FACULTEIT
RECHT EN CRIMINOLOGIE

BETEKENISVOLLE TRANSPARANTIE BIJ DE TOEPASSING VAN AI-SYSTEMEN

EEN ANALYSE VAN DE TRANSPARANTIEVERPLICHTINGEN IN DE ALGEMENE VERORDENING GEGEVENSBESCHERMING EN HET VOORSTEL VOOR EEN VERORDENING BETREFFENDE ARTIFICIËLE INTELLIGENTIE

Aantal woorden: 33.352

Annelore Mattart
Studentennummer: 01809110

Promotor: Prof. dr. Eva Lievens
Commissaris: dhr. Carl Vander Maelen

Masterproef voorgelegd voor het behalen van de graad master in de rechten.
Disclaimer: deze masterproef is een examendocument waarvan de inhoud niet werd gecorrigeerd.

Academiejaar: 2022-2023

UNIVERSITEIT
GENT

VOORWOORD

Met deze masterproef sluit ik een vijf jaar durende opleiding Rechten aan de Universiteit Gent af. Hiermee neem ik tegelijkertijd afscheid van een zeer boeiend en leerrijk hoofdstuk in mijn leven, mijn studententijd. Een periode die gekenmerkt werd door vele uitdagingen, maar bovenal een tijd was van groei, ontdekking en zelfontplooiing waarin ik mezelf en nieuwe vrienden leerde kennen, nieuwe vaardigheden leerde ontwikkelen en mijn persoonlijke visie op de wereld verfijnde. Deze masterproef, het resultaat van maandenlang hard werken, vormt het sluitstuk van deze boeiende periode. Met de eindmeet in zicht, wil ik dan ook van de gelegenheid gebruik maken om enkele personen te bedanken.

Vooreerst wil ik mijn promotor professor doctor Eva Lievens bedanken voor haar vertrouwen in mij, haar constructieve feedback en haar kostbare tijd doorheen dit traject. Ik had me geen betere promotor kunnen wensen. Ook wil ik mijn copromotor Carl Vander Maelen bedanken voor de waardevolle feedback. Uw suggesties en aanwijzingen hebben immers bijgedragen tot het verbeteren van de algehele kwaliteit van mijn masterproef.

Daarnaast wil ik ook een zeer oprechte ‘dankjewel’ aan mijn ouders richten voor hun oeverloze geduld, de motiverende woorden en de vele kansen die ze mij hebben geboden. Ik besef dat ik dit te weinig uitspreek, maar zonder jullie had ik niet gestaan waar ik nu sta. Daar ben ik jullie uit de grond van mijn hart dankbaar voor. Ook wil ik mijn zus Liselotte bedanken voor de onvoorwaardelijke zusterliefde. Jouw liefde, optimisme en steun hebben mij door de moeilijke tijden geloodst.

Ten slotte wil ik ook mijn vriendinnen bedanken voor de broodnodige momenten van ontspanning, gezellige babbels en vele lachbuien. Zonder jullie had mijn studententijd er helemaal anders uitgezien. Bedankt voor jullie vriendschap en voortdurende aanmoedigingen.

Deze masterproef markeert niet alleen het einde van mijn studie, maar ook het begin van een nieuw hoofdstuk in mijn leven waarin ik mijn talenten en kwaliteiten verder kan ontwikkelen; een avontuur dat ik nieuwsgierig en enthousiast tegemoet treed.

Annelore Mattart , 26 april 2023

SAMENVATTING

Deze masterproef analyseert de mate waarin de transparantieverplichtingen in de Algemene Verordening Gegevensbescherming (AVG) en het Voorstel voor een Verordening betreffende Artificiële Intelligentie (Voorstel) samen betekenisvolle transparantie bieden ten aanzien van de aan het AI-systeem onderworpen personen bij de toepassing van artificiële intelligentie (AI). De AVG representeert het huidig gegevensbeschermingsrechtelijk kader op Europees niveau dat het gegevensbeschermingsrecht als grondrecht maximaal poogt te eerbiedigen. Gezien AI-systemen in de regel grote hoeveelheden persoonsgegevens nodig hebben om optimaal te functioneren en tegelijkertijd aanzienlijke risico's kunnen creëren voor de rechten en vrijheden van personen, is de AVG belangrijk voor de bestrijding van deze risico's.

Echter, algemeen wordt aangenomen dat de aard van AI – meer specifiek AI-systemen die gebruik maken van *machine learning* methoden – juridische uitdagingen creëert voor de toepassing van de transparantievereisten in de AVG. Door hun complexe en ondoorzichtige besluitvorming (*black box*-karakter), en de mogelijkheid tot *self learning*, wordt het inzicht in de gegevensverwerking door deze AI-systemen beperkt. Zo bezitten AI-systemen het vermogen om enorme hoeveelheden data te verwerken op steeds complexere en minder transparante manieren, waardoor de transparantievereisten, zoals gestipuleerd in de AVG, niet vanzelfsprekend toepasbaar zijn in de context van AI.

Om tegemoet te komen aan de behoefte om in een aangepast regelgevend kader te voorzien, publiceerde de Europese Commissie op 21 april 2021 het Voorstel. In dit Voorstel werd gepoogd de unieke eigenschappen van AI aan te pakken opdat deze geautomatiseerde systemen verenigbaar zouden zijn met onder meer het recht op gegevensbescherming. Meer bepaald tracht het Voorstel complementair te zijn aan de AVG. Zodoende te kunnen oordelen of het Voorstel daadwerkelijk deze functie vervult – en bijgevolg in staat is om samen met de AVG betekenisvolle transparantie te verzekeren ten aanzien van de aan het AI-systeem onderworpen personen – worden de transparantieverplichtingen in beide rechtsinstrumenten geanalyseerd en kritisch geëvalueerd aan de hand van een zelf ontwikkelde definiëring van betekenisvolle transparantie. Deze definiëring wordt vertaald in een transparantiekader.

Dit kader wordt op beide wetgevende instrumenten toegepast, op grond waarvan de juridische uitdagingen in de AVG en het Voorstel met betrekking tot het bereiken van betekenisvolle transparantie visueel kunnen worden waargenomen. Uit de integratie van beide transparantiekaders, wordt de mate waarin de AVG en het Voorstel betekenisvolle transparantie bieden ten aanzien van de aan het AI-systeem onderworpen personen, visueel geïllustreerd.

INHOUDSTAFEL

LIJST MET AFKORTINGEN

AI	Artificiële Intelligentie
ANN	Artificiële Neurale Netwerken
AVG	Algemene Verordening Gegevensbescherming
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	Europese Unie
GEB	Gegevensbeschermingseffectbeoordeling
GOFAI	Good Old-Fashioned Artificial Intelligence
HLEG AI	High Level Expert Group on Artificial Intelligence
IoT	Internet of Things
NLP	Natural Language Processing
Voorstel	Voorstel voor een Verordening betreffende Artificiële Intelligentie

INLEIDING

Hoofdstuk 1: Situering van het onderwerp

Afdeling 1: Probleemstelling

1. Artificiële Intelligentie ('AI') zit structureel verankerd in de werking van onze huidige maatschappij en bezit het vermogen om verscheidene aspecten van ons werk én leven aanzienlijk te beïnvloeden. Hoewel AI-systemen het potentieel bezitten om een brede waaier van maatschappelijke voordelen en sociaaleconomische groei te genereren, kunnen deze technieken echter ook een aantal fundamentele grondrechten, zoals privacy, non-discriminatie en gegevensbescherming negatief beïnvloeden.

2. In het bijzonder creëert de aard van AI – meer specifiek AI-systemen die gebruik maken van *machine learning* methoden – onder meer juridische uitdagingen voor de toepassing van het transparantiebeginsel in de Algemene Verordening Gegevensbescherming ('AVG').[1] Dit beginsel stelt voorop dat persoonsgegevens ten aanzien van betrokkenen op een transparante manier worden verwerkt en houdt onder meer de verplichting in voor verwerkingsverantwoordelijken om betrokkenen op gemakkelijk toegankelijke manier te informeren over hoe en welke persoonsgegevens worden verwerkt, alsook te worden gewezen op de risico's, waarborgen en rechten met betrekking tot de verwerking.[2]

3. Door hun complexe en ondoorzichtige besluitvorming (*black box*) en de mogelijkheid tot *self learning*, wordt het inzicht in de gegevensverwerking door deze AI-systemen beperkt. Zo bezitten AI-systemen het vermogen om enorme hoeveelheden data te verwerken op steeds complexere en (soms) minder transparante manieren, waardoor het transparantiebeginsel, zoals gestipuleerd in de AVG, niet vanzelfsprekend toepasbaar is in de context van AI.[3] De vraag rijst dan ook – vanuit juridisch oogpunt – in welke mate de huidige rechtsregels toepasbaar zijn op AI. Dit maakt tot op heden een veelbesproken onderwerp uit in de literatuur.

---

[1] Verord.Raad nr. (EU) 2016/679, 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb.L.* 4 mei 2016, afl. 119, 7; C. GIAKOUMOPOULOS, G. BUTTARELLI en M. O'FLAHERTY, *Handboek Europese gegevensbeschermingswetgeving*, Luxemburg, Bureau voor publicaties van de Europese Unie, 2021, 419.

[2] Art. 5, lid 1, a) AVG

[3] M. FIERENS, E. VAN GOOL en J. DE BRUYNE, "De regulering van artificiële intelligentie (deel 1) - Een algemene stand van zaken en een analyse van enkele vraagstukken inzake consumentenbescherming", *RW* 2021, (962) 962.

Afdeling 2: Stand van zaken

4. De AVG omvat het huidig wetgevend kader dat de verwerking van persoonsgegevens door onder meer AI-systemen reguleert. Aangezien AI-systemen in de regel grote hoeveelheden persoonsgegevens nodig hebben om optimaal te functioneren en tegelijkertijd aanzienlijke risico's kunnen creëren voor de rechten en vrijheden van personen, zijn de bepalingen in de AVG belangrijk voor de bestrijding van deze risico's door het bieden van passende waarborgen in de vorm van informatieverplichtingen en controlemechanismen.[4] Echter, zoals eerder aangegeven, lijkt dit kader niet volledig aangepast aan de unieke eigenschappen van AI, waardoor het met heel wat uitdagingen af te rekenen heeft in AI-context.

5. Om te vermijden dat de unieke eigenschappen van AI een gebrek aan transparantie (en vertrouwen) veroorzaakt, achtte de Raad van de Europese Unie het noodzakelijk deze eigenschappen aan te pakken opdat deze geautomatiseerde systemen verenigbaar zouden zijn met onder meer het recht op gegevensbescherming.[5] In navolging van deze vaststelling, publiceerde de Europese Commissie op 21 april 2021 een Voorstel voor een Verordening tot vaststelling van geharmoniseerde regels betreffende Artificiële Intelligentie ('Voorstel') om tegemoet te komen aan de behoefte om in een aangepast regelgevend kader te voorzien dat het vertrouwen van burgers, overheden en bedrijven in AI versterkt door de potentiële risico's van AI op te vangen.[6]

Hoofdstuk 2: Het onderzoek

Afdeling 1: Onderzoeksopzet

6. Deze masterproef beoogt de transparantieverplichtingen in beide Europese rechtsinstrumenten in context van AI kritisch te evalueren, teneinde een antwoord te kunnen formuleren op de vraag in welke mate deze geponeerde transparantieverplichtingen resulteren in betekenisvolle transparantie ten aanzien van de aan het AI-systeem onderworpen personen.

---

[4] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 6.

[5] Concl.Raad nr. 11481/20, 21 oktober 2020 over het Handvest van de Grondrechten in de context van artificiële intelligentie en digitale verandering, https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/nl/pdf, 3.

[6] Voorstel (Comm.) voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie, 21 april 2021, COM'2021) def – 2021/0106 (COD).

Afdeling 2: Maatschappelijke en wetenschappelijke relevantie

7. AI-technologieën worden steeds prominenter gepositioneerd in onze samenleving. 2023 wordt door experts zelfs beschouwd als hét kantelpunt voor digitale technologie die lang als futuristisch werd bestempeld.[7] Op vandaag heeft AI een punt van maturiteit bereikt waardoor het niet langer als een randfenomeen kan worden beschouwd. Dit bleek des te duidelijker met de ontwikkeling van ChatGPT. Sinds het Californisch bedrijf Open AI eind vorig jaar zijn chatbot ChatGPT lanceerde, werd dit onthaald als het iPhone-moment voor AI.[8] Waar de iPhone in 2007 de manier van werken en leven drastisch veranderde, wordt dat ook verwacht van taalsoftware.[9]

Echter, volgens Chuck Robbins, CEO van techreus Cisco, heeft dergelijke technologie met een geweldig positieve kracht, ook een grote negatieve kracht. Zo kan generatieve AI worden gebruikt voor *fake* informatie of overtuigende phishingmails.[10]

8. De exponentiële groei van AI-technologieën, alsook de toename van de daaraan gekoppelde risico's en maatschappelijke voordelen, versterkte vanuit de beleidswereld en academische kringen de roep naar een meer passend en adequaat rechtskader dat burgers vertrouwen moet geven om op AI gebaseerde technologieën te omarmen en bedrijven te stimuleren AI-systemen te ontwikkelen.[11] Daarbij is vertrouwen van essentieel belang. Immers, als AI-systemen niet aantoonbaar te vertrouwen zijn, kan het gebruik ervan worden belemmerd, waardoor de potentieel grote sociale en economische voordelen van AI-systemen niet kunnen worden verwezenlijkt.[12]

9. Dit vertrouwen kan maar ontstaan wanneer burgers de impactvolle beslissingen van AI-systemen begrijpen, en indien nodig daartegen bezwaar kunnen maken.[13]

---

[7] W. DE PRETER, B. SERRURE en R. LEGRAND, "De techtrends van 2023:iPhone-moment breekt aan voor AI", De Tijd, 27 december 2022, https://www.tijd.be/dossiers/de-vooruitblik/de-techtrends-van-2023-iphone-moment-breekt-aan-voor-ai/10437322.html.

[8] B. SERRURE, "Microsoft profiteert mee van AI-hype", De Tijd, 26 april 2023, https://www.tijd.be/ondernemen/technologie/microsoft-profiteert-mee-van-ai-hype/10463654.html.

[9] S. DE SMEDT, "'Vragen hoe slim ChatGPT is, is als vragen hoe sportief mijn stofzuiger is'", De Tijd, 10 maart 2023, https://www.tijd.be/content/tijd/nl/mme-articles/10/45/32/33/10453233.

[10] R. LEGRAND, "Overheden moeten zich sneller voorbereiden op de bedreigingen van AI", De Tijd, 7 maart 2023, https://www.tijd.be/ondernemen/technologie/cisco-topman-overheden-moeten-zich-sneller-voorbereiden-op-bedreigingen-van-ai/10451824.html.

[11] Titel 1.1. Memorie van Toelichting Voorstel voor een Verordening betreffende Artificiële Intelligentie.

[12] THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (HLEG AI), *Ethische Richtsnoeren voor Betrouwbare KI,* 8 april 2019, https://op.europa.eu/nl/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1#,6.

[13] I. VAROSANEC, "On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI", *International Review of Law, Computers & Technology* 2022, (95) 95.

Het komt erop aan te kunnen vertrouwen dat de verwerking van (persoons)gegevens door AI-systemen in lijn ligt met de wettelijke voorschriften en ethische normen én dat dit vertrouwen kan worden toegeschreven aan alle mensen en processen die bij de levenscyclus van het AI-systeem betrokken zijn.[14] Transparantie is bijgevolg een noodzakelijke voorwaarde opdat deze maatschappelijke ontwikkeling doordacht kan plaatsvinden.

