 65 AI-verordening.

Standaarden, codes en richtsnoeren

De verplichtingen uit de AI-verordening zijn veelal abstract. Daarom vereisen ze interpretatie en vertaling naar de technische praktijk. Om dit te stroomlijnen voorziet de AI-verordening in de ontwikkeling van verschillende instrumenten die uitleg en context bieden. In de praktijk zullen veel aanbieders en gebruiksverantwoordelijken deze instrumenten volgen om te voldoen aan de verplichtingen onder de AI-verordening. De belangrijke zijn:

- Europese standaardiseringsorganisaties (zoals CEN-CENELEC) zijn op basis van artikel 41 verzocht om technische standaarden op te stellen voor de vereisten voor systemen met een hoog risico. Deze zullen bepalend zijn voor wat deze vereisten in de praktijk inhouden, omdat het volgen van deze standaarden een 'vermoeden van conformiteit' oplevert (artikel 32).
- Op basis van artikel 96 brengt de Europese Commissie richtsnoeren uit over de uitleg van belangrijke onderdelen zoals verboden AI en de vereisten voor systemen met een hoog risico.³²
- Het AI-bureau faciliteert het opstellen van praktijkcodes voor AI voor algemene doeleinden (artikel 56) en richtsnoeren voor systemen zonder een hoog risico (artikel 95).

Data en datagovernance (artikel 10)

Artikel 10 van de AI-verordening vereist het opzetten van adequate databeheersystemen en het verzekeren van gepaste datakwaliteit. De bepaling legt expliciet de nadruk op het respecteren van het recht op non-discriminatie. Aanbieders moeten de data analyseren "met het oog op mogelijke vooringenomenheid (...) die nadelige effecten heeft op grondrechten, of leidt tot discriminatie".³³ Concreet betekent dit dat aanbieders maatregelen treffen om vooringenomenheid in de data op te sporen, te voorkomen en te beperken.³⁴

Het waarborgen van datakwaliteit is cruciaal, omdat vooringenomenheid in trainings-, validatie- of testdata een bekende oorzaak van discriminatie is.³⁵ De verordening wijst erop dat het gebruik van historische data bestaande ongelijkheden, zoals racisme of discriminatie, kan reproduceren, bestendigen of zelfs verergeren.³⁶ Hoewel het beschikken over evenwichtige data geen garantie biedt dat een AI-systeem niet discrimineert, vormt het een noodzakelijke bescherming.³⁷

Een heikel punt in deze discussie was altijd de vraag hoe de onderliggende data getest kan worden op vooringenomenheid. Daar is vaak het verwerken van bijzondere persoonsgegevens zoals data over etniciteit, seksualiteit of religie voor nodig.³⁸ Het verzamelen en verwerken van deze gegevens is strikt gereguleerd vanwege hun gevoelige aard.³⁹ Artikel 10 adresseert deze spanning tussen het recht op non-discriminatie

32 Zie bijvoorbeeld Europese Commissie, 'Richtsnoeren van de Commissie betreffende verboden artificiële-intelligentiepraktijken zoals vastgesteld bij Verordening (EU) 2024/1689 (AI-verordening)' C(2025) 5052 final, 4 februari 2025 en Europese Commissie, 'Richtsnoeren van de Commissie betreffende de definitie van een artificiële-intelligentiesysteem zoals vastgesteld bij Verordening (EU) 2024/1689 (AI-verordening)' C(2025) 5053 final, 27 juli 2025.

33 Artikel 10(2)f AI-verordening.

34 Artikel 10(2)g AI-verordening. Er is veel literatuur beschikbaar over hoe vooringenomenheid in data gedetecteerd kan worden. Zie bijvoorbeeld FRA. *Bias in Algorithms: Artificial Intelligence and Discrimination*, 2022 en K. Shrishak, *Bias evaluation. AI-Complex Algorithms and effective Data Protection Supervision* (Support Pool of Experts Programme) 2022, European Data Protection Board.

35 Zie bijvoorbeeld het toonaangevende: J. Buolamwini, T. Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research Conference on Fairness, Accountability, and Transparency*, 2018/81 p. 1-18.

36 Overweging 67 AI-verordening.

37 Zie bijvoorbeeld Gurses, Seda and Balayn, Agathe, 'Beyond Debiasing: Regulating AI and its inequalities', EDRI, 21 september 2021; Birhane, Abeba. "Algorithmic injustice: a relational ethics approach." *Patterns* 2.2 (2021); Wachter, Sandra, Brent Mittelstadt, and Chris Russell. "Bias preservation in machine learning: the legality of fairness metrics under EU non-discrimination law." *W. Va. L. Rev.* 123 (2020): 735;

38 Voor een bespreking zie: M. van Bekkum, 'Using Sensitive Data to De-Bias AI Systems: Article 10(5) of the EU AI Act', *Computer Law & Security Review* 2025/56 en M. van Bekkum en F. Zuiderveen Borgesius. 'Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception?' *Computer Law & Security Review*, 2023/48.

39 Zie artikel 9 Algemene Verordening Gegevensverwerking.

en het recht op privacy door een speciaal regime met waarborgen te introduceren. Dit regime maakt het mogelijk bijzondere persoonsgegevens te gebruiken voor het opsporen en corrigeren van vooringenomenheid, op een veilige en gecontroleerde manier.⁴⁰ In de praktijk zal moeten blijken hoe effectief en veilig dit proces daadwerkelijk is, en of aanbieders dit ook consequent (kunnen) toepassen bij het testen van hun AI-systemen.

Technische documentatie en registratie (artikel 11 en 12)

Artikel 11 verplicht aanbieders technische documentatie op te stellen, zodat nationale bevoegde autoriteiten over de “noodzakelijke, op heldere en begrijpelijke wijze gestelde informatie” beschikken om hun toezicht effectief uit te voeren.⁴¹ Artikel 12 verplicht aanbieders daarnaast een systeem te ontwerpen dat alle relevante gebeurtenissen gedurende de levenscyclus van een hoog-risico AI-systeem automatisch registreert. Dit bevordert de traceerbaarheid van het systeem en ondersteunt effectief toezicht.⁴²

Beide verplichtingen dragen niet alleen bij aan toezicht, maar maken het ook mogelijk voor personen die door het systeem worden geraakt om het juridisch aan te vechten. Adequate technische documentatie en registratie vormen daarmee een cruciale waarborg voor het recht op een eerlijk proces en een doeltreffende voorziening in rechte.

Transparantie en informatieverstrekking (artikel 13)

Transparantieplichtingen zijn een belangrijke manier waarop door de gehele levenscyclus van een AI-systeem grondrechtenrisico's op de voorgrond blijven. Dit is vergelijkbaar met het vereiste om een passend systeem voor risicobeheer op te zetten (artikel 9) en is ook een belangrijk onderdeel van deze transparantieplichting uit artikel 13. Artikel 13 van de AI-verordening vereist dat bij de ontwikkeling van een systeem al rekening

gehouden wordt met de nodige transparantie en uitlegbaarheid. Ook schrijft de bepaling voor welke elementen in ieder geval opgenomen moeten worden in de gebruiksinstructies.⁴³ Eén daarvan is de voorziene (grondrechten)risico's bij correct gebruik en de voor de hand liggende manieren waarop het systeem misbruikt kan worden.⁴⁴

Eisen aan de transparantie die interpretatie van de output van een systeem mogelijk maken, volgen ook uit het bredere grondrechtelijke kader. In de eerste plaats is transparantie vaak noodzakelijk om een systeem te kunnen aanvechten en daarmee een belangrijke voorwaarde voor het recht op een effectieve remedie. Daarnaast eisen veel grondrechten een bepaalde mate van inzicht en transparantie over hoe een beslissing tot stand is gekomen. Bijvoorbeeld bij het recht op non-discriminatie is dit om te kunnen verzekeren dat er geen ongelijke behandeling plaatsvindt. Maar bij andere grondrechten, zoals vrijheid van meningsuiting of het recht op privéleven, is enige transparantie noodzakelijk om goed te kunnen afwegen of de inmenging met het grondrecht proportioneel en noodzakelijk is.⁴⁵ Dit alles hangt samen met zorgen over de zogenoemde ‘black box’-aard van beslissingen die door middel van een AI-systeem tot stand komen. Deze vereisten over transparantie en informatieverstrekking zijn daarmee belangrijke waarborgen voor de bescherming van grondrechten.