Afdeling 3: Onderzoeksvragen

Deze masterproef beoogt een antwoord te formuleren op de centrale onderzoeksvraag die luidt als volgt:

> ***"Zorgen de AVG en het Voorstel voor betekenisvolle transparantie ten aanzien van de aan het AI-systeem onderworpen personen?"***

Om de centrale onderzoeksvraag te kunnen beantwoorden, zal eveneens een antwoord worden gezocht op twee deelvragen die helpen de centrale onderzoeksvraag te beantwoorden. Deze luiden als volgt:

> ***"Zijn er grenzen aan de definiëring van de transparantievereisten in de AVG bij de toepassing van AI-systemen?"***

> ***"Waarin verschilt de invulling van de transparantievereisten in de AVG ten opzichte van de transparantievereisten in het Voorstel?"***

Afdeling 4: Onderzoeksmethode

4.1. Algemeen

10. Deze masterproef maakt het voorwerp uit van klassiek juridisch onderzoek op basis waarvan verschillende juridische en andere wetenschappelijke relevante bronnen bestudeerd en geanalyseerd zullen worden om op de voorgaande onderzoeksvragen een helder antwoord te kunnen formuleren. Klassiek juridisch onderzoek beoogt de kennis van en het inzicht in het recht te vergroten door beginselen, rechtsregels en juridische begrippen systematisch te beschrijven en te ordenen om onduidelijkheden en leemten in het bestaande recht aan te pakken.[15]

---

[14] THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (HLEG AI), *Ethische Richtsnoeren voor Betrouwbare KI,* 8 april 2019, https://op.europa.eu/nl/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1#, 49.

[15] J. SMITS, "What is Legal Doctrine? On The Aims and Methods of Legal-Dogmatic Research" in R. VAN GESTEL, H. MICKLITZ en E. RUBIN (eds.), *Rethinking Legal Scholarship: A Transatlantic Dialogue*, New York, Cambridge University Press, 2017, (207) 210.

Deze doelstelling sluit nauw aan bij de onderzoeksopzet van deze masterproef, namelijk de juridische aspecten van transparantie in de AVG en het Voorstel in de context van AI analyseren, interpreteren en kritisch evalueren.

11. Om dit mogelijk te maken, zal een kwalitatieve onderzoeksmethode worden gehanteerd bij het verrichten van het onderzoek. Deze methode lijkt het meest aangewezen, aangezien de nadruk specifiek wordt gelegd op het verzamelen van gedetailleerde informatie om met kennis van zaken een duidelijk en adequaat antwoord te kunnen formuleren op de eerdergenoemde onderzoeksvragen. De onderzoeksstrategie behelst het literatuuronderzoek, op grond waarvan gebruik wordt gemaakt van bestaande, door anderen geproduceerde kennis (kennisbronnen), om via reflectie tot nieuwe inzichten te komen.

Deze masterproef maakt het voorwerp uit van interdisciplinair onderzoek dat twee domeinen, met name het juridische en het technologische, met elkaar verbindt. Immers, de juridische aspecten van transparantie in AI-context kunnen slechts adequaat worden beoordeeld als rekening wordt gehouden met de reële grenzen van het technologisch kader.

4.2. Dataverzameling

12. Om een antwoord te kunnen formuleren op de onderzoeksvragen, wordt uit vijf soorten bronnen informatie geëxtraheerd. Het gaat met name om de AVG, het Voorstel, rechtsleer omtrent de problematiek inzake transparantie in AI-context (beschikbaar in de juridische databanken en tijdschriften), en richtsnoeren en aanbevelingen van het EDPB en de EDPS.

4.3. Analysemethode

13. De verzamelde data worden geanalyseerd aan de hand van een kwalitatieve inhoudsanalyse. De eerste deelvraag noopt tot beschrijvende kennis met het oog op het definiëren/beschrijven van de transparantievereisten in de AVG en haar eventuele grenzen. Het antwoord op deze vraag, wordt in hoofdzaak gebaseerd op rechtsleer die de problematiek inzake transparantie in AI-context tot voorwerp heeft. De tweede deelvraag noopt tot beschrijvende kennis met het oog op het preciseren van de invulling van het juridisch concept transparantie in twee verschillende Europese rechtsinstrumenten. Dit laat toe gelijkenissen en verschillen te identificeren.

14. Ten slotte noopt de centrale onderzoeksvraag tot beschrijvende en verklarende kennis met het oog op het evalueren van de transparantievereisten, zoals gedefinieerd in de AVG en het Voorstel. Aan de hand van deze onderzoeksvraag wordt nagegaan of het juridisch concept transparantie in deze rechtsinstrumenten bijdraagt tot betekenisvolle transparantie bij de toepassing van AI. Om deze

beoordeling te kunnen maken, wordt beroep gedaan op het eigen inzicht en analysevermogen. Om een zinvolle analyse van de transparantievereisten in beide Europese rechtsinstrumenten mogelijk te maken, werd in het bijzonder een kader gecreëerd waarin een eigen conceptualisering en definiëring van betekenisvolle transparantie ontwikkeld werd, gebaseerd op (en in lijn met) de reeds bestaande academische literatuur hieromtrent.

Hoofdstuk 3: De indeling

15. Teneinde een duidelijk antwoord te kunnen formuleren op de centrale onderzoeksvraag, is het vooreerst noodzakelijk een duidelijk technologisch begrippenkader te hanteren waarbinnen deze onderzoeksvraag moet worden gesitueerd. Dit technologisch kader – waarin het begrip AI en enkele andere fundamentele concepten worden gedefinieerd – wordt in deel I van deze masterproef beschreven.

16. In deel II wordt het juridisch kader, bestaande uit de AVG en het Voorstel, geschetst. In dit juridisch kader worden transparantieverplichtingen geponeerd. Om een degelijke analyse mogelijk te maken van de transparantieverplichtingen in deze rechtsinstrumenten, alsook een kritische houding te kunnen aannemen tijdens het analyseren ervan, is het noodzakelijk om het ruimere kader waarbinnen beide Europese rechtsinstrumenten zich situeren, te duiden. In het bijzonder wordt aandacht besteed aan de ontstaansgeschiedenis, het toepassingsgebied, de relevante actoren, de rol van transparantie in beide rechtsinstrumenten en de verhouding tussen beide.

17. In deel III van deze masterproef wordt het zelf geconstrueerd transparantiekader geduid waarin de transparantieverplichtingen in de AVG en het Voorstel later (in deel IV en V) worden ingepast. In deel IV wordt het transparantiekader specifiek toegepast op de AVG. In dit deel worden de verschillende transparantievereisten in de AVG – die rusten op verwerkingsverantwoordelijken wanneer zij persoonsgegevens verwerken – in het zelf ontwikkelde kader ingevuld en kritisch geëvalueerd. Aan de hand van deze bevindingen, zal een antwoord worden geformuleerd op de eerste deelvraag, namelijk "zijn er grenzen aan de definiëring van de transparantievereisten in de AVG bij de toepassing van AI-systemen?".

18. In deel V wordt het transparantiekader specifiek toegepast op het Voorstel. In dit deel worden eveneens de verschillende transparantievereisten – die rusten op aanbieders, dan wel gebruikers van AI-systemen – in het zelf ontwikkelde kader ingevuld en kritisch geëvalueerd. Deze vaststellingen faciliteren het antwoord op de tweede deelvraag, namelijk "waarin verschilt de invulling van de transparantievereisten in de AVG ten opzichte van de transparantievereisten in het Voorstel?", zodoende de eventuele meerwaarde van de transparantievereisten in het Voorstel te kunnen beoordelen.

19. Ten slotte worden de bevindingen uit deel IV en V geïntegreerd in een allesomvattende conclusie (deel VI). Deze conclusie wordt aan de hand van het transparantiekader gevisualiseerd en toegelicht. In het bijzonder poogt deel VI een duidelijk antwoord te formuleren op de centrale onderzoeksvraag, namelijk: “zorgen de AVG en het Voorstel voor betekenisvolle transparantie ten aanzien van de aan het AI-systeem onderworpen personen?”.

DEEL I. TECHNOLOGISCH KADER

Hoofdstuk 1: Concept, definitie en benaderingen van AI

20. De term AI werd in 1956 bedacht tijdens het *Summer Research Project on Artificial Intelligence* aan het Dartmouth College in New Hampshire door John McCarthy die AI definieerde als *"the science and engineering of making intelligent machines"*.[16] Deze notie van AI werd door McCarthy geconcipieerd vanuit het idee machines te creëren die in staat zijn menselijke intelligentie te simuleren en deze problemen te laten oplossen die tot dan toe waren voorbehouden aan de mens.[17]

21. Er circuleren heel wat definities van AI, maar tot op heden bestaat er geen eenduidige, door experten universeel aanvaarde, definitie. Vanuit deze vaststelling werd in deze bijdrage ervoor geopteerd om de grote verscheidenheid aan definities van AI te herleiden tot drie wijzen waarop AI benaderd kan worden om zodoende AI ook te situeren. Een duidelijk begrippenkader vormt immers het fundament om de probleemstelling van dit onderzoek te duiden.

Afdeling 1: De benadering van AI als 'intelligent' vermogen

22. In eerste instantie kan AI gedefinieerd worden als intelligentie die wordt weergegeven of gesimuleerd door code (algoritmen) of machines.[18] Een algoritme - als basis voor intelligentie - is een reeks instructies die de machine zegt wat het moet doen om vanuit een gegeven begintoestand een bepaald doel te bereiken.[19] Deze benadering van AI doet echter vragen rijzen over de wijze waarop intelligentie dient te worden gedefinieerd. Hoewel dit concept reeds uitvoerig bestudeerd werd door psychologen, biologen en neurowetenschappers, blijft het vanuit filosofisch oogpunt een vaag concept waarover nog geen eensgezindheid lijkt te bestaan.[20]

23. Het best gekende concept om intelligentie te benaderen, is het concept van de menselijke intelligentie. In deze optiek omschreven Philip Jansen e.a. AI als *"the science and engineering of machines with capabilities that are considered intelligent by the standard of human intelligence"*.[21]

---

[16] Kenniscentrum Data & Maatschappij. (z.d.). *Artificial Intelligence*. Geraadpleegd op 23 augustus 2022, van https://data-en-maatschappij.ai/woordenlijst#artificial-intelligence.
[17] M. COECKELBERGH, *AI Ethics*, Cambridge, The MIT Press, 2020, 66.
[18] *Ibid*., 64.
[19] *Ibid*., 70.
[20] THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (HLEG AI), A Definition of AI: Main capabilities and scientific disciplines, 18 december 2018, https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf.
[21] P. JANSEN, S. BROADHEAD, R. RODRIGUES, D. WRIGHT, P. BREY, A. FOX en N. WANG, "State of the art review", 2018. Draft of the D4.1 deliverable submitted to the European Commission on April 13, 2018. A report for The SIENNA Project, an EU H2020 research and innovation program under grant agreement no. 741716.

Intelligentie wordt in deze definitie opgevat als een algemeen cognitief vermogen dat meer specifieke vermogens omvat, waaronder het vermogen om te leren, redeneren, problemen op te lossen, begrijpen etc.[22] Volgens deze definitie, betreft AI aldus de creatie van machines die denken, redeneren en handelen.[23]

De ontwerper van bekende intelligentietests David Wechsler definieerde intelligentie op zijn beurt *als "the global capacity of a person to act purposefully, to think rationally, and to deal effectively with his environment."*[24] Op grond van deze definitie, wordt in de rechtsleer AI onder meer omschreven als het vermogen van een machine om doelgericht te handelen, rationeel te denken en doeltreffend met zijn omgeving om te gaan, zoals de mens idealiter zou moeten doen.[25] Andere wetenschappers zijn voorstander van een meer neutrale definitie die losstaat van menselijke intelligentie. Zo omschrijft AI-onderzoekster Margaret Boden intelligentie als het bezitten van diverse informatieverwerkingscapaciteiten die niet noodzakelijk exclusief menselijk zijn.[26]

24. De Britse wiskundige en pionier in de computerwetenschappen, Alan Turing, introduceerde in 1950 de Turingtest, ook wel bekend als de *imitation game*, een gedachtenexperiment over machine-intelligentie dat vertrekt vanuit de vraag of machines kunnen denken.[27] Wanneer een computer erin slaagt om tijdens een gesprek een mens te misleiden betreffende zijn hoedanigheid, slaagt de computer voor de Turingtest en kan deze als intelligent worden beschouwd.[28] Het vermogen om het imitatiespel met succes te spelen, is namelijk het door Turing vooropgestelde *"criterion for thinking*".

25. Vanuit verschillende wetenschappelijke invalshoeken kwam er kritiek op de legitimiteit van de Turingtest.[29] Een belangrijk punt van kritiek werd geuit door de Amerikaanse filosoof John Searle die de stelling poneerde dat het bewijs van imitatie van intelligentie niet noodzakelijk het bewijs van intelligentie impliceert.[30] Ter ondersteuning van zijn standpunt bedacht hij het gedachtenexperiment, de 'Chinese kamer' waarin hij zich inbeeldt opgesloten te zitten in een kamer.[31]

---

[22] *Ibid.*
[23] M. COECKELBERGH, *AI Ethics*, Cambridge, The MIT Press, 2020, 64.
[24] R. DEVILLE, N. SERGEYSSELS en C. MIDDAG, "Basic Concepts of AI for Legal Scholars" in J. DE BRUYNE en C. VANLEENHOVE (eds.), *Artificial Intelligence and the Law*, Mortsel, Intersentia, 2021 (1) 2.
[25] *Ibid.*
[26] M. BODEN, *Its Nature and Future*, Oxford, Oxford University Press, 2016, 1.
[27] K. GABRIELS, *Regels voor robots. Ethiek in tijden van AI*, Brussel, VUBPRESS, 2019, 86.
[28] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 22.
[29] *Ibid*., 23.
[30] R. DEVILLE, N. SERGEYSSELS en C. MIDDAG, "Basic Concepts of AI for Legal Scholars" in J. DE BRUYNE en C. VANLEENHOVE (eds.), *Artificial Intelligence and the Law*, Mortsel, Intersentia, 2021 (1) 3.
[31] J. SEARLE, "Minds, Brains and Programs", The Behavioral and Brain Sciences 1980, 417-424.

Hij ontvangt van mensen buiten de kamer in eerste instantie telkens vellen papier met daarop voor hem betekenisloze symbolen (input).[32] Deze symbolen zijn eigenlijk Chinese tekens, maar dat weet hij zelf niet.[33] Daarnaast krijgt hij een Engelstalig instructieboek (computerprogramma) dat beschrijft hoe hij moet reageren op de symbolen.[34]

Vervolgens zoekt hij de symbolen in het instructieboek op en volgt systematisch de regels (bijvoorbeeld 'als je symbool X ziet, schrijf dan symbool Y').[35] In de volgende stap van het experiment dient Searle zijn eigenhandig geschreven symbolen (output) terug te geven aan de mensen buiten de kamer.[36] Buiten de kamer waarin hij zich bevindt, worden deze symbolen beschouwd als een geschreven dialoog in het Chinees en lijkt het dus alsof Searle Chinees begrijpt.[37] Searle echter voerde louter instructies uit, zonder de dialoog echt te begrijpen.[38] Op grond van deze bevinding, concludeert Searle dat als de persoon in de kamer geen Chinees begrijpt op basis van de implementatie van het juiste programma om Chinees te begrijpen, dan begrijpt ook geen enkele digitale computer uitsluitend op die basis Chinees omdat geen enkele computer iets heeft wat een persoon niet heeft.[39]

26. Met dit gedachtenexperiment wilde Searle aantonen dat de ogenschijnlijke vaststelling dat een systeem erin slaagt om een mens te imiteren, nog niet betekent dat het systeem ook werkelijk denkt als een mens.[40] Immers, het vermogen om informatie te verwerken en menselijk gedrag te imiteren, is niet hetzelfde als het vermogen om te denken en te begrijpen. Het louter volgen van voorgeprogrammeerde instructies is onvoldoende voor écht begrip en échte intelligentie.[41]

---

[32] *Ibid.*
[33] *Ibid.*
[34] *Ibid.*
[35] *Ibid.*
[36] *Ibid.*
[37] *Ibid.*
[38] *Ibid.*
[39] J. SEARLE, "Chinese room argument", Scholarpedia, 2009, http://www.scholarpedia.org/article/Chinese_room_argument.
[40] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 23.
[41] K. GABRIELS, *Regels voor robots. Ethiek in tijden van AI*, Brussel, VUBPRESS, 2019, 87.