Wel geldt ook voor deze transparantievereisten dat in de praktijk pas duidelijk gaat worden hoe effectief zij zijn. De specifieke wijze waarop transparantie geboden wordt (welke data, op welke manier, en wanneer) kunnen namelijk bepalend zijn voor de vraag of het kan bijdragen aan effectieve grondrechtenbescherming.⁴⁶

40 Artikel 10(5) AI-verordening, in samenstel met de vereisten van de Algemene Verordening Gegevensbescherming, zie overweging 70 AI-verordening.

41 Artikel 10(1) AI-verordening.

42 Artikel 12(1) AI-verordening.

43 Rekening houdend met het niveau van de gebruiksverantwoordelijken, overweging 72 AI-verordening.

44 Artikel 13(2) AI-verordening.

45 Artikel 8, 10 en 14 EVRM. Zie bijvoorbeeld de bespreking van het SyRI algoritme door de Rechtbank Den Haag waar het gebrek aan transparantie in relatie tot het recht op non-discriminatie en bescherming van het privéleven centraal stond: Rechtbank Den Haag, 5 februari 2020, ECLI:NL:RBDHA:2020:865 (SyRI), ro. 6.80 ev.

46 Zie bijvoorbeeld: N. Diakopoulos, ‘Transparency’ in: M. Dubber, F. Pasquale en S. Das (eds), *The Oxford Handbook of Ethics of AI*, 2020.

Menselijk toezicht (artikel 14)

Artikel 14 verplicht aanbieders AI-systemen zo te ontwerpen dat menselijk toezicht effectief kan plaatsvinden tijdens het gebruik. Dit toezicht is expliciet gericht op het beperken van de (grondrechten)risico's en vormt tegelijkertijd ook een belangrijke mensenrechtelijke waarborg. De EU 'Ethics guidelines for trustworthy AI' formuleren ook als belangrijkste principe dat mensen enige mate van controle of invloed over de systemen moeten hebben.⁴⁷ Het argument is vaak dat menselijke toezicht belangrijk is voor de kwaliteit van de beslissingen, de context gevoeligheid, de uitlegbaarheid en uiteindelijk ook verantwoordelijkheidstoedeling.⁴⁸

Het vereiste om menselijk toezicht in te bouwen dient ook als mechanisme om de belangrijke koppeling tussen ontwikkelaars en gebruiksverantwoordelijken te waarborgen.⁴⁹ Het is immers essentieel dat degene die het toezicht uitoefent, zo goed mogelijk wordt uitgerust om dit effectief te doen.⁵⁰ De AI-verordening specificeert dat het van belang is dat degene die het toezicht gaat uitoefenen in staat moet worden gesteld om de output van het systeem kritisch te beoordelen, deze waar nodig in twijfel te trekken en te bepalen wanneer een specifiek systeem juist niet ingezet moet worden.⁵¹ De AI-verordening benoemt expliciet dat effectief menselijk toezicht ook inhoudt dat mensen zich bewust moeten zijn van de zogenaamde *automation bias* die inhoudt dat mensen vaak de neiging hebben om geautomatiseerde systemen onterecht te veel te vertrouwen.⁵²

Verplichtingen gebruiksverantwoordelijken (artikelen 26 en 27)

Een bijzonder aspect van de AI-verordening is dat het niet alleen verplichtingen oplegt aan de aanbieders van AI-systemen, maar dat het ook de organisaties die ze daadwerkelijk in gebruik nemen verantwoordelijkheden oplegt. In overweging 93 benadrukt de verordening dat risico's niet alleen

tijdens de ontwikkeling en het ontwerp kunnen ontstaan, maar ook door het gebruik van het systeem:

“Gebruiksverantwoordelijken van AI-systemen met een hoog risico spelen daarom een cruciale rol bij het waarborgen van de bescherming van de grondrechten, in aanvulling op de verplichtingen van aanbieders bij de ontwikkeling van het AI-systeem.”

Zij zijn immers:

“(...) het best in staat om te begrijpen hoe het AI-systeem met een hoog risico concreet zal worden gebruikt en kunnen derhalve potentiële aanzienlijke risico's identificeren die niet in de ontwikkelingsfase voorzien werden, want zij hebben preciezere kennis van de gebruikcontext, de personen of groepen personen die waarschijnlijk zullen worden geraakt, met inbegrip van kwetsbare groepen”⁵³

Artikel 26 van de AI-verordening beschrijft de kern van deze verplichtingen. Allereerst moeten AI-systemen worden gebruikt zoals beschreven in de gebruiksaanwijzing. Aanbieders hebben namelijk, als het goed is, bij het opstellen van deze instructies al zoveel mogelijk rekening gehouden met de bescherming van grondrechten. Daarnaast zijn gebruiksverantwoordelijken verplicht het functioneren van de systemen te monitoren en, wanneer zich een concreet risico voordoet of een incident plaatsvindt, de aanbieder en de bevoegde autoriteiten te informeren. In dergelijke gevallen moet het gebruik van het systeem bovendien onmiddellijk worden gestaakt.⁵⁴

Artikel 27 creëert vervolgens een belangrijke verplichting voor gebruiksverantwoordelijken die openbare diensten verlenen, zowel private organisaties als publiekrechtelijke organen. Deze moeten een beoordeling van de gevolgen voor grondrechten

47 EU High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy Artificial Intelligence', 8 april 2019.

48 Zie bijvoorbeeld: L. Enqvist, "Human Oversight" in the EU Artificial Intelligence Act: What, When and by Whom? Law, Innovation and Technology, 2023/15. Zie ook de koppeling met het verbod op volledig geautomatiseerde besluitvorming in artikel 22 AVG en de bijbehorende jurisprudentie en literatuur zoals HvJEU, C-634/21, ECLI:EU:C:2023:957, 7 december 2023 (SCHUFA Holding).

49 Overweging 73 AI-verordening.

50 Zie ook de connectie met artikel 22 AVG. Zie HvJEU, 7 december 2023, c-634/21 (SCHUFA holding).

51 Artikel 14(4) AI-verordening.

52 Artikel 14(4)b.

53 Overweging 93 AI-verordening.

54 Artikel 26(5) en overweging 91 en 93 AI-verordening.

uitvoeren, voordat zij een systeem met een hoog risico in gebruik nemen. Ook wel naar verwezen als ‘*Fundamental Rights Impact Assessment*’ of kortweg ‘*FRIA*’.⁵⁵ Dit is een belangrijke grondrechtelijke waarborg bij het gebruik van AI in het leveren van publieke diensten.⁵⁶ Het doel van de beoordeling is om de specifieke risico’s voor de rechten van personen of groepen die waarschijnlijk worden getroffen in kaart te brengen en vervolgens te bepalen hoe deze risico’s kunnen worden

ondervangen.⁵⁷ De bepaling noemt een aantal noodzakelijke elementen voor de beoordeling, die betrekking hebben op het identificeren van risico’s binnen de specifieke gebruikscontext en op de wijze waarop deze risico’s kunnen worden beperkt. Het EU AI-bureau ontwikkelt hiervoor een sjabloon.⁵⁸ In Nederland is de ‘*Impact Assessment Mensenrechten en Algoritmes*’ of kortweg ‘*IAMA*’ ontwikkeld die ook houvast zou kunnen bieden.⁵⁹

AI-modellen voor algemene doeleinden (hoofdstuk V)

De AI-verordening creëert een apart regime voor AI-modellen voor algemene doeleinden (GPAI), met aanvullende normen voor modellen die een systeemrisico opleveren. Deze zijn toegevoegd aan de verordening door de opkomst van krachtige generatieve AI-systemen en modellen zoals ChatGPT, Claude en andere *foundation models*.