Afdeling 2: De benadering van AI als een wetenschap

27. Naast de mogelijkheid om AI te definiëren als een artificieel 'intelligent' vermogen, toebehorend aan een machine, kan AI eveneens benaderd worden als een wetenschap.[42] Dit is met name het geval wanneer de voornaamste doelstelling van AI-onderzoek erin bestaat om het concept intelligentie en de daarmee verbonden cognitieve functies op systematische wijze te bestuderen.[43] Haar doel bestaat er dan in om de term intelligentie wetenschappelijk beter te duiden opdat een beter begrip van de mens en andere levende wezens die natuurlijke intelligentie bezitten, kan ontluiken.[44] In dit opzicht is AI als wetenschap gerelateerd aan andere wetenschappelijke disciplines zoals onder meer psychologie en de cognitiewetenschappen.[45]

Afdeling 3: De benadering van AI als een technologie

28. Wanneer AI-onderzoek in belangrijke mate gericht is op het ontwikkelen van technologieën voor verscheidene praktische doeleinden, wordt AI benaderd als een ingenieursdiscipline.[46] Zo omschrijven Steels e.a. AI als een wetenschappelijke en ingenieursdiscipline die tracht methoden en technologieën te vinden om systemen te bouwen die functies van het menselijk brein imiteren. AI kan dan de vorm aannemen van nuttige apparaten, ontworpen door mensen, voor praktische doeleinden die de schijn van intelligentie en intelligent gedrag wekken.[47]

29. Zoals uit voorgaande paragrafen blijkt, is het niet eenvoudig om AI eenduidig te beschrijven. Niettemin bevatten deze benaderingen en definities vaak een gemeenschappelijke component die het lerend vermogen (*infra* 13, nr. 34) van een computer of systeem benadrukt, waarbij data fungeren als brandstof.[48]

---

[42] M. COECKELBERGH, *AI Ethics*, Cambridge, The MIT Press, 2020, 67.
[43] P. JANSEN, S. BROADHEAD, R. RODRIGUES, D. WRIGHT, P. BREY, A. FOX en N. WANG, "State of the art review", 2018. Draft of the D4.1 deliverable submitted to the European Commission on April 13, 2018. A report for The SIENNA Project, an EU H2020 research and innovation program under grant agreement no. 741716.
[44] M. BODEN, *Its Nature and Future*, Oxford, Oxford University Press, 2016, 2.
[45] M. COECKELBERGH, *AI Ethics*, Cambridge, The MIT Press, 2020, 67.
[46] P. JANSEN, S. BROADHEAD, R. RODRIGUES, D. WRIGHT, P. BREY, A. FOX en N. WANG, "State of the art review", 2018. Draft of the D4.1 deliverable submitted to the European Commission on April 13, 2018. A report for The SIENNA Project, an EU H2020 research and innovation program under grant agreement no. 741716.
[47] M. BODEN, *Its Nature and Future*, Oxford, Oxford University Press, 2016, 2.
[48] T. BUYSE, "Frankenstein de baas blijven. Artificiële intelligentie in Vlaanderen", Gids op Maatschappelijk Gebied, 2021, (46) 48.

Hoofdstuk 2: Soorten AI

30. Er kunnen drie soorten van AI onderscheiden worden op basis van hun ontwikkelingsniveau: gerichte AI (*narrow AI*), algemene AI (*general AI*) en super AI (*superintelligence AI*).[49] Alle huidige werkende AI-systemen zijn voorbeelden van gerichte AI.[50] Gerichte AI betreft een technologie die uitsluitend in staat is om een bepaalde, zeer specifieke opdracht uit te voeren, zoals onder meer gezichtsherkenning, kanker opsporen, inschatten of iemand kredietwaardig is, etc.[51] Machines handelen *alsof* ze intelligent zijn.[52]

31. Algemene AI daarentegen, *is* intelligent.[53] Het is een technologie die in staat is om – al dan niet tegelijkertijd – meer dan één opdracht uit te voeren en om de informatie uit de ene opdracht ook voor een andere te gebruiken.[54] Het is een technologie die capabel is om elke cognitieve taak die menselijke intelligentie vereist, uit te voeren en hiermee de menselijke intelligentie evenaart.[55] Naast het bezitten van een algemeen cognitief vermogen, wordt algemene AI verondersteld ook over emotionele intelligentie te beschikken.[56] Deze technologie bestaat momenteel niet, maar wereldwijd stellen tal van ontwerpers en computerwetenschappers alles in het werk om deze technologie alsnog te verwezenlijken.[57]

32. Super AI, ten slotte, wordt gedefinieerd als een vorm van AI die in staat is de menselijke intelligentie te overtreffen door cognitieve vaardigheden te manifesteren en zelf denkvermogen te ontwikkelen. Deze soort van AI is een dankbaar onderwerp voor films en de populaire media, maar deze technologie bestaat nog lang niet en het is nog maar de vraag in hoeverre die er ooit komt.[58]

33. Hoewel een aantal prominente AI-onderzoekers, zoals onder meer Max Tegmark, dit onderscheid liever niet maken, is het voor deze masterproef in ieder geval van wezenlijk belang om een onderscheid te maken in wat AI momenteel kan, nog niet kan en potentieel nooit zal kunnen om angsten weg te nemen of er net vertrouwen in te creëren.[59] Deze opdeling is op vandaag vooral van belang voor het garanderen van draagvlak en maatschappelijke aanvaarding van AI als een belangrijke motor voor verdere maatschappelijke ontwikkelingen. De opdeling heeft dus geen technologische meerwaarde.

---

[49] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 21.
[50] L. LAUWAERT, *Wij, Robots*, Tielt, Lannoo Campus, 2021, 22.
[51] *Ibid*., 23.
[52] K. GABRIELS, *Regels voor robots. Ethiek in tijden van AI*, Brussel, VUBPRESS, 2019, 82.
[53] *Ibid.*
[54] L. LAUWAERT, *Wij, Robots*, Tielt, Lannoo Campus, 2021, 22.
[55] M. COECKELBERGH, *AI Ethics*, Cambridge, The MIT Press, 2020, 66.
[56] L. LAUWAERT, *Wij, Robots*, Tielt, Lannoo Campus, 2021, 22.
[57] *Ibid.*
[58] *Ibid.*
[59] K. GABRIELS, *Regels voor robots. Ethiek in tijden van AI*, Brussel, VUBPRESS, 2019, 82.

Hoofdstuk 3: Twee invalshoeken met betrekking tot het lerend vermogen

34. Binnen het onderzoeksveld van gerichte AI kunnen op vandaag twee grote manieren van "leren" onderscheiden worden, met name een kennis-gebaseerde benadering en een data-gebaseerde benadering.[60]

Afdeling 1: Kennis-gebaseerd lerend vermogen

35. In de eerste fase van AI, van 1950 tot eind jaren '80, domineerde de kennis-gebaseerde benadering van AI, ook wel *Symbolic AI* genaamd.[61] Symbolische AI steunt op de symbolische weergave van de realiteit in het domein van hogere cognitieve functies, zoals abstract redeneren en besluitvorming.[62] Binnen deze benadering creëren menselijke deskundigen nauwkeurige, op regels gebaseerde procedures – bekend als algoritmen – die een machine kan volgen om een vakkundige beslissing, inschatting of aanbeveling te maken op basis van de inkomende gegevens, en bijgevolg te fungeren als een expertsysteem.[63]

Deze algoritmen nemen de vorm aan van een 'als-dan-constructie'.[64] De gespecialiseerde kennis van deskundigen wordt m.a.w. door een programmeur in de vorm van een instructie vertaald in een computerprogramma die de machine in staat stelt om geldige deducties te maken uit de menselijke expertkennis die het bezit.[65] MYCIN was de naam van een van de eerste expertsystemen die in de jaren '70 ontwikkeld werd.[66] Dit expertsysteem ontving data van patiënten en schatte vervolgens de kans in dat de patiënt een bloedstollingsziekte of bacteriële infectie had.[67]

36. Alle intelligentie in het expertsysteem is rechtstreeks afkomstig van menselijke expertise die werd vastgelegd in een voor een computer leesbaar formaat. Expertsystemen zijn bijgevolg in hoge mate mensenwerk.[68] Gezien dit gegeven, heeft een expertsysteem het voordeel dat het transparant is en mensen makkelijk kunnen begrijpen hoe deze systemen specifieke beslissingen nemen.[69]

---

[60] T. GILS, E. WAUTERS, B. BENICHOU, J. DE BRUYNE en P. VALCKE, "Artificiële Intelligentie en gegevensbescherming: een verkennende gids", *Kenniscentrum Data en Maatschappij*, 2020, https://data-en-maatschappij.ai/publicaties/ai-en-gegevensbescherming-een-verkennende-gids.
[61] M. COECKELBERGH, *AI Ethics*, Cambridge, The MIT Press, 2020, 71.
[62] *Ibid.*
[63] SCIENTIFIC FORESIGHT UNIT (STOA), *Artificial intelligence: How does it work, why does it matter, and what can we do about it?, juni 2020*, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf.
[64] L. LAUWAERT, *Wij, Robots*, Tielt, Lannoo Campus, 2021, 23.
[65] *Ibid.*
[66] L. STEELS (ed.), *Artificiële intelligentie. Naar een vierde industriële revolutie?*, Brussel, KVAB Press, 2017, 15.
[67] L. LAUWAERT, *Wij, Robots*, Tielt, Lannoo Campus, 2021, 23.
[68] *Ibid.*
[69] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 17.

Wanneer het systeem een beslissing heeft genomen, kan men immers eenvoudig achterhalen waarop de beslissing is gebaseerd door terug te vallen op de input en het algoritme.[70] In dit opzicht kan bijgevolg zowel de eindbeslissing als de tussenstappen in het beslissingsproces verklaard worden, wat eveneens impliceert dat fouten in het systeem makkelijk kunnen worden opgespoord.[71]

37. Er zijn echter ook enkele nadelen verbonden aan deze op kennis-gebaseerde systemen.[72] In eerste instantie vergt het vastleggen en schrijven van de regels enorm veel tijd. Daarenboven is het moeilijk vooraf alle mogelijke regels neer te schrijven, anticiperend op elke mogelijke situatie waarin het systeem potentieel kan terechtkomen. Ten slotte ageren kennis-gebaseerde systemen zeer stabiel in een gekende context, maar ondernemen ze geen actie als de programmeur geen regel voor een bepaalde situatie vooraf definieerde.[73] Expertsystemen "leren" namelijk niet automatisch bij, waardoor ze regelmatig gevoed moeten worden met nieuwe (statistische) regels.[74] Dit is problematisch gezien onze wereld vaak complex en moeilijk voorspelbaar is.

Ondanks de beperkingen, blijft kennis-gebaseerde AI bijzonder nuttig bij de ondersteuning van mensen die werken aan repetitieve problemen in welomschreven domeinen, zoals onder meer machinebesturing en beslissingsondersteunende systemen.[75] Deze AI-technieken worden ook wel *Good Old-Fashioned Artificial Intelligence (GOFAI)* genoemd.[76]

Afdeling 2: Data-gebaseerd lerend vermogen

38. In de jaren '80 ontstond een paradigmaverschuiving van een kennis-gebaseerde benadering van AI *(symbolic AI)* naar een data-gebaseerde benadering van AI *(subsymbolic AI).*[77] Subsymbolisch betekent dat er niet langer regels zijn die in woorden zijn uit te drukken, maar dat het systeem van verschillende voorbeelden geleerd heeft wat de regels moeten zijn.[78] De kennis-gebaseerde benadering domineerde aanvankelijk het AI-onderzoek door de schaarste van data en het gebrek aan voldoende rekenkracht van computers en intern computergeheugen.

---

[70] L. LAUWAERT, *Wij, Robots*, Tielt, Lannoo Campus, 2021, 24.
[71] E. ILKOU en M. KOUTRAKI, "Symbolic Vs Sub-symbolic AI Methods: Friends or Enemies?", CEUR WS 2020, (1) 1.
[72] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 17.
[73] *Ibid.*
[74] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 19.
[75] SCIENTIFIC FORESIGHT UNIT (STOA), *Artificial intelligence: How does it work, why does it matter, and what can we do about it?, juni 2020*, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf.
[76] L. LAUWAERT, *Wij, Robots*, Tielt, Lannoo Campus, 2021, 23.
[77] SCIENTIFIC FORESIGHT UNIT (STOA), *Artificial intelligence: How does it work, why does it matter, and what can we do about it?, juni 2020*, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf.
[78] Van Zwol, T. (2017, 22 oktober). Kunstmatige intelligentie: omarmen of wantrouwen? Scientias. Geraadpleegd op 29 september 2022, van https://scientias.nl/kunstmatige-intelligentie-omarmen-wantrouwen/.

Door de exponentiële toename van rekenkracht, de beschikbaarheid van (big) data, het massale gebruik van sociale media, smartphones, snelle mobiele netwerken en het groeiende *Internet of Things* (*IoT*), wint de data-gebaseerde benadering elke dag aan belang.[79] *Het IoT* duidt de situatie aan waarin elektronisch gestuurde toestellen en gebruiksvoorwerpen, zoals auto's rechtstreeks met het internet verbonden zijn en zelf informatie uitwisselen over het internet, zowel met mensen als met andere toestellen.[80]

2.1. Machinaal leren

39. Machinaal leren *(machine learning)* kan beschouwd worden als de kern van de data-gebaseerde benadering.[81] De term machinaal leren werd in 1959 bedacht door Arthur Samuel die machinaal leren definieerde als *"a field of study that gives computers the ability to learn without being explicitly programmed"*.[82] Hoewel deze definitie eerder vaag is, duidt het een zeer belangrijk kenmerk van machinaal leren aan, namelijk het incrementele proces van zelfleren dat ontstaat door de automatische detectie van patronen tussen input en output en de blootstelling aan data.[83]

Dit betekent dat machinaal leren bottom-up in grote hoeveelheden data patronen zal proberen te herkennen om een specifiek probleem op te kunnen lossen.[84] Dit impliceert dat – in tegenstelling tot een expertsysteem – het AI-systeem zelf zal leren om aan binnenkomende informatie (input) een beslissing te koppelen (output), zonder dat er regels of programmering aan te pas komt.[85] Het betreft bijgevolg een AI-systeem dat functioneert op basis van een zelflerend algoritme.[86]

40. De wijze waarop *machine-learning* algoritmes "leren" is zeer gelijklopend met de manier waarop mensen leren. Afhankelijk van de wijze waarop het leren plaatsvindt, kunnen drie categorieën onderscheiden worden: gesuperviseerd leren *(supervised learning),* ongesuperviseerd leren *(unsupervised learning)* en versterkend leren *(reinforcement learning).*[87]

---

[79] B. BENICHOU, J. KINDT en M. BEUDELS, "Informatieverplichtingen in het gegevensbeschermingsrecht: *much ado about nothing?*" in S. VAN AGGELEN (ed.), *Informatie en recht*, Mortsel, Intersentia, 2021, (197) 197; M. COECKELBERGH, *AI Ethics*, Cambridge, The MIT Press, 2020, 3.
[80] B. BENICHOU, J. KINDT en M. BEUDELS, "Informatieverplichtingen in het gegevensbeschermingsrecht: *much ado about nothing?*" in S. VAN AGGELEN (ed.), *Informatie en recht*, Mortsel, Intersentia, 2021, (197) 197.
[81] R. DEVILLE, N. SERGEYSSELS en C. MIDDAG, "Basic Concepts of AI for Legal Scholars" in DE BRUYNE, J. en VANLEENHOVE, C. (eds.), *Artificial Intelligence and the Law*, Mortsel, Intersentia, 2021, 1.
[82] W. WANG en K. SIAU, "Artificial Intelligence, Machine Learning, Automation, Robotics, Future of of Work and Future of Humanity: A Review and Research Agenda", *Journal of Database Management* 2019, (61) 63.
[83] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 20-21.
[84] *Ibid*., (17) 22.
[85] L. LAUWAERT, *Wij, Robots*, Tielt, Lannoo Campus, 2021, 24.
[86] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 33.
[87] P. KIM, *MATLAB Deep Learning*, Seoul, Apress, 2017, 12.

2.1.1. Gesuperviseerd leren

41. Bij gesuperviseerd leren of gecontroleerd leren krijgt het systeem via de 'supervisor' voorbeelden aangereikt, waarbij duidelijk aangegeven is wat de gewenste output is bij een gegeven input *(labeled data).*[88] In het kader van gesuperviseerd leren is het labelen van inputdata een noodzakelijke voorwaarde in het leerproces van een gesuperviseerd zelflerend algoritme. *Data labeling* is het proces van het identificeren van ruwe data en het toevoegen van één of meerdere zinvolle en informatieve labels om meer context en uitleg te bieden aan het zelflerend algoritme.[89] Indien we bijvoorbeeld een algoritme wensen te trainen op het herkennen van katten en honden, dan bieden we het algoritme gelabelde foto's aan, gelabeld "dit is een kat", "dit is een hond" of "dit is iets anders dan een kat of een hond".[90]

42. Het systeem zoekt vervolgens het verband of patroon tussen de aangeleverde input- en outputdata, waarna het algoritme probeert op basis van de inputdata een gekende set van outputdata te voorspellen en kennis te vergaren.[91] Het algoritme heeft een enorme hoeveelheid data (voorbeelden) nodig om de aangeleerde kennis te kunnen verbeteren *(model training)* en dus effectief en nauwkeurig te zijn.[92]

Eenmaal het algoritme voldoende voorbeelden heeft geanalyseerd, creëert het een model, waarna het algoritme in staat is om in zeer korte tijd patronen te identificeren in een grote set van nieuwe data.[93] Over het algemeen zijn gesuperviseerd lerende algoritmes voornamelijk geschikt om data te categoriseren, te voorspellen, te detecteren en aan te bevelen.[94] De meeste bekende AI-toepassingen gebaseerd op een gesuperviseerd lerend algoritme, zijn op heden de zoekfunctie op foto's bij Google Search en Microsoft Bing.[95]

---

[88] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 38.
[89] AWS. What is data labeling for machine learning? *AWS*. Geraadpleegd op 3 oktober 2022, van https://aws.amazon.com/sagemaker/data-labeling/what-is-data-labeling/#:~:text=In%20machine%20learning%2C%20data%20labeling,model%20can%20learn%20from%20it.
[90] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 24.
[91] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 43.
[92] *Ibid.*
[93] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 24.
[94] *Ibid.*
[95] *Ibid.*

2.1.2. Ongesuperviseerd leren

43. Bij ongesuperviseerd leren, dient het systeem zelf structuur aan te brengen in de data, zonder te weten wat die voorstellen *(unlabeled data).*[96] Op basis van gelijksoortige kenmerken in de inputdata, zal het ongesuperviseerd lerend algoritme intern een model creëren waardoor automatisch verschillende clusters of verzamelingen zullen ontstaan.[97] Ongesuperviseerd leren is vooral geschikt om clusteringproblemen op te lossen.[98] De meest bekende AI-toepassingen gebaseerd op een ongesuperviseerd lerend algoritme zijn op dit moment de aanbevelingsfuncties bij Netflix en Amazon waarbij het AI-systeem de klanten in clusters opdeelt op basis van hun kijkgedrag, respectievelijk koopgedrag en op basis daarvan films of producten aanbeveelt.[99]

2.1.3. Versterkend leren

44. Versterkend leren tracht een predictief model te construeren op basis van de terugkoppeling (*feedback*) die het systeem geeft wanneer het willekeurig parameters aanpast volgens de "vallen en opstaan"-methode.[100] In tegenstelling tot het (on)gesuperviseerd leren, krijgt het systeem dus geen voorbeelden aangereikt in het leerproces, maar leert het wat het moet doen door de huidig bekomen uitkomst steeds af te toetsen aan meetbare criteria en bijgevolg positieve of negatieve feedback terug te koppelen naar het model.[101]

Wanneer een willekeurige aanpassing een positief effect genereert, krijgt het systeem een beloning. Wanneer daarentegen blijkt dat een willekeurige aanpassing een nadelig effect genereert, wordt het systeem bestraft.[102] Uiteindelijk zal het systeem beslissingen nemen om de beloning te maximaliseren en de straf te minimaliseren door middel van dynamische programmering.[103] De bekendste toepassingen van versterkend leren zijn terug te vinden in de gaming-wereld (bijvoorbeeld Alpha Go) en de simulatie-wereld (bijvoorbeeld zelfrijdende wagens).[104]

---

[96] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 39.
[97] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 25.
[98] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 38.
[99] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 25.
[100] *Ibid.,* (17) 27.
[101] *Ibid.*
[102] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 40.
[103] *Ibid.*
[104] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 27.

2.2. Deep learning

45. *Deep learning* is een subcategorie van *machine learning*.[105] Dit betekent dat *deep learning* een specifieke vorm is van machinaal leren.[106] Concreet maakt *deep learning* gebruik van verschillende artificiële neurale netwerken (ANN), die patronen en complexe verbanden zoeken op diepliggende en hiërarchische niveaus in datasets.[107] ANN is een techniek die geïnspireerd is op de complexe structuur van ons brein dat bestaat uit neurale netwerken van lagen neuronen.[108] Neuronen zijn bijzondere cellen die elektrische inputsignalen van naburige neuronen ontvangen en produceren – afhankelijk van de input – een output die vervolgens wordt doorgegeven aan andere neuronen.[109]

46. Een artificieel neuraal netwerk bestaat uit minimaal drie lagen neuronen.[110] De eerste laag neuronen die de originele input ontvangt, wordt de invoerlaag *(input layer)* genoemd.[111] De tussenlaag *(hidden layer)* bestaat uit één of meerdere lagen neuronen. Wanneer er meerdere lagen neuronen zijn, spreekt men van een 'diep' neuraal netwerk. De laatste laag neuronen, wordt de uitvoerlaag *(output layer)* genoemd.[112]

Elk neuron van laag X is verbonden met elk neuron van laag X+1. Elke verbinding tussen neuronen heeft een gewicht, namelijk een getal van 0 tot 1 dat het signaal ertussen regelt.[113]Dat gewicht is bepalend voor de kracht waarmee het signaal via die verbinding aankomt bij het doelneuron en kan negatief (remmend) of positief (stimulerend) zijn.[114] Het gewicht geeft met andere woorden aan hoe belangrijk die verbinding is om tot een juiste oplossing te komen. In een eerste fase krijgen alle verbindingen een willekeurig gewicht. Deze gewichten worden tijdens het trainingsproces aangepast om de performantie van het netwerk te optimaliseren.[115]

---

[105] J. HAZENBERG, *Technologie de baas*, Amsterdam, Spectrum, 2019, 39.
[106] L. LAUWAERT, *Wij, Robots*, Tielt, Lannoo Campus, 2021, 25.
[107] K. GABRIELS, *Regels voor robots. Ethiek in tijden van AI*, Brussel, VUBPRESS, 2019, 28.
[108] R. DEVILLE, N. SERGEYSSELS en C. MIDDAG, "Basic Concepts of AI for Legal Scholars" in DE BRUYNE, J. en VANLEENHOVE, C. (eds.), *Artificial Intelligence and the Law*, Mortsel, Intersentia, 2021, 7.
[109] K. GABRIELS, *Regels voor robots. Ethiek in tijden van AI*, Brussel, VUBPRESS, 2019, 28.
[109] R. DEVILLE, N. SERGEYSSELS en C. MIDDAG, "Basic Concepts of AI for Legal Scholars" in DE BRUYNE, J. en VANLEENHOVE, C. (eds.), *Artificial Intelligence and the Law*, Mortsel, Intersentia, 2021, 7.
[110] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 27.
[111] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 35.
[112] *Ibid.*
[113] *Ibid.*
[114] *Ibid.*
[115] W. VAN BIESEN, N. VEYS, J. DECRUYENAERE, R. PELEMAN en S. STERCKX, "Hoe artificiële intelligentie, digitalisering en big data ons kunnen helpen bij verantwoordbare zorg", *tvgg* 2021, (1) 4.

47. Het ongetraind neuraal netwerk wordt verschillende voorbeelden gegeven, waarna het netwerk elk voorbeeld bekijkt en alle lineaire combinaties in het neuraal netwerk verfijnt tot het erin slaagt de voorbeelden zo goed mogelijk te simuleren en zeer complexe relaties tussen de invoerlaag en uitvoerlaag te ontdekken.[116]

48. De tussenliggende lagen zijn verborgen lagen die niet waarneembaar zijn en die niet door de gebruiker achterhaald kunnen worden (*black box*).[117] Dit betekent dat de gebruiker niet kan kiezen welke stappen worden genomen, en bovendien niet weet wat er precies in die lagen gebeurt.[118] Alleen de input, de output en het aantal neuronen in de verborgen lagen worden door de gebruiker bepaald.[119]

49. De meest bekende toepassingen van diepe neurale netwerken zijn onder meer gezichtsherkenning, gezichtsdetectie, objectherkenning en objectdetectie.[120] Zo is het *DeepFace*-algoritme van Facebook getraind op vier miljoen afbeeldingen die door Facebook-gebruikers werden geüpload en wordt het ingezet om automatisch mensen te *taggen* in Facebook-foto's.[121]

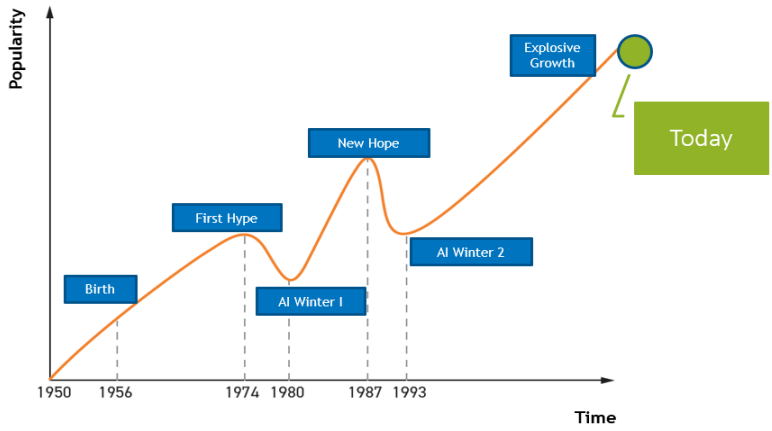
Hoofdstuk 4: *Black Box*

50. AI-technologieën worden steeds prominenter gepositioneerd in onze samenleving, aangezien ze het potentieel bezitten om een brede waaier van maatschappelijke voordelen en economische groei te genereren. AI-technologie kent immers verscheidene toepassingen en wordt op verschillende domeinen ingezet, zoals onder meer industriële productie, landbouw, vervoer, gezondheidszorg, financiën en verzekeringen, veiligheid (militair en rechtshandhaving), sales en marketing, media, amusement, wetenschap en onderwijs.[122] AI heeft op vandaag een punt van maturiteit bereikt en zit structureel verankerd in de werking van onze maatschappij waardoor het niet langer als een randfenomeen kan worden beschouwd.

---

[116] R. DEVILLE, N. SERGEYSSELS en C. MIDDAG, "Basic Concepts of AI for Legal Scholars" in DE BRUYNE, J. en VANLEENHOVE, C. (eds.), *Artificial Intelligence and the Law*, Mortsel, Intersentia, 2021, 7.
[117] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 35.
[118] R. DEVILLE, N. SERGEYSSELS en C. MIDDAG, "Basic Concepts of AI for Legal Scholars" in DE BRUYNE, J. en VANLEENHOVE, C. (eds.), *Artificial Intelligence and the Law*, Mortsel, Intersentia, 2021, 7.
[119] *Ibid.*
[120] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 29.
[121] *Ibid.*
[122] M. COECKELBERGH, *AI Ethics*, Cambridge, The MIT Press, 2020, 74.

Figuur 1 illustreert de exponentiële groei van AI in de tijd. Deze figuur toont duidelijk aan dat sinds 1993 een explosieve groei van AI-technologieën zich aftekent.



Figuur1[123]: Exponentiële groei van AI in de tijd

51. De ontwikkeling en het gebruik van AI met haar specifieke kenmerken brengt echter ook een breed scala aan ethische en wettelijke uitdagingen met zich mee. In het bijzonder creëren de ondoorzichtigheid/ondoorgrondelijkheid (*black box*), de complexiteit, de afhankelijkheid van data en het zelflerend karakter van AI ethische en juridische uitdagingen en problemen inzake transparantie en uitlegbaarheid van AI-systemen.

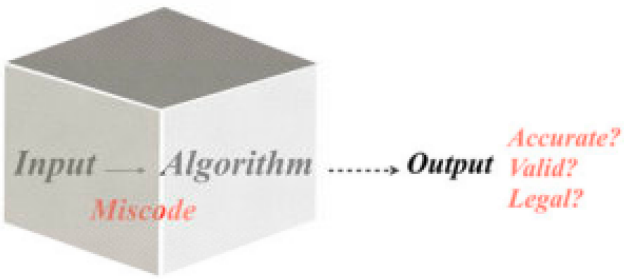
52. Transparantie bij de toepassing van een AI-systeem is in grote mate afhankelijk van het soort algoritme dat geïmplementeerd wordt.[124] In dit opzicht, kan aldus geconcludeerd worden dat niet elke vorm van AI even zorgelijk is vanuit transparantieoverwegingen. Wanneer onomkeerbaar bewezen kan worden waarom een algoritme een bepaalde beslissing heeft genomen, is er sprake van een transparant algoritme, een *white box*.[125] Dit is met name het geval bij expertsystemen.[126]

AI-systemen die daarentegen gebruik maken van *machine-learning* en in het bijzonder van diepe neurale netwerken, laten niet toe te achterhalen waarom het algoritme een welbepaalde beslissing heeft genomen, aangezien men niet kan nagaan wat in de verborgen lagen van het netwerk gebeurt.[127] In dit geval is er sprake van een zwarte doos, ook wel een *black box* genaamd waarbij de interne operaties van het systeem niet transparant zijn waardoor het inzicht in de werking ervan wordt beperkt.

[123] G.M. DE KETELAERE, *Mens versus machine*, Kalmthout, Pelckmans, 2020, 202.
[124] E. MANNENS, "Wat je moet weten over AI" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (17) 37.
[125] *Ibid.*
[126] *Ibid.*
[127] *Ibid.*

Een *black box* is, algemeen geformuleerd, een ondoorzichtig systeem waarbij de notie ondoorzichtigheid niet alleen verwijst naar belemmeringen tussen toegang en informatie, maar ook de kwestie betreft van de begrijpelijkheid van dergelijke informatie.[128]

Figuur 2 illustreert het potentiële *black box*-karakter van AI-systemen en de daaraan verbonden risico's.[129] Zonder inzicht in de wijze waarop de output tot stand is gekomen, is het niet mogelijk de nauwkeurigheid, de geldigheid en wettigheid ervan te toetsen.[130]



Figuur 2[131]: *Black box*

53. Het *black box*-gegeven en de exponentiële groei van AI versterkt de roep naar (meer) transparantie. Er worden immers enorme hoeveelheden data verwerkt door AI-systemen op steeds complexere en (soms) minder transparante manieren. Deze evolutie noopt bijgevolg tot het goed beheer van data die nodig is voor de werking van AI en het – vanuit de wetgeving – garanderen van meer transparantie bij de verwerking van deze data door AI-systemen. Dit is immers een noodzakelijke voorwaarde opdat deze maatschappelijke ontwikkeling doordacht kan plaatsvinden.

[128] F. PALMIOTTO, "The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings" in M. EBERS en M. CANTERO GAMITO (eds.), *Algorithmic Governance and Governance of Algorithms,* Zwitserland, Springer, 2021, (49) 56.
[129] *Ibid.*
[130] *Ibid.*
[131] *Ibid.*

DEEL II. JURIDISCH KADER

54. In deel II wordt het juridisch kader, bestaande uit de AVG en het Voorstel, geschetst. In dit juridisch kader worden transparantieverplichtingen geponeerd. In deze masterproef wordt geanalyseerd of deze transparantieverplichtingen in staat zijn betekenisvolle transparantie te bieden ten aanzien van de aan het AI-systeem onderworpen personen wiens gegevens worden verwerkt. In het bijzonder maken AI-systemen die een *black box* zijn, het verdere voorwerp uit van dit onderzoek.

55. Om een degelijke analyse mogelijk te maken, alsook een kritische houding te kunnen aannemen tijdens het analyseren, is het noodzakelijk om het ruimere kader waarbinnen beide Europese rechtsinstrumenten zich situeren, te duiden. In het bijzonder wordt aandacht besteed aan de ontstaansgeschiedenis, het toepassingsgebied, de relevante actoren, de rol van transparantie in beide rechtsinstrumenten en de verhouding tussen beide.