De algemene normen voor GPAI-systemen zijn te vinden in artikel 53. Aanbieders moeten onder andere technische documentatie bijhouden, een auteursrechtbeleid voeren, en een publieke samenvatting van trainingsdata aanleveren. Daarnaast zijn er aanvullende normen voor modellen met een systeemrisico (artikel 55) zoals modevaluatie, *adversarial testing*, het inventariseren van de systemische risico’s en cybersecurity. De verordening licht toe in overweging 110 dat deze systemische risico’s ook echt gaan over grondrechten rondom thema’s zoals veiligheid, desinformatie, en discriminatie. Toezicht ligt niet op nationaal niveau, maar bij het AI-bureau. Echter, samenwerking wordt gezocht wanneer GPAI-systemen gecombineerd worden met AI-systemen met een hoog risico die weer onder de nationale toezichthouders vallen.

3.3 Transparantieverplichtingen en AI-testomgevingen (hoofdstuk IV en VI)

Transparantieverplichtingen (hoofdstuk IV)

Zoals aangegeven in de bespreking van artikel 13 kan transparantie een belangrijke mensenrechtelijke waarborg zijn. Waar artikel 13 transparantieverplichtingen creëert voor alleen aanbieders van AI-systemen met een hoog risico,⁶⁰ creëert artikel 50 transparantieverplichtingen voor zowel aanbieders als gebruiksverantwoordelijken met betrekking tot een aantal specifiek type AI-systemen ongeacht of ze aangewezen zijn als hoog risico.

Het gaat om mensen informeren als ze interacteren met een AI-systeem of wanneer ze het onderwerp zijn van emotieherkenningssysteem of biometrische categorisatie, en om duidelijk maken wanneer content AI-gegenereerd is of wanneer iets een *deepfake* betreft. Dit kan bijvoorbeeld gelden voor chatbots of online content op sociale media. De precieze invulling van deze verplichtingen wordt verder uitgewerkt door het EU AI-bureau in praktijkcodes.

AI-testomgevingen (hoofdstuk VI)

Hoofdstuk VI richt zich op het ondersteunen van innovatie. Daartoe moeten, op grond van artikel 57, lidstaten AI-testomgevingen voor regelgeving

55 Artikel 27(1) AI-verordening.

56 Zie A. Mantelero, ‘[The Fundamental Rights Impact Assessment \(FRIA\) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template](#)’. *Computer Law & Security Review* 2024/54 en ENNHRI, ‘[ENNHRI calls on the European Commission to ensure effective Fundamental Rights Impact Assessments \(FRIAs\) under the EU AI Act](#)’, 7 april 2025.

57 Overweging 96 AI-verordening.

58 Artikel 27(5) AI-verordening.

59 Zie de [IAMA](#).

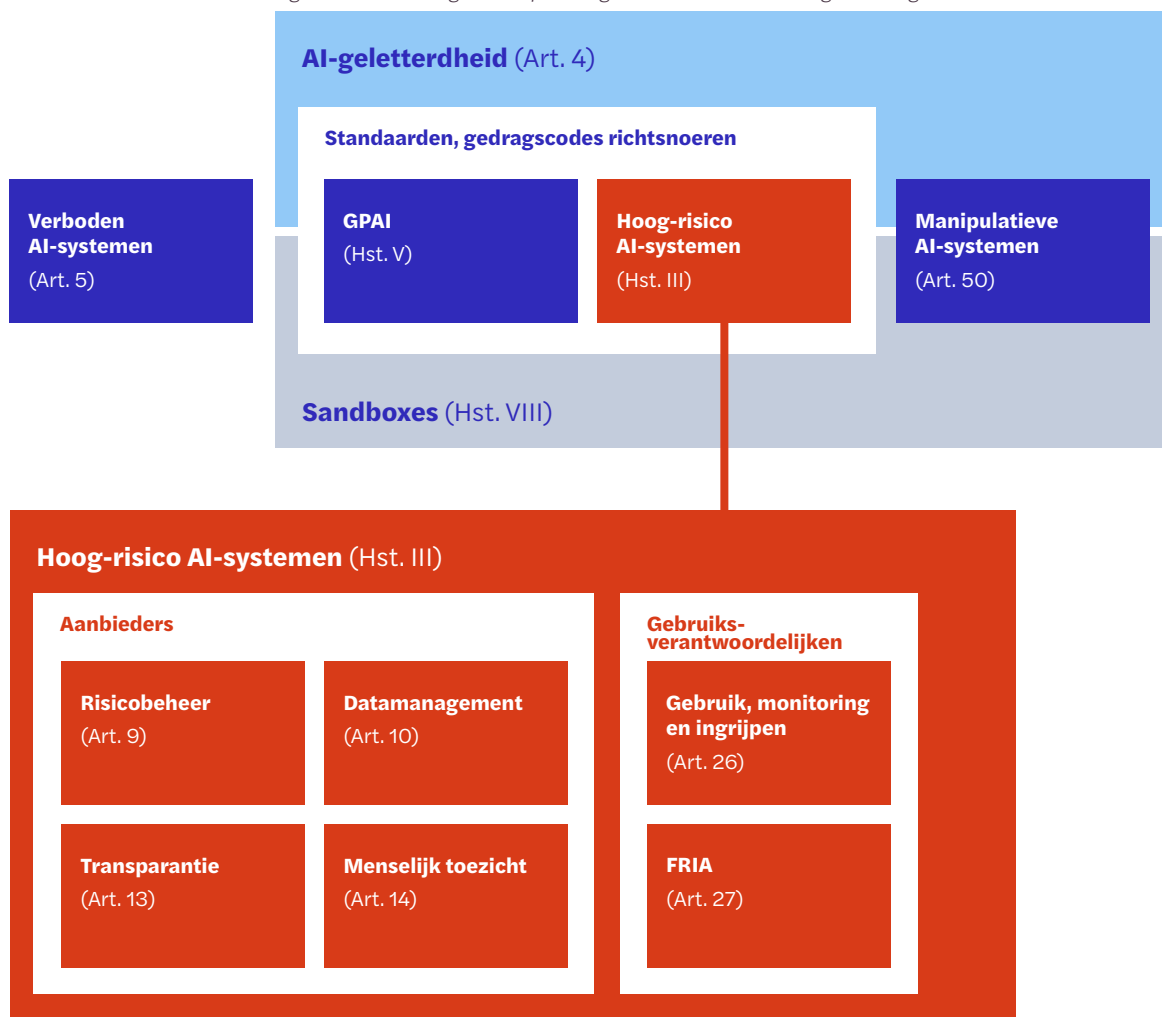
60 Via artikel 16 AI-verordening.

ontwikkelen: gecontroleerde omgevingen waarin AI-systemen getest en ontwikkeld kunnen worden voordat ze op de markt verschijnen. Het doel van deze testomgevingen is tweeledig: ze bevorderen rechtszekerheid en markttoegang en maken het mogelijk om opgedane lessen effectief te delen. Nationale toezichthouders begeleiden deze testomgevingen, leveren supervisie en helpen bij het identificeren van risico's, waaronder ook grondrechtenrisico's.⁶¹

De uitvoering van deze testomgevingen voor regelgeving verschilt per lidstaat. Sommige lidstaten

bieden vooral een vragenloket, terwijl anderen een volledige testomgeving inrichten.⁶² Ongeacht de vorm is het identificeren en adresseren van grondrechtenrisico's altijd een essentieel onderdeel. In Nederland is de testomgeving bij het schrijven van deze tekst nog in ontwikkeling; naar verwachting zal begin 2026 een vragenloket operationeel zijn, later gevolgd door een uitgebreidere testomgeving.⁶³ Op Europees niveau bestaan meerdere complementaire programma's die innovatie in vergelijkbare testomgevingen ondersteunen op een manier die voldoende bescherming biedt voor onder meer grondrechten.⁶⁴

Figuur 1: Verhouding van verplichtingen uit de AI-verordening die aan grondrechten raken.



61 Artikel 57(6) AI-verordening. De verordening schrijft geen verplichte betrokkenheid van grondrechtenautoriteiten voor, maar een rol in de identificaties van risico's en de beantwoording van vragen is te voorzien.

62 [Overzicht van hoe lidstaten de AI-testomgeving voor regelgeving aanvliegen](#) van artificialintelligenceact.eu.

63 Zie [RDI voorstel](#), 25 maart 2025.

64 Zie bijvoorbeeld de [European Digital Innovation Hubs](#), [EUSAIR project](#), de [AI Continent Action Plan](#), en de [Sectoral AI Testing and Experimentation Facilities](#).

4. Grondrechtenrisico's van Bijlage III hoog-risico AI-systemen

De AI-verordening onderscheidt twee categorieën AI-systemen met een 'hoog risico' waarvoor de aanvullende verplichtingen uit hoofdstuk 3 gelden. Zoals daar besproken, verwijst het 'hoog risico' specifiek naar de kans dat deze systemen grondrechten van mensen aantasten.⁶⁵

Artikel 6 van de verordening geeft aan dat de volgende systemen als hoog risico worden aangemerkt:⁶⁶

- AI-systemen die in Bijlage III van de verordening staan, óf
- AI-systemen die worden gebruikt in de context van in Bijlage I genoemde productwetgeving.

Dit hoofdstuk richt zich op de grondrechtenrisico's van de genoemde systemen in Bijlage III. De risico's van systemen die verband houden met producten uit Bijlage I worden apart besproken. Voor alle genoemde systemen in Bijlage III wordt aangegeven welke grondrechten het meest waarschijnlijk worden geraakt en, waar beschikbaar, wordt een voorbeeld gegeven van de mogelijke impact. Hoewel in theorie bij de meeste systemen genoeg alle grondrechten geraakt kunnen worden, komen vaak enkele rechten als eerste in beeld. Daarbij geldt dat het recht op non-discriminatie in vrijwel alle contexten relevant blijft.

4.1 Biometrische AI-systemen

Aangewezen AI-systemen

- A. Biometrische identificatie op afstand
- B. Biometrische categorisatie op basis van gevoelige of beschermde kenmerken
- C. Emotieherkenningsysteem

De AI-verordening benoemt drie typen biometrische systemen als systemen met een hoog risico. Deze systemen worden in de praktijk al ingezet, bijvoorbeeld gezichtsherkenningssoftware door de politie bij demonstraties,⁶⁷ of digitale horloges die gezondheidsdata analyseren.⁶⁸

Bijzonder aan biometrische systemen is dat zij in vrijwel iedere context gebruikt kunnen worden, waarbij de betrokken grondrechten afhangen van de specifieke toepassing. De andere zeven categorieën zijn daarentegen gericht op, en begrensd door een bepaalde sector. Deze keuze is gemaakt vanwege de intieme en persoonlijke

⁶⁵ Zie ook hiervoor in sectie 3.2.

⁶⁶ Onder specifieke voorwaarden hoeven aanbieders wiens AI-systemen onder de definitie van hoog risico vallen toch niet aan de verplichtingen uit hoofdstuk III AI-verordening te voldoen, zie de filterbepalingen van artikel 6(3) en (4) AI-verordening. Voor een bespreking zie FRA, [Assessing High-risk Artificial Intelligence: Fundamental Rights Risks](#), 2025, p. 23.

⁶⁷ Amnesty, [Recording Dissent: Camera Surveillance at Peaceful Protests in the Netherlands](#), 16 oktober 2024.

⁶⁸ Autoriteit Persoonsgegevens, [Rapportage AI & Algoritmes Nederland](#), 5 juli 2025, hoofdstuk 3.

aard van biometrische gegevens.⁶⁹ Hierdoor kunnen biometrische AI-systemen ook diepgaand ingrijpen op iemands grondrechten en autonomie, omdat diens lichaam immers het directe onderwerp van het AI-systeem is. Door hun bijzondere karakter gelden ook aanvullende verplichtingen, bijvoorbeeld op het gebied van transparantie.⁷⁰

Ongeacht de context, zijn bij biometrische AI-systemen in ieder geval het recht op privacy (art. 7 Handvest) en gegevensbescherming (art. 8 Handvest) van belang. Ook het recht op non-discriminatie (art. 21 Handvest) kan snel geraakt worden bij biometrische systemen, met name bij gezichtsherkenning of emotiedetectie.⁷¹ Specifiek noemenswaardige contexten zijn die van rechtshandhaving, onderwijs en arbeid waar het gebruik van biometrische systemen vanwege de gevoelige aard deels verboden is.⁷²

4.2 AI-systemen in kritieke infrastructuur

Aangewezen AI-systemen

Veiligheidscomponent bij het kritieke infrastructuur (wegverkeer, water, gas, verwarming en elektriciteit)

Bij AI in kritieke infrastructuur staat betrouwbaarheid centraal. Een fout kan immers verregaande gevolgen hebben. Denk bijvoorbeeld aan de impact op mensen met een kwetsbare gezondheid wanneer de verwarming uitvalt in een koude winter. Of de impact van het wegvallen van schoon drinkwater uit de kraan, met name voor mensen die aan huis gebonden zijn. Hoewel deze systemen minder complexe maatschappelijke dynamieken met zich meebrengen, kan onder meer het recht op respect voor het privéleven en socialezekerheidsrechten geraakt worden, bijvoorbeeld als bepaalde groepen disproportioneel risico lopen.

4.3 Onderwijs en beroepsopleiding

Aangewezen AI-systemen

- A. Toelating tot onderwijsniveau of instelling
- B. Evaluatie leerresultaten
- C. Beoordeling passend onderwijsniveau
- D. Monitoring toetsen

Er is een levendige maatschappelijke discussie over de digitalisering van het onderwijs in het algemeen, en het gebruik van AI in het bijzonder.⁷³ De zorgen gaan vooral om de vraag in hoeverre de technologie toegankelijk is voor iedereen, in hoeverre het daadwerkelijk inzicht geeft over het individuele leerproces, de afhankelijkheid van grote technologiebedrijven, leerlingen die buiten de boot kunnen vallen, en ten slotte ook over overmatige controle en surveillance van leerlingen. Daarnaast worden de voordelen gezien in het kunnen aansluiten bij de individuele leerbehoeftes, een passend leerniveau kunnen toewijzen, en om de integriteit van toetsing en diplomering te beschermen.

De AI-verordening inventariseert zelf expliciet de mensenrechten die geraakt kunnen worden:

“Wanneer dergelijke systemen op ondeugdelijke wijze zijn ontworpen en worden gebruikt, kunnen zij bijzonder ingrijpend zijn en in strijd zijn met het recht op onderwijs en opleiding, alsook met het recht niet te worden gediscrimineerd, en kunnen historische patronen van discriminatie in stand worden gehouden, bijvoorbeeld ten nadele van vrouwen, bepaalde leeftijdsgroepen, personen met een handicap of personen met een bepaalde raciale of etnische afkomst of seksuele gerichtheid.”⁷⁴

69 Overweging 54 AI-verordening.

70 Artikel 5(3), 14(5) 50(3) en overweging 63 AI-verordening.

71 Zie bijvoorbeeld J. Buolamwini en T. Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” *Proceedings of Machine Learning Research Conference on Fairness, Accountability, and Transparency*, 2018/81 p. 1–15.