Hoofdstuk 1: Algemene Verordening Gegevensbescherming

Afdeling 1: Inleiding

56. Op 25 mei 2018 trad de AVG in werking. Deze verordening verving de richtlijn gegevensbescherming die sinds 1995 beschouwd werd als het belangrijkste wettelijke instrument van de Europese Unie ('EU') op het gebied van gegevensbescherming.[132] De richtlijn bood een antwoord op de noodzaak tot uniformisering van de verschillende nationale wetgevingen inzake gegevensbescherming met als doel een hoog beschermingsniveau en het vrij verkeer van persoonsgegevens tussen de verschillende lidstaten te waarborgen.[133]

57. Met de richtlijn werd complete harmonisatie beoogd, maar werd in de praktijk in de lidstaten verschillend omgezet waardoor binnen de EU uiteenlopende gegevensbeschermingswetgevingen van kracht waren.[134] Daarnaast vonden belangrijke technologische ontwikkelingen plaats, waardoor nieuwe economische en maatschappelijke uitdagingen in een digitaal tijdperk ontstonden.[135]

---

[132] Richtl. EP. Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31.

[133] Preambule 10 Verord.Raad nr. (EU) 2016/679, 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb.L.* 4 mei 2016, afl. 119, 7.

[134] C. GIAKOUMOPOULOS, G. BUTTARELLI en M. O'FLAHERTY, *Handboek Europese gegevensbeschermingswetgeving*, Luxemburg, Bureau voor publicaties van de Europese Unie, 2021, 35.

[135] *Ibid.*

Deze vaststellingen maakten een hervorming en modernisering van het bestaand wettelijk kader noodzakelijk.[136] Door de overschakeling van een richtlijn naar een verordening heeft de Europese wetgever het recht op bescherming van persoonsgegevens, zoals verankerd in artikel 8 van het Handvest van de grondrechten van de EU, rechtstreeks en op uniforme wijze in de lidstaten toepasbaar willen maken.[137]

Afdeling 2: Toepassingsgebied van de AVG in de context van AI

2.1. Materieel toepassingsgebied

58. Om te kunnen bepalen of de verwerking van gegevens door AI-systemen onder het toepassingsgebied van de AVG ressorteert, dient vooreerst het materieel toepassingsgebied van de AVG nader te worden bekeken. Overeenkomstig artikel 2 AVG is de AVG van toepassing op de verwerking van persoonsgegevens die geheel of gedeeltelijk geautomatiseerd verloopt, evenals op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Uit het tweede deel van de zinsnede van artikel 2, lid 1 AVG blijkt dat gegevensbescherming geboden door het Unierecht geenszins beperkt is tot geautomatiseerde gegevensverwerking, waardoor de bescherming van de AVG zich eveneens uitstrekt tot de manuele verwerking van persoonsgegevens in een bestand.[138]

59. In dit kader is de vaststelling dat een verwerking al dan niet geautomatiseerd verloopt weinig relevant, aangezien de beschermingsregeling in beginsel op beide soorten verwerkingen van toepassing is.[139] De verwerking van persoonsgegevens door AI-systemen wordt niet expliciet gereguleerd in de AVG, omdat de AVG een technologisch neutraal wettelijk kader wil bieden.[140] Het speelt geen rol of persoonsgegevens geautomatiseerd, dan wel handmatig worden verwerkt. De AVG is bijgevolg gericht op het waarborgen van de bescherming van persoonsgegevens, ongeacht de middelen die voor de verwerking worden gebruikt (een eenvoudig computerprogramma, een complex AI-systeem of gewoon een mens).[141]

---

[136] *Ibid.*
[137] GEGEVENSBESCHERMINGSAUTORITEIT (GBA), *Aanbeveling betreffende de verwerking van persoonsgegevens voor direct marketingdoeleinden*, 17 januari 2020, nr. 01/2020, https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2020.pdf.
[138] C. GIAKOUMOPOULOS, G. BUTTARELLI en M. O'FLAHERTY, *Handboek Europese gegevensbeschermingswetgeving*, Luxemburg, Bureau voor publicaties van de Europese Unie, 2021, 120.
[139] D. DE BOT (ed.), *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Mechelen, Wolters Kluwer, 2020, 220.
[140] Overw. 15 AVG
[141] N. SMUHA, "From a 'Race to AI' to a 'Race to AI regulation': Regulatory Competition for Artificial Intelligence", *Law, Innovation & Technology* 2021, (1) 8.

De verwerking door AI-systemen betreft een geautomatiseerde verwerking, en valt bijgevolg onder het materieel toepassingsgebied van de AVG op voorwaarde dat zij persoonsgegevens verwerken.[142]

60. De notie 'persoonsgegevens' wordt in artikel 4, 1) AVG gedefinieerd als "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene')". Als identificeerbaar wordt beschouwd "een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatiemiddel, zoals een naam, een identificatienummer, locatiegegevens, een online identificatiemiddel of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die persoon".[143]

61. De betrokkene is de natuurlijke persoon wiens persoonsgegevens worden verwerkt.[144] Hiertegenover staat de verwerkingsverantwoordelijke. Dit is de actor die – conform de AVG – ten aanzien van de betrokkene de naleving van de AVG dient te verzekeren bij de verwerking van zijn/haar persoonsgegevens. Een verwerkingsverantwoordelijke wordt in de AVG gedefinieerd als "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt".[145]

2.2. Territoriaal toepassingsgebied

62. De verwerking van persoonsgegevens door AI-systemen ressorteert onder de AVG indien zij plaatsvindt in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Europese Unie, ongeacht of de verwerking al dan niet in de Unie plaatsvindt.[146] Indien de verwerking echter wordt verricht door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, ressorteert zij eveneens onder het toepassingsgebied indien de verwerking gericht is op burgers van de EU door hen producten of diensten aan te bieden of hun gedrag te volgen/observeren.[147]

---

[142] L. MITROU, *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection (GDPR) 'Artificial Intelligence-Proof'? ,*Athene, University of Economics and Business, 2018, 74.
[143] Art. 4, (1) AVG.
[144] Art. 4, (1) AVG.
[145] Art. 4, (7) AVG.
[146] Art. 3, lid 1 AVG.
[147] Art. 3, lid 2 AVG.

Afdeling 3: Transparantie als grondbeginsel

63. Artikel 5 AVG stipuleert een aantal belangrijke beginselen die moeten worden nageleefd bij de verwerking van persoonsgegevens. Zo bepaalt artikel 5, lid 1, a) AVG dat persoonsgegevens dienen te worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Dit beginsel wordt omschreven als het beginsel van "rechtmatigheid, behoorlijkheid en transparantie". In tegenstelling tot richtlijn 95/46/EG waarin transparantie alleen genoemd werd in overweging 38 als onderdeel van de vereiste om gegevens op een behoorlijke wijze te verwerken, wordt transparantie in de AVG toegevoegd als een fundamenteel grondbeginsel.[148]

64. Transparantie wordt niet expliciet gedefinieerd in de AVG, maar de kern van transparantie wordt in de overwegingen 39 en 58 van de AVG gespecificeerd waarin beknoptheid, toegankelijkheid en begrijpelijkheid van informatie over de verwerking van persoonsgegevens centraal staan. Gezien de afwezigheid van een eenduidige definitie, werd in deel III een eigen conceptualisering en definiëring van transparantie ontwikkeld.

Hoofdstuk 2: Het Voorstel voor een Verordening betreffende Artificiële Intelligentie

Afdeling 1: Inleiding

65. Sinds een aantal jaren hebben de Europese instellingen belangstelling getoond voor het versterken van de regelgeving inzake artificiële intelligentie om tegemoet te komen aan de vraag naar een meer transparant, robuust en coherent wettelijk kader voor het reguleren van de ontwikkeling en het gebruik van AI, omdat de reeds bestaande regelgeving, zoals de AVG, inadequaat wordt geacht om de specifieke risico's in verband met AI op te vangen.[149]

Om te vermijden dat het potentieel *black box*-karakter van AI-systemen een gebrek aan transparantie veroorzaakt, achtte de Raad van de Europese Unie het noodzakelijk de unieke eigenschappen van AI-systemen aan te pakken opdat deze geautomatiseerde systemen verenigbaar zouden zijn met de grondrechten, meer bepaald het recht op gegevensbescherming.[150]

---

[148] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679*, 11 april 2018, WP260rev.01, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf, 5.

[149] G. LAZCOZ en P. DE HERT, "Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities", *Brussels Privacy Hub* 2022, (1) 8.

[150] Conclusie van het voorzitterschap nr. 11481/20, 21 oktober 2020 over het Handvest van de Grondrechten in e context van artificiële intelligentie en digitale verandering, https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vli6mrzmjby8.

Om hieraan tegemoet te komen, publiceerde de Europese Commissie op 21 april 2021 een Voorstel dat geharmoniseerde regels bevat voor het in de handel brengen, in gebruik stellen en gebruiken van AI-systemen binnen de Europese Unie, zodoende rechtszekerheid te garanderen om investeringen en innovatie in AI te bevorderen, het beheer en de doeltreffende handhaving van de bestaande wetgeving inzake grondrechten en veiligheid te versterken en de ontwikkeling van een eengemaakte markt voor wettige, veilige en betrouwbare AI-systemen te vergemakkelijken.[151]

Afdeling 2: Toepassingsgebied van het het Voorstel

66. Met dit rechtskader wordt beoogd een rechtskader voor betrouwbare en transparante AI te creëren dat de potentiële risico's van AI opvangt, zonder innovatie af te remmen en zonder ondernemingen te veel te belasten.[152] Om deze doelstellingen te bereiken, gaat het Voorstel uit van een risicogebaseerde benadering op grond waarvan de toepasselijke geharmoniseerde regels worden bepaald in functie van de intensiteit en de omvang van de risico's die gepaard gaan met het AI-systeem.[153]

67. Het Voorstel streeft naar een evenwichtige aanpak die beperkt blijft tot de noodzakelijke minimumvereisten om de risico's en problemen in verband met AI aan te pakken, zonder de technologische ontwikkeling van AI onnodig te beperken of te belemmeren.[154] Op grond van deze benadering worden vier soorten AI-systemen onderscheiden in het Voorstel. Het betreffen AI-systemen die 1) een onaanvaardbaar risico, 2) een hoog risico, 3) een beperkt risico en 4) een laag of minimaal risico met zich meebrengen.[155]

---

[151] Voorstel (Comm.) voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie, 21 april 2021, COM'2021) def – 2021/0106 (COD); Titel 1.1. Memorie van Toelichting Voorstel voor een Verordening betreffende Artificiële Intelligentie.

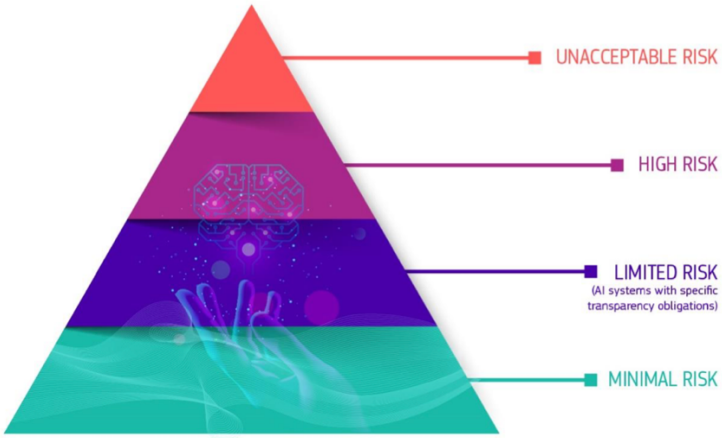
[152] M. FIERENS, E. VAN GOOL en J. DE BRUYNE, "De regulering van artificiële intelligentie (deel 1)- Een algemene stand van zaken en een analyse van enkele vraagstukken inzake consumentenbescherming", *RW* 2021, (962) 967.

[153] Overw. 14 Voorstel voor een Verordening betreffende Artificiële Intelligentie; Titel 1.1. Memorie van Toelichting Voorstel voor een Verordening betreffende Artificiële Intelligentie.

[154] Titel 1.1. Memorie van Toelichting Voorstel voor een Verordening betreffende Artificiële Intelligentie.

[155] Titel 5.2. Memorie van Toelichting Voorstel voor een Verordening betreffende Artificiële Intelligentie.

Figuur 3 visualiseert de risicogebaseerde benadering als een piramidale structuur.[156]



Figuur 3[157]: De risicogebaseerde benadering in een piramidale structuur

2.1. Materieel toepassingsgebied

68. Transparantie van AI-systemen wordt in het Voorstel als een essentieel beginsel beschouwd om de eerbiediging van de grondrechten van de betrokken personen te waarborgen.[158] Net zoals in de AVG ontbreekt een eenduidige definitie in het Voorstel van de notie 'transparantie'. In deze masterproef worden alleen de door het oorspronkelijke voorstel geponeerde transparantieverplichtingen voor AI-systemen met een hoog risico en beperkt risico geanalyseerd, aangezien alleen deze twee categorieën AI-systemen het voorwerp uitmaken van transparantieverplichtingen in het Voorstel.[159]

Immers, AI-systemen die volgens het Voorstel een onaanvaardbaar risico creëren voor de waarden en grondrechten van de Unie, waaronder het recht op gegevensbescherming en privacy, worden verboden.[160] Het Voorstel omvat hieromtrent een uitputtende lijst van verboden praktijken op het gebied van AI.[161]

---

[156] Europese Commissie, *Regulatory framework proposal on artificial intelligence*, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (consultatie 6 maart 2023).
[157] *Ibid.*
[158] Arts. 1 c), 13 en 52 Voorstel voor een Verordening betreffende Artificiële Intelligentie; Overw. 14, 38, 39, 43, 47, 69, 70 Voorstel voor een Verordening betreffende Artificiële Intelligentie; V. RAPOSO, "Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence", *International Journal of Law and Information Technology* 2022, (88) 103.
[159] Overw. 47 en 70 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[160] Overw. 15 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[161] Art. 5 Voorstel voor een Verordening betreffende Artificiële Intelligentie.

Met betrekking tot AI-systemen met een minimaal risico beoogt het Voorstel aanbieders van dergelijke AI-systemen ertoe aan te zetten de dwingende voorschriften voor AI-systemen met een hoog risico vrijwillig toe te passen door de ontwikkeling van *soft law* instrumenten, zoals gedragscodes.[162] De regulering van AI-systemen met een laag risico wordt bijgevolg overgelaten aan zelfregulering.

2.1.1. AI-systemen met een hoog risico

69. Titel III van het Voorstel bevat het toepasselijke regime voor AI-systemen die een hoog risico inhouden voor de gezondheid, veiligheid of grondrechten van natuurlijke personen in een aantal welomschreven toepassingen, producten en sectoren.[163] In het bijzonder vindt titel III van het Voorstel toepassing op twee subcategorieën van AI-systemen. Vooreerst geldt de regeling voor AI-systemen die producten of veiligheidscomponenten zijn van producten die reeds onder de in bijlage II opgenomen harmonisatiewetgeving van de Unie ressorteren die vooraf een conformiteitsbeoordeling door derden moeten ondergaan.[164]

Ten tweede worden in bijlage III ook andere autonome AI-systemen gespecificeerd als AI-systemen met een hoog risico.[165] Het gaat om AI-systemen die ingezet worden op de volgende gebieden, namelijk biometrische identificatie en categorisering van natuurlijke personen, beheer en exploitatie van kritieke infrastructuur, onderwijs en beroepsopleiding, werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid, toegang en gebruik van essentiële particuliere diensten en openbare diensten, uitkeringen, rechtshandhaving, migratie, asiel en beheer rechtscontroles, rechtsbedeling en democratische processen.[166]

70. Het merendeel van de verplichtingen die het Voorstel poneert met betrekking tot AI-systemen met een hoog risico, rusten op de aanbieders van dergelijke AI-systemen.[167] Een aanbieder wordt in het Voorstel omschreven als "een natuurlijke persoon of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem ontwikkelt of beschikt over een AI-systeem dat is ontwikkeld met het oog op het in de handel brengen of in gebruik stellen".[168]

---

[162] Art. 69 Voorstel voor een Verordening betreffende Artificiële Intelligentie; I. VAROSANEC, "On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI", *International Review of Law, Computers & Technology* 2022, (95) 104.
[163] M. VEALE en F. ZUIDERVEEN BORGESIUS, "Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach", *Computer Law Review International* 2021, (97) 102.
[164] Art. 6, lid 1 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[165] Art. 6, lid 2 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[166] Bijlage III Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[167] Art. 16 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[168] Art. 3, (2) Voorstel voor een Verordening betreffende Artificiële Intelligentie.