72 Artikel 5 AI-verordening en zie onderdeel 3.1.

73 Zie bijvoorbeeld: E. Smeets, R. Geurts, en D. van Helvoirt, *Algoritmen in het Onderwijs: Een onderzoek in opdracht van het College voor de Rechten van de Mens*, 2024 en B. Karstens en L. Kool, *Naar Hoogwaardig Digitaal Onderwijs*, *Rathenau Instituut*, 2022.

74 Overweging 56 AI-verordening. Betreft respectievelijk artikel 14 en 21 Handvest.

Een voorbeeld in Nederland betreft een student die klaagde bij het College dat surveillancesoftware haar gezicht niet herkende vanwege haar donkere huidskleur.⁷⁵ Onder de AI-verordening zou dit systeem nu als hoog risico worden geclassificeerd, met strengere transparantie-eisen en toezichtmogelijkheden om discriminatie te voorkomen.

4.4 Werkgelegenheid

Aangewezen AI-systemen

- A. Systemen voor werving en selectie
- B. Systemen die van invloed zijn op o.a. arbeidsvoorwaarden, contractuele betrekkingen, monitoring of evaluatie.

De opname van arbeidsgerichte AI-systemen in Bijlage III van de AI-verordening vloeit voort uit een groeiende bezorgdheid over digitale uitbuiting en discriminatie op de arbeidsmarkt.⁷⁶

AI-systemen worden in steeds grotere mate ingezet in werving en selectie. Onderzoek laat zien dat deze systemische vooroordelen kunnen versterken en al hebben geleid tot discriminatie op basis van geslacht, etniciteit of leeftijd.⁷⁷ Daarnaast is er door campagnes tegen de uitbuiting van platformwerkers aandacht voor de manier waarop platformbedrijven algoritmes gebruiken om

werknemers te controleren en sturen, wat aanleiding geeft tot zorgen over arbeidsuitbuiting.⁷⁸ Deze ontwikkelingen onderstreepten de noodzaak om arbeidsgerichte AI-systemen als hoog-risicosystemen te classificeren.⁷⁹

Relevante mensenrechten zijn allereerst non-discriminatie (art. 21 Handvest), gegevensbescherming (art. 8 Handvest) en privacy (art. 7 Handvest). Daarnaast zijn specifieke werknemersrechten van groot belang. Zo is het recht op collectieve onderhandelingen (art. 28 Handvest) relevant: AI-systemen kunnen de aard van arbeidsrelaties ingrijpend veranderen, bijvoorbeeld door gepersonaliseerde arbeidsvoorwaarden aan te bieden, waardoor traditionele collectieve onderhandelingsstructuren worden ondermijnd, vooral in platformwerk.⁸⁰ Ook het recht op informatie en consultatie is belangrijk (art 27 Handvest). Gebrek aan transparantie en uitlegbaarheid kan het recht van werknemers ondermijnen om geïnformeerd te worden over beslissingen die hun werk en arbeidsvoorwaarden beïnvloeden.⁸¹

Een concreet voorbeeld uit Nederland betreft rechtszaken tegen taxiplatforms Uber en Ola. Chauffeurs claimden dat zij geautomatiseerd werden ontslagen en geen verhaal konden halen. Het Hof oordeelde dat er sprake was van oneigenlijk ontslag en verboden geautomatiseerde profilering.⁸²

75 College voor de Rechten van de Mens, [2023-111](#) (antispieksoftware Proctorio).

76 Zie bijvoorbeeld: European Parliament. Directorate General for Parliamentary Research Services, [Data Subjects, Digital Surveillance, AI and the Future of Work](#), 2020 en het College voor de Rechten van de Mens over [digitalisering in werving in selectie en discriminatie](#).

77 Zie bijvoorbeeld: College voor de Rechten van de Mens, [Recruiter of Computer? Zo voorkom je als werkgever discriminatie door algoritmes bij werving en selectie](#), december 2021; de Zwart, H., & Wiggers, P. (2022). *Als de machine kiest: diversiteit en inclusie in kunstmatige intelligentie voor werving en selectie*. Hogeschool van Amsterdam.

78 Zie bijvoorbeeld Human Rights Watch, [The Gig Trap: Algorithmic, Wage and Labor Exploitation in Platform Work in the US](#), 2022.

79 Ook heeft het geleid tot de platformwerkrichtlijn: Richtlijn (EU) 2024/2831 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende de verbetering van de arbeidsvoorwaarden bij platformwerk. Voor een bespreking zie [‘The EU Platform Work Directive: What’s new, what’s missing, what’s next?’](#) ETUI, 6 augustus 2024.

80 Zie ook Internationale Arbeidsorganisatie, Verdrag betreffende het recht zich te organiseren en collectief te onderhandelen 1949(nr. 98).

81 Zie ook Richtlijn 2002/14/EG van het Europees Parlement en de Raad van 11 maart 2002 tot vaststelling van een algemeen kader betreffende de informatie en de raadpleging van de werknemers in de Europese Gemeenschap.

82 Hof Amsterdam, 4 april 2023, ECLI:NL:GHAMS:2023:793 en [persbericht Workers Info Exchange](#).

4.5 Essentiële diensten

Aangewezen AI-systemen

- A. Systemen die beoordelen of iemand in aanmerking komt voor overheidsuitkeringen of -diensten
- B. Systemen die besluiten over kredietwaardigheid of -score
- C. Systemen mbt levens- of ziektekostenverzekering
- D. Classificatie noodoproepen

AI gebruikt bij overheidsdiensten, zoals fraudeopsporing door risicoprofilering, staat de afgelopen jaren hoog op de maatschappelijke agenda.

In Nederland is dit te herleiden tot controverses rond het toeslagenschandaal en Systeem Risico Indicatie.⁸³ Vooral het toeslagenschandaal heeft geleid tot een bredere bereidheid om zorgvuldiger om te gaan met algoritmes binnen overheidsdiensten. Dit resulteerde in de oprichting van de ‘algoritmetoezichthouder’ bij de Autoriteit Persoonsgegevens (de Directie Coördinatie Algoritmes),⁸⁴ als ook de ontwikkeling van een reeks beleidsinstrumenten zoals het algoritme-register en verschillende impactassessments en richtlijnen voor het beoordelen van algoritmes.⁸⁵

AI-systemen in deze context raken vaak aan sociale grondrechten die minder direct afdwingbaar zijn, maar ook aan wel direct afdwingbare rechten zoals non-discriminatie en rechtsbescherming.

De AI-verordening somt in overweging 58 zelf al op welke grondrechten voor de deelonderwerpen relevant zijn: Voor sub a (overheidsuitkeringen en diensten) gaat het om het recht op sociale

bescherming (Art. 34 Handvest), non-discriminatie (Art. 21 Handvest), menselijke waardigheid (Art. 1 Handvest) en een doeltreffende voorziening in rechte (Art. 47 Handvest). Bij sub b (kredietwaardigheid) en sub c (verzekeringen) identificeert de AI-verordening vooral financiële uitsluiting en discriminatie als belangrijke risico (Art. 21 Handvest). Ten slotte raakt sub d (noodoproepen) aan “het leven en de gezondheid van personen en hun eigendom” (Art. 2 en 17 Handvest).

4.6 Rechtshandhaving⁸⁶

Aangewezen AI-systemen

- A. Beoordelen risico dat iemand slachtoffer wordt van een misdrijf
- B. Leugendetectors
- C. Beoordelen betrouwbaarheid van bewijsmateriaal
- D. Beoordelen risico op recidive
- E. Profileren van mensen

De inzet van risicoprofileringsystemen in het kader van rechtshandhaving is het onderwerp van stevige maatschappelijke discussies. Vooral de zogenoemde *predictive policing*-systemen (sub a, d en e) vormen een heikel punt. Maatschappelijke organisaties pleiten al lange tijd voor een volledig verbod op het gebruik van dergelijke AI-systemen door de politie, vanwege de risico's voor grondrechten.⁸⁷ Ook de Wetenschappelijke Adviesraad van de politie adviseerde om niet verder te investeren in algoritmische toepassingen die gericht zijn op het voorspellen van (crimineel) gedrag op individueel niveau, juist vanwege de bijbehorende grondrechtenrisico's.⁸⁸

83 Zie Kamerstukken II, 2023-2024, 35 867, nr. 6 (rapport parlementaire enquête fraudebeleid en Dienstverlening: blind voor mens en recht) en Rechtbank Den Haag, 5 februari 2020, ECLI:NL:RBDHA:2020:865 (SyRI).

84 Kamerstukken II, 2022-2023, 26 643, nr. 953.

85 Zie de [IAMA](#), [het algoritmekader](#), en [het toetsingskader risicoprofilering](#) ontwikkeld door het College.

86 Deze categorie AI-systemen met een hoog risico ligt dicht tegen twee andere categorieën aan: De categorie biometrische AI (specifiek de biometrische identificatie op afstand in Annex III(1)a) en het verbod op real time biometrische surveillance (artikel 5 AI-verordening). Beide gaan immers ook over het gebruik van AI door rechtshandavingsautoriteiten.

87 Zo pleiten ALLAI, Fair Trials, Algorithm Watch, Amnesty, Bits of Freedom en EDRI [allen voor een totaal](#) verbod op predictive policing waar de AI-verordening bevat slechts een gedeeltelijk verbod bevat, alleen voor geïndividualiseerde risicoscores die alleen op basis van profilering of persoonskenmerken plaatvinden

88 Wetenschappelijke Adviesraad Politie, [Navigeren in Niemandslan. Zeven urgente uitdagingen rondom digitalisering en AI in politiewerk](#), juni 2025, p. 21.

Verschillende grondrechten kunnen ernstig geschonden worden door het gebruik van AI-systemen in het kader van rechtshandhaving, zoals het recht op een eerlijk proces (art. 47 Handvest). De AI-verordening erkent dit expliciet en stelt dat deze systemen kunnen leiden tot “controle, arrestatie of vrijheidsberoving van natuurlijke personen” en andere negatieve effecten op grondrechten, waarbij het “aanzienlijke machtsverschil” tussen autoriteiten en burgers deze risico’s nog verergert.⁸⁹

Het grootste risico ligt op het gebied van discriminatie en gelijke behandeling vooral wanneer AI-systemen getraind zijn op problematische historische data of onvoldoende getest zijn (Art. 21 Handvest). Dit heeft in het recente verleden al tot stigmatisering en diepe schade geleid.⁹⁰ Daarnaast kan het vermoeden van onschuld fundamenteel worden aangetast wanneer AI-systemen individuen als potentiële criminelen

classificeren zonder dat sprake is van daadwerkelijk strafbaar handelen.⁹¹ Ook het recht op een eerlijk proces en de rechten van verdediging kunnen zoals gezegd worden bedreigd, omdat veel AI-systemen ondoorzichtig zijn en burgers onvoldoende inzicht geven in de besluitvorming.⁹² Daarnaast kan het recht op privacy worden geschonden door de grootschalige verzameling en analyse van gegevens die nodig is voor *predictive policing* en profileringsystemen (Art. 7 en 8 Handvest).

Een relevant praktijkvoorbeeld komt uit de gemeente Amsterdam. Het locatie gebaseerde *predictive policing*-systeem CAS (Criminaliteits Anticipatie Systeem) wordt daar sinds 2015, niet zonder kritiek, gebruikt.⁹³ Het systeem verdeelt de stad in een raster en voorspelt per blok hoe hoog het risico op strafbare feiten is, om vervolgens de politie-inzet in de stad te informeren.

Bijlage I: nog een lijst AI-systemen met een hoog risico

Naast de lijst in Bijlage III is er ook een categorie systemen die op basis van Bijlage I kunnen kwalificeren als hoog risico. Hier gaat het om AI-systemen die onderdeel zijn van een breed scala aan producten waar de EU geharmoniseerde regels voor heeft opgesteld: medische hulpmiddelen, speelgoed, auto's, vliegtuigen en nog meer. Op basis van artikel 6(1) gelden ze als hoog risico wanneer:

- Het AI-systeem valt onder één van de wetten opgesomd in Bijlage I. Dit kan zijn als product of als veiligheidscomponent van een product. Één:
- Dit product dat onder één van de wetten in Bijlage I valt moet op basis van die wetgeving zelfstandig een conformiteitsbeoordeling doorlopen.

Bij deze categorie systemen met een hoog risico gaat het vooral om de veiligheid en gezondheid van mensen. Naast privacy, gegevensbescherming en non-discriminatie komen andere grondrechten minder snel in beeld.

89 Zie overweging 59 AI-verordening.

90 Amnesty, *Automated Racism: How police data and algorithms code discrimination into policing*, februari 2025.

91 Zie overweging 42 van de AI-verordening, die expliciet stelt dat mensen “nooit mogen worden beoordeeld op basis van door AI voorspeld gedrag dat uitsluitend gebaseerd is op hun profilering, persoonlijkheidskenmerken of kenmerken” zonder redelijk vermoeden gebaseerd op objectieve feiten. Overweging 59 waarschuwt dat “de uitoefening van belangrijke procedurele grondrechten, zoals het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, evenals de rechten van de verdediging” kunnen worden belemmerd “wanneer dergelijke AI-systemen onvoldoende transparant, verklaarbaar en gedocumenteerd zijn”.

92 Zie ook overweging 59 AI-verordening.

93 Voor een omschrijving zie het [algoritmeregister](#). De [Algemene Rekenkamer](#) was in 2022 zeer kritisch over de inzet van dit systeem. Ook [Amnesty](#) heeft zich kritisch geuit.

4.7 Migratie, asiel en grensbeheer

Aangewezen AI-systemen

- A. Leugendetectors
- B. Beoordelen risico op illegale migratie of veiligheid van iemand die het land betreedt
- C. Behandeling van aanvragen voor asiel, visa of verblijfsvergunningen
- D. Identificatie van mensen

De toepassing van AI-systemen in de context van migratie, asiel en grensbeheer vindt plaats tegen een complexe en zorgelijke maatschappelijke achtergrond, waarin het steeds striktere grensbeleid van de EU in toenemende mate op AI-systemen steunt.⁹⁴

De AI-verordening benadrukt de “bijzonder kwetsbare positie” van mensen die in een migratie- en asielcontext onderwerp zijn van dergelijke technologieën.⁹⁵ Daarbij legt de verordening direct de link met de risico's voor hun mensenrechten:

“De nauwkeurigheid, niet-discriminerende aard en transparantie van de AI-systemen die in deze context worden gebruikt, zijn derhalve van bijzonder belang om de eerbiediging van de grondrechten van de betrokken personen te waarborgen, en met name hun recht op vrij verkeer, non-discriminatie, bescherming van privéleven en persoonsgegevens, internationale bescherming en goed bestuur.”⁹⁶

Ook benadrukt de verordening dat het gebruik van AI-systemen in migratie, asiel en grensbeheer

niet gebruikt mogen worden door staten om hun verplichtingen onder het VN-vluchtelingenverdrag te omzeilen of gebruikt mogen worden om inbreuk te maken op het beginsel van non-refoulement.⁹⁷