In een aantal gevallen rusten ook verplichtingen op de gebruikers van AI-systemen. Een gebruiker wordt omschreven als "een natuurlijke persoon of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem onder eigen verantwoordelijkheid gebruikt".[169]

2.1.2. AI-systemen met een beperkt risico

71. Titel IV, artikel 52 van het Voorstel bevat drie specifieke transparantieverplichtingen voor AI-systemen met een beperkt risico.[170] De door het Voorstel geponeerde specifieke transparantieverplichtingen vinden met name toepassing op AI-systemen die bedoeld zijn om met natuurlijke personen te interageren, zoals chatbots, emotieherkenningssystemen of biometrische indelingssystemen en AI-systemen die beeld-, audio-, of videomateriaal genereren, zoals *deep fakes*.[171]

72. Een chatbot wordt niet in het Voorstel gedefinieerd, maar kan worden omschreven als een geautomatiseerd digitaal systeem dat gebruik maakt van AI en *Natural language processing* ('NLP') waarmee natuurlijke personen via natuurlijke taal kunnen communiceren, bijvoorbeeld in het kader van klantenservice ter verbetering van de dienstverlening.[172] Emotieherkenningssystemen worden wel in het Voorstel gedefinieerd. Het betreffen AI-systemen die ontworpen zijn om emoties of intenties van natuurlijke personen vast te stellen of af te leiden op basis van hun biometrische gegevens.[173]

Biometrische indelingssystemen daarentegen, worden gedefinieerd als AI-systemen die ontwikkeld zijn om natuurlijke personen in specifieke categorieën in te delen, zoals geslacht, leeftijd, haarkleur, oogkleur, tatoeages, etnische afkomst, seksuele geaardheid of politieke overtuiging, op basis van hun biometrische gegevens.[174]

73. Het Voorstel definieert de notie 'biometrische gegevens' als persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd.[175]

---

[169] Art. 3, (4) Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[170] Overw. 70 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[171] Art. 52 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[172] N. AHMAD, M. HAMID, A. ZAINAL, M. RAUF en Z. ADNAN, "Review of Chatbots Design Techniques", *International Journal of Computer Applications* 2018, (7) 7.
[173] Art. 3, 34 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[174] Art. 3, 35 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[175] Art. 3, 33 Voorstel voor een Verordening betreffende Artificiële Intelligentie.

2.2. Territoriaal toepassingsgebied

74. Het Voorstel is van toepassing op aanbieders die AI-systemen in de EU in de handel brengen of in gebruik stellen, ongeacht of deze aanbieders in de EU of in een derde land gevestigd zijn, alsook op gebruikers van AI-systemen die zich in de Unie bevinden.[176] Ten slotte ressorteren ook aanbieders en gebruikers van AI-systemen die zich in een derde land bevinden wanneer de output van het systeem in de Unie wordt gebruikt onder het toepassingsgebied van het Voorstel teneinde natuurlijke personen die zich in de EU bevinden doeltreffend te beschermen.[177]

Hieruit blijkt duidelijk dat een AI-systeem pas onder het toepassingsgebied van het Voorstel valt vanaf het moment dat ze op de markt wordt gebracht. Het Voorstel is bijgevolg niet van toepassing in de ontwikkelingsfase van het AI-systeem.

Hoofdstuk 3: De verhouding tussen de AVG en het Voorstel

75. In de Memorie van Toelichting bij het Voorstel wordt de verhouding tussen de AVG en het Voorstel verduidelijkt. Hieruit blijkt dat het Voorstel geen afbreuk doet aan de AVG en een aanvulling op dit kader vormt.[178] Het EDPB en de EDPS raden in hun Gezamenlijk Advies ten zeerste aan ook in de bindende tekst van het Voorstel te verduidelijken dat de AVG van toepassing is op elke verwerking van persoonsgegevens die binnen het toepassingsgebied van het Voorstel valt.[179]

In dit kader is het belangrijk op te merken dat de AVG maar toepassing zal vinden wanneer persoonsgegevens worden verwerkt. Wanneer AI-systemen bijgevolg gegevens zouden verwerken die geen persoonsgegevens zijn, dan zal de bescherming van de AVG ten aanzien van de aan het AI-systeem onderworpen personen geen toepassing vinden.

---

[176] Art. 2, (a) en (b) Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[177] Art. 2, (c) Voorstel voor een Verordening betreffende Artificiële Intelligentie; Overw. 11 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[178] Titel 1.2. Memorie van Toelichting Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[179] EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR (EDPB-EDPS), *Gezamenlijk advies over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie)*, 18 juni 2021, nr. 5/2021, https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_nl.pdf, 9-10.

DEEL III. TRANSPARANTIEKADER: THEORETISCHE CONCEPTUALISERING VAN BETEKENISVOLLE TRANSPARANTIE

76. Om betekenisvolle transparantie te kunnen beoordelen in de AVG en het Voorstel, is er nood aan een definitie van betekenisvolle transparantie met betrekking tot de verwerking van gegevens door AI-systemen. Er bestaat echter geen universeel aanvaarde definitie van het begrip transparantie, omdat de betekenis van transparantie afgestemd is op de verschillende disciplines die diverse aspecten van transparantie benadrukken.[180] Immers, in bepaalde disciplines duidt transparantie op de fysieke eigenschap van een materiaal en het vermogen ervan om licht door te laten, terwijl in andere vakgebieden transparantie wordt beschouwd als een middel om een gewenst maatschappelijk doel te bereiken, zoals bijvoorbeeld het ter verantwoording roepen van overheidsfunctionarissen.[181]

77. In deze masterproef wordt geopteerd voor een zelf ontwikkelde theoretische conceptualisering en definiëring van het begrip betekenisvolle transparantie in AI-context, gebaseerd op (en in lijn met) de reeds bestaande academische literatuur hieromtrent. Deze definitie vormt zodoende een adequaat kader om de transparantievereisten, zoals enerzijds gedefinieerd in de AVG, en anderzijds, zoals geformuleerd in het Voorstel, op kritische wijze te analyseren en evalueren. De definiëring van betekenisvolle transparantie wordt vertaald in een zelf ontwikkeld transparantiekader.

[180] I. VAROSANEC, "On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI", *International Review of Law, Computers & Technology* 2022, (95) 97.
[181] S. LARSSON en F. HEINTZ, "Transparency in artificial intelligence", *Internet Policy Review* 2020, (1) 5.

Hoofdstuk 1: Situering transparantiekader

78. Het ontwikkelde transparantiekader situeert zich op twee assen; assen aan de hand waarvan transparantie getoetst kan worden. De verticale as illustreert het onderscheid tussen externe en interne transparantie.[182] Externe transparantie refereert naar transparantie die aanbieders, dan wel gebruikers van AI-systemen moeten verschaffen ten aanzien van personen die aan het AI-systeem worden onderworpen.[183] Interne transparantie daarentegen, refereert naar transparantie met betrekking tot de werking van een AI-systeem binnen een organisatie zodoende een gepast en weloverwogen gebruik van AI-systemen te verzekeren.[184]

79. Het Voorstel roept voor AI-systemen met een beperkt risico transparantieverplichtingen in het leven, zowel voor gebruikers als aanbieders van deze AI-systemen, die moeten worden gerespecteerd ten aanzien van de personen die worden onderworpen aan dergelijke AI-systemen. Dit kadert binnen de externe transparantie. De verplichtingen die het Voorstel creëert in hoofde van de aanbieders van hoog risico AI-systemen om ten aanzien van gebruikers transparantie te verzekeren, kadert binnen de interne transparantie.

Echter, de verplichtingen die opgelegd worden aan de aanbieders van hoog risico AI-systemen ten aanzien van de gebruikers, kunnen indirect – wanneer deze laatste eveneens als verwerkingsverantwoordelijken worden beschouwd – tot op zekere hoogte de naleving van hun verplichtingen uit de AVG vergemakkelijken en dragen bijgevolg bij tot externe transparantie.[185]

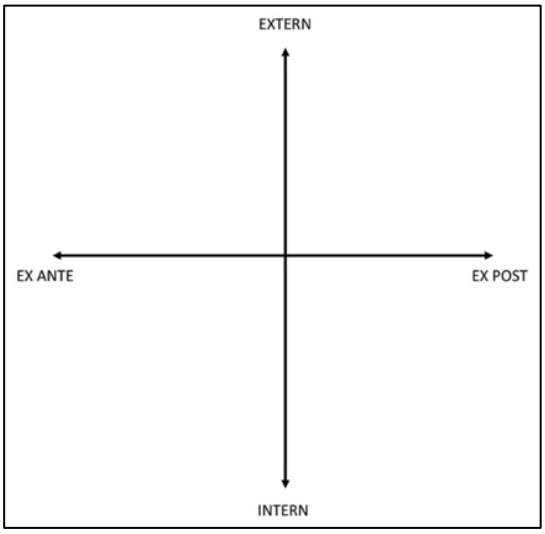
---

[182] T. GILS, E. WAUTERS, B. BENICHOU, J. DE BRUYNE en P. VALCKE, "Artificiële Intelligentie en gegevensbescherming: een verkennende gids", *Kenniscentrum Data en Maatschappij*, 2020, https://data-en-maatschappij.ai/uploads/publications/20200602_Rapport-AI-GDPR_aug2020.pdf, 76.
[183] *Ibid.*
[184] *Ibid.*
[185] S. BARROS VALE, "GDPR and the AI Act interplay: lessons from FPF's ADM case-law report", Future of Privacy Forum 2022 (blog), https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/; EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR (EDPB-EDPS), *Gezamenlijk advies over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie)*, 18 juni 2021, nr. 5/2021, https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_nl.pdf, 10.

80. De horizontale as steunt op het door Felzmann e.a. gehanteerde onderscheid tussen prospectieve en retrospectieve transparantie.[186] Prospectieve transparantie beschrijft de wijze waarop het AI-systeem in het algemeen beslissingen genereert en de algemene werking van het systeem voorafgaand aan de verwerking.[187] Retrospectieve transparantie verwijst daarentegen naar de post hoc verklaringen over hoe en waarom een welbepaalde concrete beslissing werd gegenereerd in een individueel geval.[188]

Naar analogie wordt op dit assenstelsel een onderscheid gemaakt tussen transparantie 'ex ante' en transparantie 'ex post'. Transparantie ex ante heeft betrekking op transparantie in alle fasen van de gegevensverwerking (*infra* 37, nr. 89) voordat een output wordt gegenereerd. Transparantie ex post verwijst naar transparantie met betrekking tot de output.

Figuur 4 illustreert het assenstelsel waarin het transparantiekader moet worden gesitueerd.



Figuur 4: Het assenstelsel met vier kwadranten

81. Refererend naar de centrale onderzoeksvraag, in combinatie met het assenstelsel, wordt de mate van betekenis die kan worden ontleend aan de invulling van de transparantievereisten in de beide Europese rechtsinstrumenten beoordeeld vanuit het oogpunt van de persoon die wordt onderworpen aan het AI-systeem. Bijgevolg strekt de analyse van 'betekenisvolle' transparantie – aan de hand van het vooropgestelde kader – zich enkel uit tot externe transparantie, zowel ex ante als ex post.

[186] H. FELZMANN, E. VILLARONGA, C. LUTZ en A. TAMO-LARRIEUX, "Transparency you can trust: transparency requirements for artificial intelligence between legal norms and contextual concerns", *Big Data & Society* 2019, (1) 2.
[187] *Ibid.*
[188] *Ibid.*

Hoofdstuk 2: Dimensies van transparantie

82. Door transparantie in AI-context aan de hand van verschillende dimensies te omschrijven, wordt een multidimensionaal perspectief gehanteerd dat het veelzijdig karakter van transparantie benadrukt.[189] Op basis van deze twee geïdentificeerde dimensies wordt de mate waarin transparantie haar vertrouwensfunctie (die essentieel wordt geacht bij het gebruik van AI-systemen) al dan niet realiseert met betrekking tot de verwerking van (persoons)gegevens door AI-systemen, systematisch beoordeeld in de AVG en het Voorstel.

Vanuit deze visie wordt transparantie bijgevolg niet beschouwd als een doel op zich, maar als een middel om vertrouwen te creëren in de aanvaarding van het gebruik van op AI-gebaseerde technologieën binnen de maatschappij, in het bijzonder door de personen die worden onderworpen aan AI-systemen.

Afdeling 1: Verklaarbaarheid

83. In eerste instantie dient transparantie vanuit een informerende dimensie te worden beoordeeld waarbij transparantie een belangrijk instrument is om eventuele informatieasymmetrie tussen de persoon die wordt onderworpen aan het AI-systeem en de aanbieder (ontwikkelingsfase), dan wel de gebruiker (implementatiefase) te corrigeren.[190] Het gaat hier over deze informatie die volgens de wetgever dient te worden verstrekt om "inzicht" te bieden in de verschillende fasen van gegevensverwerking door het AI-systeem zodat de ontvanger van de informatie autonoom de verwerking van (persoons)gegevens door het AI-systeem kan doorzien en begrijpen, alsook de gevolgen die aan de verwerking verbonden kunnen worden.[191]

84. Verklaarbaarheid wordt in deze optiek gedefinieerd als de eigenschap van een AI-systeem om – door informatieverstrekking – door de persoon die wordt onderworpen aan het AI-systeem autonoom te worden begrepen.[192]

---

[189] N. BALASUBRAMANIAM, M. KAUPPINEN, K. HIEKKANEN en S. KUJALA, "Transparency and Explainability of AI Systems: Ethical Guidelines in Practice" in V. GERVASI en A. VOGELSANG (eds.), *Requirements Engineering Foundation for Software Quality*, Cham, Springer, 2022, (3) 13; H. FELZMANN, E. FOSCH-VILLARONGA, C. LUTZ en A. TAMO-LARRIEUX, "Towards Transparency by Design for Artificial Intelligence", *Science and Engineering Ethics* 2020, (3333) 3335.

[190] A. BIBAL, M. LOGNOUL, A. DE STREEL en B. FRENAY, "Legal requirements on explainability in machine learning", *Artificial Intelligence & Law* 2021, (149) 150; I. KOIVISTO, *Thinking Inside the Box: The Promise and Boundaries of Transparency in Automated Decision-Making*, San Domenico Fiesoli, European University Institute, 2020, (1) 15; N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI en K. YEUNG, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", *LEADS Lab* 2021, (1) 41.

[191] G. MALGIERI en G. COMANDÉ, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law* 2017, (1) 4.

[192] A. BIBAL, M. LOGNOUL, A. DE STREEL en B. FRENAY, "Legal requirements on explainability in machine learning", *Artificial Intelligence & Law* 2021, (149) 149.

Verklaarbaarheid heeft dus betrekking op het vermogen om de technische processen van een AI-systeem te verklaren.[193] Er wordt bijgevolg een proactieve benadering van informatieverstrekking gehanteerd die toegesneden is op individueel begrip. De aanwezigheid van een informerende dimensie ondersteunt het gegeven dat informatieverstrekking traditioneel, zoals in de AVG, een van de belangrijkste elementen betreft van transparantie. Eveneens wordt het verstrekken van informatie in alle AI-beleidsdocumenten voorafgaand aan het Voorstel beschouwd als een belangrijk onderdeel van de algemene transparantieverplichting.[194]

85. Deze dimensie omvat eveneens een belangrijk relationeel aspect dat de nadruk legt op het gegeven dat informatieverstrekking maar transparantie zal bewerkstelligen als de verstrekte informatie tegemoetkomt aan de informatiebehoeften van de ontvanger. Pas dan kan de informatie daadwerkelijk door de ontvanger worden begrepen.[195] Transparantie kan immers niet als een individuele of geïsoleerde eigenschap worden beschouwd, maar moet steeds beoordeeld worden in de relatie tot de ontvanger van de informatie.[196] Dit gegeven werd reeds benadrukt bij de beschrijving van het *black box*-karakter van bepaalde AI-systemen (*infra* 20-21, nr. 52).