Naast deze algemene risico's brengen de specifieke technologieën die aangewezen worden in Bijlage III ook hun eigen potentiële problemen met zich mee. Zo bestaat controversie rond het gebruik van leugendetectors, die zeer snel tot discriminatie kunnen leiden, vooral in cultureel diverse contexten.⁹⁸ Een relevant voorbeeld is het project ‘iBorderCtrl’;⁹⁹ een controversieel Europees systeem voor geautomatiseerde grenscontrole. Hierbij moeten reizigers via een videoverbinding een interview afleggen met een avatar die fungeert als een *automatic deception detection system*.¹⁰⁰

4.8 Rechtsbedeling en democratische processen

Aangewezen AI-systemen

- A. Systemen gebruikt in de rechtspleging
- B. Systemen die de uitslag van een verkiezing of referendum beïnvloeden

Deze laatste categorie AI-systemen met een hoog risico omvat systemen die mogelijk de kern kunnen raken van de democratische rechtsstaat en de impact die deze kunnen hebben op “de individuele vrijheden en het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht”.¹⁰¹ De verordening benadrukt dat ook bij rechtmatig gebruik van een AI-systeem bij rechtspleging dat

94 Y. Yang, F. Zuiderveen Borgesius, P. Beckers en E. ‘Automated decisionmaking and artificial intelligence at European borders and their risks for human rights’. Preprint, arXiv, 2024.; C. Jones and R. Lanneau, *Automating Authority: Artificial intelligence in European police and border regimes*, State Watch, april 2025; European Parliament. Directorate General for Parliamentary Research Services. *Artificial Intelligence at EU Borders: Overview of Applications and Key Issues*. Publications Office, 2021.

95 Overweging 60 AI-verordening.

96 Overweging 60 AI-verordening. Zie onder andere artikel 21, 7, en 8 Handvest.

97 Overweging 60 AI-verordening.

98 Zie bijvoorbeeld: Autoriteit Persoonsgegevens, *Rapportage AI & Algoritmes Nederland*, 5 juli 2025, hoofdstuk 3 en N. Vavoula, ‘Regulating AI at Europe’s Borders. Where the AI Act Falls Short.’ *Verfassungsblog*, 13 december 2024.

99 Voor een omschrijving zie: iborderctrl.no/start en cordis.europa.eu/project/id/700626.

100 Zie de [projectomschrijving](https://projectomschrijving.cordis.europa.eu) op cordis.europa.eu. Er is veel kritiek op de ontwikkeling van het gehele systeem. Voor een overzicht zie: iborderctrl.no/start. Specifieke kritiek gaat op de leugendetectiefunctie, voornamelijk gebaseerd op het feit dat de detectie van ‘micro-expressies’ onvoldoende wetenschappelijk onderbouwd is. Zie: iborderctrl.no/blog:bio-markers-of-scientific-deceit en J. Sánchez-Monedero en L. Dencik. ‘The Politics of Deceptive Borders: “Biomarkers of Deceit” and the Case of iBorderCtrl’. *Information, Communication & Society* 25, 2022/3 p 413-30.

101 Overweging 61 AI-verordening. Zie Artikel 47 Handvest.

“de uiteindelijke besluitvorming moet een door de mens aangestuurde activiteit blijven”.¹⁰² In Nederland ontwikkelt de rechterlijke macht stapsgewijs beleid voor het gebruik van AI.¹⁰³

De tweede categorie systemen richt zich op het beïnvloeden van verkiezingen. De verordening koppelt deze toepassingen aan de relevante regelgeving voor politieke campagnes en omvat elk type systeem dat raakt aan het fundamentele kiesrecht (art. 4 van de Grondwet).

¹⁰² Overweging 61 AI-verordening.

¹⁰³ ‘[Landelijk programma Artificiële Intelligentie](#)’, Rechtspraak, 5 juni 2025.

5. Grondrechtentoezicht in de AI-verordening

5.1 Toezichtstructuur en integratie van grondrechten

Het belang van het beschermen van grondrechten bij de ontwikkeling en inzet van AI komt duidelijk naar voren in de manier waarop de AI-verordening handhaving en toezicht vormgeeft. Een analyse van hoe de verordening grondrechten wil beschermen is daarom onvolledig zonder een overzicht van het toezichtmechanisme.¹⁰⁴

De toezichtstructuur van de AI-verordening is gebaseerd op het Europese ‘Nieuwe Wetgevingskader’ voor productveiligheid.¹⁰⁵ In de formule van het Wetgevingskader staan de markttoezichthouders centraal in de handhaving. Daarnaast leunt het voor een belangrijk deel op marktpartijen in de vorm van zelfevaluatie en certificering door private partijen. Marktpartijen beoordelen zichzelf en elkaar op conformiteit en certificeren producten voordat ze op de markt komen.

Deze aanpak is veelal effectief om productveiligheid te verzekeren waarbij technische defecten centraal staan. Fabrikanten voeren conformiteitsbeoordelingen uit, andere private instanties certificeren complexere producten, en markttoezichthouders controleren achteraf of de regels worden nageleefd. AI-systemen brengen daarbovenop echter een ander type complexere risico's en potentiële problemen met zich mee. De AI-verordening beoogt daarom meer te beschermen dan de fysieke veiligheid en stelt

mede de bescherming van grondrechten centraal bij de regulering van AI. De primaire manier waarop de verordening dit verankerd heeft in de handhaving is door het introduceren van een nieuwe actor in het markttoezicht: de grondrechtenautoriteit.¹⁰⁶

5.2 Rol van grondrechtenautoriteiten

Grondrechtenautoriteiten zijn bestaande overheidsinstanties of -organen die zich bezighouden met de bescherming van fundamentele rechten, zoals gelijke behandeling of mensenrechten, en worden door lidstaten vastgesteld. In de verschillende lidstaten is een breed palet aan typen instanties aangewezen, met name mensenrechteninstellingen, gelijke behandelingsorganen, gegevensbeschermingsautoriteiten en ombudsmannen.¹⁰⁷ Zij werken allemaal aan de bescherming van grondrechten en kunnen in hun mandaat in aanraking komen met AI-systemen met een hoog risico.

Naast hun bestaande bevoegdheden kent de AI-verordening deze autoriteiten in artikel 77 enkele specifieke bevoegdheden toe. Zo zijn zij bevoegd documentatie over een specifiek AI-systeem op te vragen en kunnen zij de markttoezichthouder verzoeken een systeem technisch te testen.¹⁰⁸ Deze bevoegdheden dragen bij aan het uitvoeren van het bestaande mandaat van de verschillende typen grondrechtenautoriteiten, maar leggen ook de basis voor een proactieve signaleringsrol van de grondrechtenautoriteiten

¹⁰⁴ Ten tijde van schrijven werkt de Europese Commissie aan een geüpdatete *interpretative note* over de rol en verantwoordelijkheden van de artikel 77 autoriteiten. Deze sectie geeft daarom slechts een lezing van de AI-verordening op hoofdlijnen.

¹⁰⁵ Mededeling van de Commissie, De Blauwe Gids van 2022: richtlijnen voor de uitvoering van de productvoorschriften van de EU, 2022/C 247/01.

¹⁰⁶ Artikel 77 AI-verordening.

¹⁰⁷ Zie [de geconsolideerde lijst](#) van de Europese Commissie met alle aangewezen grondrechtenautoriteiten.

¹⁰⁸ Respectievelijk Artikel 77(1) en (3) AI-verordening.

in het markttoezicht. Het versterkt de positie van grondrechtenautoriteiten om onderzoek te doen naar specifieke systemen en om signalen bij de desbetreffende markttoezichthouder neer te leggen.

Naast deze bevoegdheden die de onderzoeks, monitorings- en signaleringsfunctie versterken, speelt de grondrechtenautoriteit op punten ook een rol in het casusgerichte markttoezicht. Zo moet bijvoorbeeld de markttoezichthouder de relevante grondrechtenautoriteiten informeren als er grondrechtenrisico's worden vastgesteld bij een specifiek AI-systeem, of wanneer een ernstig incident heeft plaatsgevonden.¹⁰⁹ Daarnaast werken de grondrechtenautoriteit(en) en de markttoezichthouder samen bij de evaluatie van de conformiteit van AI-systemen waarbij grondrechtenrisico's zijn vastgesteld.¹¹⁰

Zo draagt de AI-verordening bij aan een toezicht waarbij grondrechtenautoriteiten hun expertise kunnen inzetten voor zowel signalering en monitoring, als evaluatie van specifieke AI-systemen met hoog risico.

5.3 De markttoezichthouder als cruciale schakel in grondrechtentoezicht

Uit het vorige onderdeel blijkt al duidelijk dat de markttoezichthouder een sleutelrol speelt in het grondrechtentoezicht. Als centrale actor in het markttoezicht betreft zij op het juiste moment de grondrechtenautoriteiten. Dit gebeurt concreet in de volgende situaties:

- Bij een melding van een ernstig incident met grondrechtenschendingen, informeert de markttoezichthouder de relevante grondrechtenautoriteiten.¹¹¹
- Bij vermoeden van grondrechtenrisico's bij een systeem, informeert de markttoezichthouder de grondrechtenautoriteiten en verleent deze zijn volledige medewerking.¹¹²
- In voortkomend geval wordt de evaluatie van systemen met mogelijke grondrechtenrisico's in samenwerking met de grondrechtenautoriteiten uitgevoerd.¹¹³
- Wanneer een systeem formeel aan alle vereisten voldoet maar toch nog grondrechtenrisico's inhoudt, kan de markttoezichthouder na raadpleging van de grondrechtenautoriteit aanvullende maatregelen opleggen.¹¹⁴

Het vermogen om deze toezichtsverplichtingen goed uit te voeren, zal afhangen van of markttoezichthouders goed in staat zijn adequaat te identificeren wanneer welke grondrechtenrisico's kunnen optreden. Zeker nu de verantwoordelijkheid bij hen ligt om de juiste grondrechtenautoriteit(en) op het juiste moment te betrekken. Dit is des te meer van belang, nu naar verwachting in de praktijk veel casussen een grondrechtelijke dimensie hebben waar mogelijk ook verschillende grondrechtenautoriteiten betrokken zijn.

5.4 Uitvoering van grondrechtentoezicht in Nederland¹¹⁵

De uitvoering van het toezicht verschilt aanzienlijk per lidstaat.¹¹⁶ Op basis van adviezen van de relevante toezichthouders is in Nederland gekozen voor een vrij gecentraliseerde benadering.¹¹⁷ Het College is aangewezen als grondrechtenautoriteit voor fundamentele rechten in brede zin, terwijl de Autoriteit Persoonsgegevens specifiek

¹⁰⁹ Artikel 73(7), 79(2) en 82 AI-verordening.

¹¹⁰ Artikel 79(2) AI-verordening.

¹¹¹ Artikel 73(7) AI-verordening.

¹¹² Artikel 79(2) AI-verordening.

¹¹³ Artikel 79(2) AI-verordening.

¹¹⁴ Artikel 82(1) AI-verordening.

¹¹⁵ Ten tijde van de publicatie van dit document is de toezichtsstructuur in Nederland nog niet formeel vastgelegd.

¹¹⁶ Zie het overzicht in voetnoot 107.

¹¹⁷ Kamerstukken II, 2024/25, 22112, nr. 3979.

grondrechtenautoriteit voor gegevensbescherming is. Daarnaast zijn hoge colleges van recht vastgesteld als autoriteiten voor AI-gebruik binnen de rechtspraak, om de onafhankelijkheid van de rechterlijke macht te waarborgen.¹¹⁸ Het College heeft in de inrichtingsfase van het Nederlandse grondrechtentoezicht aangegeven dat het waarde hecht aan een taakopvatting waar de grondrechtenautoriteit naast het casusgerichte toezicht ook een actieve en proactieve rol speelt in onderzoek, advisering, signalering en voorlichting.¹¹⁹

Deze hybride structuur, die traditioneel markttoezicht combineert met grondrechtenexpertise, is innovatief maar complex. De effectiviteit hangt af van heldere verantwoordelijkheidsverdeling, efficiënte informatie-uitwisseling en voldoende capaciteit bij alle betrokken autoriteiten.¹²⁰ De komende jaren zijn cruciaal voor het verder ontwikkelen van deze samenwerkingsstructuur en het opdoen van praktijkervaring in het toezicht op AI in een snel veranderende technologische omgeving.

118 De procureur-generaal bij de Hoge Raad, de voorzitter van de Afdeling Bestuursrechtspraak van de Raad van State, het gerechtsbestuur van de Centrale Raad van Beroep, en het gerechtsbestuur van het College van Beroep voor het bedrijfsleven.

119 Brief van het College voor de Rechten van de Mens, 'Advies met betrekking tot het inrichten van grondrechtentoezicht voor Artificiële Intelligentie (AI)', 18 oktober 2024.

120 Zo ook: M. Almada en N. Petit, 'The EU AI Act: Between the rock of product safety and the hard place of fundamental rights', (2025), 62, *Common Market Law Review*, Issue 1, pp. 85-120 en F. Palmiotto, '[The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation](#)', *European Journal of Risk Regulation*. 2025;16(2):770-793.

6. Conclusie: toezicht op AI betekent het beschermen van grondrechten

De AI-verordening maakt duidelijk dat effectief toezicht op kunstmatige intelligentie in de kern draait om de bescherming van grondrechten. Dit uitgangspunt is niet alleen zichtbaar in de risicobenadering van de verordening, waarin grondrechtenrisico's centraal staan, maar is door de gehele verordening heen verweven als leidend principe.

Het is echter niet vanzelfsprekend dat de grondrechtenbescherming die de AI-verordening biedt en die in deze publicatie is besproken, in de praktijk ook daadwerkelijk effectief zal functioneren. Door de verschillende hoofdstukken heen zijn meerdere aandachtspunten benoemd waar implementatie van de verordening extra zorg vereist. Twee aspecten verdienen hierbij bijzondere nadruk.

De eerste categorie betreft de verplichtingen in de verordening die vrij abstract geformuleerd zijn en die pas concreet worden via bijvoorbeeld technische standaarden of een model voor een grondrechteneffectenbeoordeling. De effectiviteit van deze bepalingen hangt grotendeels af van hoe gedetailleerd en bruikbaar deze standaarden en modellen worden opgesteld.

De tweede categorie heeft betrekking op de bescherming die afhankelijk is van de vaardigheden en capaciteiten van aanbieders, gebruiksverantwoordelijken en toezichthouders. Alleen als deze partijen grondrechtenrisico's adequaat kunnen inschatten, kunnen de vereisten uit Hoofdstuk III van de verordening en het grondrechtentoezicht in de praktijk effectief worden toegepast. Als horizontale wetgeving

overstijgt de AI-verordening sectorgrenzen en raakt zij vrijwel alle grondrechten. Van het recht op privacy en non-discriminatie tot vrijheid van meningsuiting en het recht op een eerlijk proces. Deze brede reikwijdte benadrukt dat AI-systemen potentieel ingrijpende gevolgen kunnen hebben voor vrijwel alle aspecten van het maatschappelijke leven. Het is daarom cruciaal dat aanbieders, gebruiksverantwoordelijken en toezichthouders niet alleen begrijpen hoe de AI-verordening beoogt grondrechten te beschermen, maar ook goed inzicht hebben in de concrete risico's die AI-systemen voor grondrechten in hun eigen context kunnen opleveren. Grondige kennis van de specifieke context en de relevante grondrechten is noodzakelijk om de AI-verordening effectief toe te passen en te handhaven.

www.mensenrechten.nl