Afdeling 2: Controle

86. Betekenisvolle transparantie vereist niet alleen een dimensie verklaarbaarheid, maar vereist eveneens een dimensie controle. Controle wordt als een inherent onderdeel van betekenisvolle transparantie beschouwd, aangezien – in de optiek van deze masterproef – transparantie maar zinvol kan zijn wanneer het onder meer doeltreffende controle over (persoons)gegevens mogelijk maakt. De doeltreffendheid van de controledimensie is immers een maatstaf voor betekenisvolle transparantie.

87. In deze masterproef worden twee doelstellingen van controle geïdentificeerd op grond waarvan de betekenis van controle – met betrekking tot de verwerking van (persoons)gegevens door AI-systemen – verduidelijkt wordt. De eerste geïdentificeerde doelstelling van controle, is veiligheid en precisie.[197] Deze vorm van controle benadrukt het belang van de menselijke autonomie, in die zin dat men ervan uitgaat dat de tussenkomst van een mens fouten en schade zal voorkomen.[198]

---

[193] THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (HLEG AI), *Ethische Richtsnoeren voor Betrouwbare KI,* 8 april 2019, https://op.europa.eu/nl/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1#, 22.
[194] Hoofdstuk II, sectie 4 Ethische Richtsnoeren voor betrouwbare AI van de AI HLEG; Hoofdstuk 5, D) c) White Paper on Artificial Intelligence – a European approach to excellence and trust
[195] J. KEMPER en K. KOLKMAN, "Transparent to whom? No algorithmic accountability without a critical audience", *Information, communication & society* 2019, (2081) 2086.
[196] H. FELZMANN, E. FOSCH-VILLARONGA, C. LUTZ en A. TAMO-LARRIEUX, "Towards Transparency by Design for Artificial Intelligence", *Science and Engineering Ethics* 2020, (3333) 3336.
[197] J. DAVIDOVIC, "On the purpose of meaningful human control of AI", *SSRN* 2022, (1) 2.
[198] *Ibid.*

In dit opzicht is de vraag/nood om controle maar zinvol wanneer mensen in staat worden geacht beter te zijn in een bepaalde cognitieve taak dan het AI-systeem.[199] Controlemechanismen nemen in dit opzicht de vorm aan van menselijke tussenkomst (in de AVG)/menselijk toezicht (in het Voorstel) of een verbod op het gebruik van AI-systemen voor de verwerking van (persoons)gegevens.

Deze vorm van controle is gelinkt aan transparantie, vermits menselijke tussenkomst/toezicht maar nuttig en doeltreffend kan zijn als de persoon door wie dit wordt uitgeoefend over voldoende informatie beschikt over de werking van het AI-systeem. Deze transparantie kan dus ook betekenisvol zijn omdat ze bijdragen aan de controle die de aan het AI-systeem onderworpen personen kunnen uitoefenen over hun (persoons)gegevens.

88. De tweede geïdentificeerde doelstelling van controle heeft te maken met procedurele rechtvaardigheid en eerlijkheid.[200] In dit opzicht is controle gelieerd aan informatie die de ontvanger van deze informatie moet toelaten de werking en de prestaties van een aanbieder van AI-systemen (ontwikkelingsfase), dan wel een gebruiker van AI-systemen (implementatiefase) te begrijpen, en zo nodig te ageren. Dit bouwt verder op de principaal-agent theorie waarin een principaal (de persoon die wordt onderworpen aan het AI-systeem) informatie van de agent (aanbieder, respectievelijk gebruiker van het AI-systeem) nodig heeft om na te gaan of de agent zich aan het contract houdt.[201]

Toegepast op de verwerking van (persoons)gegevens door AI-systemen, moet controle de principaal toelaten om voldoende vertrouwen te hebben in de rechtmatigheid van de verwerking door het AI-systeem. De dimensie controle, als onderdeel van de notie 'betekenisvolle transparantie', moet de aan het AI-systeem onderworpen persoon in dit opzicht toelaten (eventueel) te ageren door zijn subjectieve rechten tegenover de aanbieder (ontwikkelingsfase), dan wel de gebruiker (implementatiefase) uit te oefenen.[202] Dit wordt in de literatuur omschreven als *'rights-enabling transparency'*.[203]

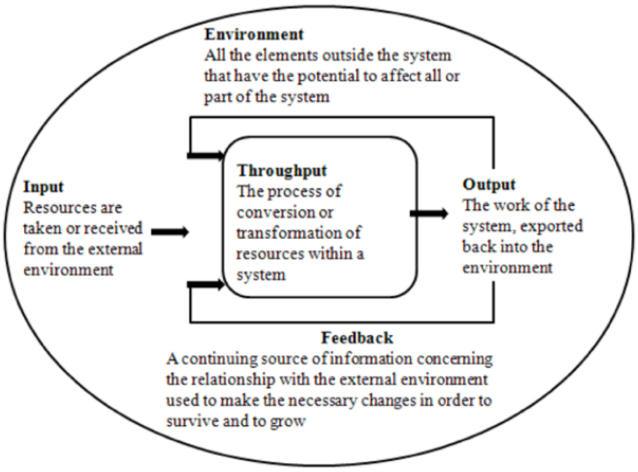
---

[199] *Ibid.*
[200] *Ibid.*, 3-4.
[201] D. TIELENBURG, *The 'Dark Sides' of Transparency: Rethinking Information Disclosure as a Social Praxis*, onuitg. masterproef Filosofie Universiteit Utrecht, 2018, 11.
[202] N. SMUHA, "Beyond a Human rights-based approach to AI Governance: Promise, Pitfalls, Plea", *Philosophy & Technology* 2020, (1) 14; S. WACHTER, B. MITTELSTADT en C. RUSSEL, "Counterfactual explanations without opening the black box: automated decisions and the GDPR", *Harvard Journal of Law & Technology* 2018, (842) 844.
[203] P. HACKER en J. PASSOTH, "Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond" in A. HOLZINGER, R. GOEBEL, R. FONG, T. MOON, K. MÜLLER en W. SAMEK (eds.), *xxAI – Beyond Explainable AI*, Lecture Notes in Computer Science, 2022, (343) 344; A. SELBST en J. POWLES, "Meaningful information and the right to explanation", *International data Privacy Law* 2017, (233) 236.

Hoofdstuk 3: Drie fasen

89. De invulling van betekenisvolle transparantie zal eveneens vanuit de verschillende fasen van de gehele levenscyclus van de verwerking van (persoons)gegevens benaderd worden, om op die manier over een volledig kader te beschikken waaraan de transparantievereisten in de AVG en het Voorstel kunnen worden getoetst.[204] Deze fasen zijn immers een belangrijk fundament waarop het kader is gebouwd en biedt een basis voor het in kaart brengen van de uitdagingen in verband met AI gedurende de volledige gegevensverwerkingscyclus.[205] De dimensies verklaarbaarheid en controle zullen in elke fase van de gegevensverwerking verduidelijkt worden.

90. De drie fasen van de gegevensverwerking worden gedefinieerd en verduidelijkt aan de hand van het wetenschappelijk model van de Systeemtheorie van Katz en Kahn (figuur 5).[206]



Figuur 5[207]: Katz en Kahn Systeemtheorie

[204] V. RUBIN, J. BURKELL, S. CORNWELL, T. ASUBIARO, Y. CHEN, D. POTTS en C. BROGLY, "AI Opaqueness: What Makes AI Systems More Transparent?", *Proceedings of the Annual Conference of CAIS* 2020, (1) 1; J. WALMSLEY, "Artificial Intelligence and the value of transparency", *AI & society* 2021, (585) 586.
[205] A. BAQAIS, Z. BAIG en M. GROBLER, "Transparency and Opacity in AI Systems: An Overview", Interaction Design for explainable AI 2018, (12) 14; T. TIMAN en F. GROMME, "Wat is rechtvaardige AI? Een kader voor het ontwikkelen en toepassen van algoritmes voor automatische besluitvorming", *Beleid en Maatschappij* 2020, (425) 433.
[206] B. RAMOSAJ en G. BERISHA, "Systems Theory and Systems Approach to Leadership", *ILIRIA International Review* 2014, (59) 61.
[207] *Ibid.*

91. In de inputfase worden (persoons)gegevens (data) verzameld om het AI-systeem te "voeden". Transparantie heeft in deze fase zowel betrekking op de dataverzameling voor het trainen en gebruiken van AI-systemen, alsook op de kwaliteit van de aangeleverde data in de implementatiefase en datasets in de ontwikkelingsfase van AI-systemen.[208] Deze fase heeft betrekking op transparantie ex ante (*supra* 33, nr. 80).

Dataverzameling gaat dus over hoe en welke gegevens verzameld worden van de persoon die aan het AI-systeem onderworpen wordt.[209] Zo kan onder meer de verzameling van gegevens die als input fungeren voor de training van het AI-algoritme een verwerking van persoonsgegevens uitmaken.[210] Dit kan bijvoorbeeld in de hypothese waarin persoonsgegevens automatisch worden gedetecteerd door *cookies*.[211]

De werking van AI-systemen, alsook de mogelijke vertekeningen ervan, worden daarnaast ook bepaald door de kwaliteit van de aangeleverde data(sets).[212] Door transparantie te bieden omtrent deze zaken, wordt het mogelijk de redenen te identificeren waarom het AI-systeem foutieve beslissingen heeft gegenereerd, wat op zijn beurt kan helpen om ongewenste gevolgen voor de personen die worden onderworpen aan het AI-systeem te remediëren en toekomstige fouten te voorkomen.[213]

---

[208] N. BALASUBRAMANIAM, M. KAUPPINEN, K. HIEKKANEN en S. KUJALA, "Transparency and Explainability of AI Systems: Ethical Guidelines in Practice" in V. GERVASI en A. VOGELSANG (eds.), *Requirements Engineering Foundation for Software Quality*, Cham, Springer, 2022, (3) 11; E. BERTINO, "The Quest for Data Transparency", *IEEE Computer Society* 2020, (67) 68; H. FELZMANN, E. FOSCH-VILLARONGA, C. LUTZ en A. TAMÒ-LARRIEUX, "Towards Transparency by Design for Artificial Intelligence", *Science and Engineering Ethics* 2020, (3333) 3346-3348; T. GILS, E. WAUTERS, B. BENICHOU, J. DE BRUYNE en P. VALCKE, "Artificiële Intelligentie en gegevensbescherming: een verkennende gids", *Kenniscentrum Data en Maatschappij*, 2020, https://data-en-maatschappij.ai/publicaties/ai-en-gegevensbescherming-een-verkennende-gids, 82; P. VAN DE WAERDT, "Information asymmetries: recognizing the limits of the GDPR on the data-driven market", *Computer Law & Security Review* 2020, (1) 15.

[209] T. URBAN, D. TATANG, M. DEGELING, T. HOLZ en N. POHLMANN, "The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under the GDPR", *Cornell University* 2018, (1) 8.

[210] P. VALCKE en S. ROSSELLO, "The artificial lawyer. Reflecties over de impact van AI op het recht en de rechtspraktijk" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (175) 187.

[211] *Ibid.*

[212] P. HACKER, "A legal framework for AI training data – from first principles to the Artificial Intelligence Act", *Law, Innovation and Technology* 2021, (257) 260; F. MENGES, T. LATZO, M. VIELBERTH, S. SOBOLA, H. PÖHLS, B. TAUBMANN, J. KÖSTLER, A. PUCHTA, F. FREILING, H. REISER en G. PERNUL, "Towards GDPR-compliant data processing in modern SIEM systems", *Computers & Security* 2021, (1) 1; GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 13 en 33.

[213] H. FELZMANN, E. FOSCH-VILLARONGA, C. LUTZ en A. TAMÒ-LARRIEUX, "Towards Transparency by Design for Artificial Intelligence", *Science and Engineering Ethics* 2020 (3333) 3347.

92. De tweede fase is de procesfase die de eigenlijke verwerking door het AI-systeem representeert. Dit is het proces van conversie of transformatie van een input tot een output, opnieuw zowel voor het trainen als gebruiken van AI-systemen. Zo kan bijvoorbeeld het algoritme van een AI-gezichtsherkenningssysteem getraind worden met foto's van bepaalde personen.[214] In deze fase heeft transparantie betrekking op het gegeven dat (persoons)gegevens worden verwerkt door een AI-systeem, de wijze waarop deze input wordt verwerkt tot een output, alsook op de risico's die aan deze verwerking verbonden zijn.[215]

In deze fase houdt transparantie in de dimensie verklaarbaarheid in het bijzonder verband met het verschaffen van nauwkeurige informatie over de reële mogelijkheden en reële beperkingen van AI-systemen, zodat valse verwachtingen bij de betrokkenen en onjuiste interpretaties van de resultaten worden vermeden.[216] Deze fase heeft betrekking op transparantie ex ante (*supra* 33, nr. 80).

93. Transparantie dient eveneens te worden verzekerd over het resultaat van de verwerking, namelijk de output. In deze fase wordt de nadruk gelegd op deze informatie die de aan het AI-systeem onderworpen persoon moet toelaten te weten welke de gevolgen zijn van een bepaalde output. Deze fase heeft betrekking op transparantie ex post (*supra* 33, nr. 80).

Hoofdstuk 4: Integratie van de dimensies en fasen

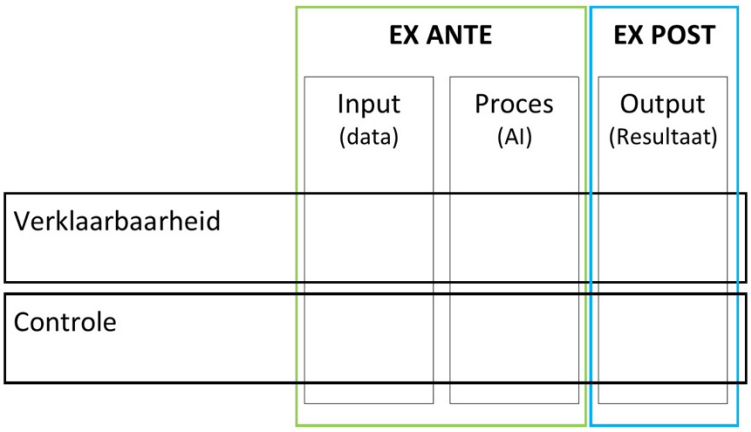
94. Het concept betekenisvolle transparantie omvat twee belangrijke aspecten, met name een verklaarbaarheidsdimensie en een controledimensie. Betekenisvolle transparantie impliceert bijgevolg enerzijds maximale reductie van de informatieasymmetrie in de verschillende fasen van de gegevensverwerking – mits respect voor het relationele aspect van de verklaarbaarheidsdimensie – en anderzijds doeltreffende controle over de (persoons)gegevens.

95. Betekenisvolle transparantie vereist dus enerzijds daadwerkelijke transparantie op het niveau van de dimensie verklaarbaarheid in de verschillende fasen van de gegevensverwerking en anderzijds doeltreffende controle in de controledimensie. Betekenisvolle transparantie stelt bijgevolg uiteenlopende eisen in deze verscheidene stadia.[217]

---

[214] P. VALCKE en S. ROSSELLO, "The artificial lawyer. Reflecties over de impact van AI op het recht en de rechtspraktijk" in J. DE BRUYNE en N. BOUTECA (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, (175) 187-188.
[215] *Ibid*.
[216] J. DE BRUYNE en T. GILS, "Wat brengt de toekomst: de regulering van artificiële intelligentie" in P. VAN EECKE (ed.), *Recht & Elektronische handel*, Mortsel, Intersentia, 2021, (581) 602.
[217] T. ZARSKY, "Transparent Predictions", *University of Illinois Law Review* 2013, (1503) 1532.

Het zelf ontwikkelde transparantiekader plaatst de dimensies horizontaal ten opzichte van de verticale fasen. Zo ontstaan er zes te beschrijven vlakken. In deel IV en V wordt het transparantiekader met zijn zes vlakken toegepast op beide Europese rechtsinstrumenten; elke dimensie wordt beoordeeld met betrekking tot elke fase (zie bijlagen A en B). De combinatie van de dimensies en de fasen, resulteert in onderstaand transparantiekader (figuur 6).



Figuur 6: Het transparantiekader

Concluderend gesteld, gaat de dimensie verklaarbaarheid over die informatie die ter beschikking moet worden gesteld over de input, het proces en de output. Gaat het over de controledimensie, dan gaat het over controlemechanismen die controle toelaten over de (persoons)gegevens in de inputfase, in de procesfase en in de outputfase.

DEEL IV. TOEPASSING VAN HET TRANSPARANTIEKADER OP DE AVG

96. Vermits de AVG van toepassing is op de verwerking van persoonsgegevens door AI-systemen, moet de verwerkingsverantwoordelijke de bepalingen van de AVG respecteren wanneer deze persoonsgegevens verwerkt door middel van AI-systemen. AI-systemen hebben in de regel grote hoeveelheden persoonsgegevens nodig om optimaal te functioneren. Dit kan aanzienlijke risico's met zich meebrengen voor de rechten en vrijheden van personen. De bepalingen van de AVG zijn bijgevolg van groot belang in functie van de bestrijding van de risico's en het bieden van passende waarborgen.[218]

97. Echter, de toepassing en naleving van het huidig regelgevend kader kan bijzonder uitdagend zijn wanneer persoonsgegevens door AI-systemen worden verwerkt, omdat het transparantiebeginsel uit de AVG en het potentiële *black box*-karakter van AI, alsook haar zelflerend vermogen op gespannen voet staan. In dit onderdeel wordt nader onderzocht of, en in welke mate, de bepalingen van de AVG die transparantie dienen te verzekeren bij de verwerking van persoonsgegevens door AI-systemen, compatibel zijn met de technische aard van op AI-gebaseerde technologieën. Daarnaast wordt eveneens nagegaan of deze bepalingen in staat zijn om betekenisvolle transparantie te verzekeren in AI-context ten aanzien van personen die aan een AI-systeem worden onderworpen (in casu: de betrokkenen wiens persoonsgegevens worden verwerkt).

98. Deel IV poogt in het bijzonder – aan de hand van de invulling van het transparantiekader – een antwoord te formuleren op de eerste deelvraag, met name: "zijn er grenzen aan de definiëring van de transparantievereisten in de AVG bij de toepassing van AI-systemen?".

Hoofdstuk 1: Overkoepelende transparantieverplichting – modaliteiten van transparantie

99. Vooraleer over te gaan tot de daadwerkelijke invulling van het zelf ontwikkelde transparantiekader met de verscheidene geïdentificeerde transparantieverplichtingen in de artikelen 13-15 AVG, moet vooreerst de overkoepelende transparantieverplichting ex artikel 12 AVG toegelicht worden. Artikel 12 AVG bevat een overkoepelende transparantieverplichting die het beginsel van transparante informatie en communicatie vaststelt.

[218] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 6.

Deze verplichting is overkoepelend, omdat zij zowel toepassing vindt op de volledige gegevensverwerkingscyclus (*i.e.* de drie reeds genoemde verticale fasen), alsook op de twee geïdentificeerde horizontale dimensies 'verklaarbaarheid' en 'controle'.[219]

100. Met betrekking tot de vermeende toepasselijkheid van artikel 12 AVG op deze twee dimensies, wordt verwezen naar de twee – door het EDPB aangewezen – kerngebieden waarop de overkoepelende verplichting toepassing vindt. Het gaat met name om de verstrekking van informatie aan betrokkenen in verband met een behoorlijke verwerking van persoonsgegevens (*i.e.* de dimensie verklaarbaarheid), en om de communicatie met betrokkenen over hun rechten uit hoofde van de AVG (*i.e.* de dimensie controle).[220]

101. Artikel 12 AVG bevat algemene voorschriften/modaliteiten waaraan de informatie of communicatie over de verscheidene fasen heen in de verklaarbaarheidsdimensie moet voldoen om de informatieasymmetrie maximaal te reduceren. Deze modaliteiten vereisen dat de informatie of communicatie 1) beknopt, transparant en begrijpelijk moet zijn, 2) er een duidelijke en eenvoudige taal moet gebruikt worden, 3) de informatie gemakkelijk toegankelijk moet zijn, 4) de informatie schriftelijk *"of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen"* moet worden verstrekt en 5) de informatie kosteloos moet worden verstrekt.

Deze vereisten ondersteunen duidelijk het relationele aspect van de dimensie verklaarbaarheid. Ze dragen bij tot het maximaal beperken van eventuele informatieasymmetrie tussen de betrokkene en de verwerkingsverantwoordelijke.

Afdeling 1: Kwalitatieve voorwaarden van informatie en communicatie

102. De verstrekking van de informatie aan en de communicatie met betrokkenen dient in een beknopte, transparante, begrijpelijke vorm te gebeuren. De vereiste van 'beknoptheid' houdt een verplichting in voor de verwerkingsverantwoordelijke om de informatie/communicatie op een efficiënte en bondige wijze weer te geven om informatiemoeheid te voorkomen.[221]

[219] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679*, 11 april 2018, WP260rev.01, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf, 6.
[220] *Ibid.,* 4.
[221] *Ibid.,* 7.

103. Vervolgens dient de informatie/communicatie ook 'transparant' te zijn. In deze optiek houdt transparantie (in de enge zin) in dat de informatie inzake gegevensverwerking duidelijk afgescheiden dient te zijn van andere informatie die niet geassocieerd is met gegevensverwerking of -bescherming, zoals contractbepalingen of algemene gebruiksvoorwaarden.[222] Ten slotte dient de informatie 'begrijpelijk' te zijn.

Deze kwaliteitsvoorwaarde impliceert dat de informatie begrepen moet kunnen worden door een gemiddeld lid van het beoogde (doel)publiek.[223] Deze vereiste houdt nauw verband met de vereiste om duidelijke en eenvoudige taal te hanteren.[224] In dit kader dient de verwerkingsverantwoordelijke kennis te hebben van de personen van wie gegevens worden verkregen, teneinde te kunnen bepalen wat de doelgroep waarschijnlijk zal begrijpen.[225]

Afdeling 2: De vorm van de informatie en communicatie – duidelijke en eenvoudige taal

104. Opdat aan de kwalitatieve voorwaarden van de informatie zou kunnen worden voldaan, moet duidelijke en eenvoudige taal gebruikt worden.[226] Dit betekent dat informatie op een zo eenvoudig mogelijke manier moet worden aangeboden, waarbij complexe zinnen en zinsconstructies dienen te worden vermeden, alsook abstracte en ambivalente formuleringen die ruimte laten voor verschillende interpretaties.[227] Deze taalvereiste draagt in het bijzonder bij tot de begrijpelijkheid van de informatie.

In dit kader geeft het EDPB in haar richtsnoeren inzake transparantie aan welke constructies of woorden beter worden vermeden. Algemeen wordt aanvaard dat de informatie die aan de betrokkene wordt verstrekt, geen te juridische, technische of specialistische taal of terminologie mag bevatten.[228] Deze stelling dient evenwel genuanceerd te worden. Dergelijke juridische of vaktechnische taal of terminologie kan evenwel aanvaard worden, mits er tegelijkertijd een versie wordt toegevoegd die voor de gemiddelde betrokkene begrijpelijk is.[229]

---

[222] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679*, 11 april 2018, WP260rev.01, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf, 7.
[223] *Ibid.*, 8.
[224] *Ibid.*
[225] *Ibid.*
[226] D. DE BOT (ed.), De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit, Mechelen, Wolters Kluwer Belgium, 2020, 604.
[227] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679*, 11 april 2018, WP260rev.01, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf, 9.
[228] D. DE BOT (ed.), De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit, Mechelen, Wolters Kluwer Belgium, 2020, 605.
[229] *Ibid.,* 605.

Afdeling 3: De vorm van de informatie – gemakkelijk toegankelijk

105. Zoals gestipuleerd door artikel 12, lid 1 AVG, dient de verstrekking van informatie aan de betrokkene in een gemakkelijk toegankelijke vorm te geschieden. Dit betekent dat de betrokkene de informatie niet zelf moet uit- of opzoeken, maar dat het voor de betrokkene onmiddellijk duidelijk moet zijn waar en hoe deze informatie te vinden is.[230] Voorbeelden van gemakkelijk toegankelijke informatie zijn een rechtstreekse vermelding van de informatie, het plaatsen van een link naar de informatie, het duidelijk markeren van de informatie of het presenteren van de informatie als een antwoord op een vraag.[231]

In principe heeft deze vereiste van gemakkelijk toegankelijke vorm enkel betrekking op de informatie, aangezien met betrekking tot de communicatie kan en mag worden uitgegaan van individuele communicatie van de verwerkingsverantwoordelijke naar de betrokkene, zodat deze op geen enkele manier moet zoeken naar die communicatie.[232]

Afdeling 4: De manier van informatieverstrekking

106. Artikel 12, lid 1 AVG bepaalt dat de informatie schriftelijk of met andere middelen wordt verstrekt. De schriftelijke informatieverstrekking aan of communicatie met betrokkenen wordt als uitgangspunt beschouwd, maar de AVG staat ook het gebruik toe van niet nader gespecifieerde middelen toe, zoals elektronische middelen.[233] De belangrijkste vormen van schriftelijke elektronische middelen zijn informatienota's en/of privacyverklaringen.[234] Andere schriftelijke elektronische middelen zijn contextuele '*just-in-time'*-pop-upberichten, 3D Touch-berichten, mededelingen die verschijnen wanneer de muis eroverheen beweegt en privacydashboards.[235]

---

[230] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679*, 11 april 2018, WP260rev.01, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf, 8.
[231] *Ibid.*
[232] D. DE BOT (ed.), De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit, Mechelen, Wolters Kluwer Belgium, 2020, 605.
[233] *Ibid.*
[234] *Ibid.,* 606.
[235] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679*, 11 april 2018, WP260rev.01, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf, 13.

Afdeling 5: Het kosteloze karakter van de informatieverstrekking

107. Krachtens artikel 12, lid 5 AVG kunnen verwerkingsverantwoordelijken in principe geen kosten aanrekenen aan betrokkenen voor de verstrekking van informatie uit hoofde van de artikelen 13-14 AVG, of voor de mededelingen en maatregelen uit hoofde van de artikelen 15 t.e.m. 22 AVG (inzake de rechten van betrokkenen).[236] Echter, indien een verzoek van een betrokkene kennelijk ongegrond of buitensporig is, voorziet artikel 12, lid 5 AVG in de mogelijkheid voor de verwerkingsverantwoordelijke om een redelijke vergoeding in rekening te brengen.

Het EDPB merkt in dit kader op dat dit aspect van transparantie ook inhoudt dat informatie die is verstrekt op grond van transparantieverplichtingen, niet afhankelijk kan worden gesteld van financiële transacties, zoals de betaling voor of de aankoop van diensten of goederen.[237]

Hoofdstuk 2: Verklaarbaarheid in de AVG

108. In dit hoofdstuk wordt de dimensie verklaarbaarheid met betrekking tot de drie fasen, namelijk de input, het proces en de door het AI-systeem gegenereerde output beoordeeld vanuit het standpunt van de AVG. Bij de invulling van de drie beschikbare vlakken binnen de dimensie verklaarbaarheid van het ontwikkelde transparantiekader, worden de – in de artikelen 13-15 AVG – relevante transparantieverplichtingen in verband met de verwerking van persoonsgegevens door AI-systemen ingepast (zie bijlage A).

109. Volledigheidshalve wordt gewezen op het onderscheid tussen de hypothese waarin de gegevens rechtstreeks (artikel 13 AVG), dan wel onrechtstreeks (artikel 14 AVG) bij de betrokkene worden verzameld. Dit onderscheid tussen beide is van belang, gezien onder meer het ogenblik van de informatieverstrekking anders geregeld is. Het tijdig verstrekken van de informatie is immers een fundamenteel element van transparantie, alsook de verplichting om gegevens op een behoorlijke wijze te verwerken.[238]

In de hypothese waarbij de gegevens rechtstreeks bij de betrokkene worden verzameld, moet de informatie op grond van artikel 13 AVG *"bij de verkrijging van persoonsgegevens"* worden verstrekt. Deze zinsnede dient op zo'n manier te worden geïnterpreteerd dat het de betrokkene maximale bescherming en controle biedt, waardoor de informatie zo snel mogelijk moet worden verstrekt.[239]

---

[236] *Ibid.,*15.
[237] *Ibid.*
[238] *Ibid.,*17.
[239] D. DE BOT (ed.), De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit, Mechelen, Wolters Kluwer Belgium, 2020, 633.

Bij voorkeur gebeurt de informatieverstrekking voorafgaandelijk aan de verwerking, zeker als de informatie de betrokkene moet toelaten om de verwerking al dan niet te aanvaarden, zoals bij de informatie over geautomatiseerde besluitvorming.[240]

Wanneer het daarentegen gaat om de hypothese waarin persoonsgegevens indirect verkregen worden, worden de termijnen waarbinnen de vereiste informatie aan de betrokkene moet worden verstrekt, vermeld in artikel 14, lid 3, a) t.e.m. c) AVG. In beginsel dient de informatie te worden verstrekt binnen een "redelijke termijn" na de verkrijging van de persoonsgegevens, maar in elk geval uiterlijk binnen één maand, "afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt" (artikel 14, lid 3, a) AVG).

Afdeling 1: Input

110. In de inputfase moet transparantie worden verzekerd met betrekking tot de dataverzameling voor het trainen en gebruiken van AI-systemen, alsook met betrekking tot de kwaliteit van de aangeleverde data in de implementatiefase en datasets in de ontwikkelingsfase van AI-systemen.[241] Transparantie met betrekking tot de input, gaat in wezen over de vraag met welke persoonsgegevens het AI-systeem wordt gevoed en wat de kwaliteit ervan is.

111. De reeds eerder benoemde informatieasymmetrie tussen personen die worden onderworpen aan AI-systemen (in casu: de betrokkenen) en de aanbieders, dan wel de gebruikers van AI-systemen (in casu: de verwerkingsverantwoordelijken) ontstaat al vanaf het moment waarop de verzameling van persoonsgegevens plaatsvindt.[242] Transparantie vereist met betrekking tot de input dat een begrijpelijk beschrijvend overzicht wordt gegeven van de persoonsgegevens waarmee het systeem werd gevoed (zowel voor het trainen als gebruiken van het AI-systeem), alsook van de maatregelen die werden genomen om de kwaliteit van de aangeleverde data(sets) te handhaven en te verzekeren.

---

[240] *Ibid.*

[241] EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR (EDPB-EDPS), *Gezamenlijk advies over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie)*, 18 juni 2021, nr. 5/2021, https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_nl.pdf, 20.

[242] T. URBAN, D. TATANG, M. DEGELING, T. HOLZ en N. POHLMANN, "The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under GDPR", *Cornell University* 2018, (1) 1; P. VAN DE WAERDT, "Information asymmetries: recognizing the limits of the GDPR on the data-driven market", *Computer Law & Security Review* 2020, (1) 3.

Betrokkenen dienen over deze aspecten van AI-systemen te worden geïnformeerd, aangezien informatie hieromtrent nuttig is voor betrokkenen om de gegevensverwerking door het systeem te begrijpen en controle over de (persoons)gegevens te behouden.[243] Controle moet in dit opzicht gelinkt worden met de doelstelling van procedurele rechtvaardigheid en eerlijkheid. Immers, door informatie te verstrekken omtrent welke (persoons)gegevens van de betrokkene werden verzameld, alsook omtrent de kwaliteit van de aangeleverde data(sets), kan de betrokkene de rechtmatigheid van de verwerking beoordelen en eventueel ageren. Dit is vooral belangrijk in tijden van Big Data waarin de kwaniteit van de gegevens soms belangrijker wordt geacht dan de kwaliteit ervan.

1.1. Informatie omtrent de dataverzameling

112. Met betrekking tot het aspect van de dataverzameling, voorzien de artikelen 14, lid 1, d) en 15, lid 1, b) AVG dat de verwerkingsverantwoordelijke – om een eerlijke en transparante verwerking te garanderen – de betrokkene moet informeren over de betrokken categorieën van persoonsgegevens die werden verzameld om het AI-systeem te "voeden". Overweging 39 AVG stipuleert eveneens in dit kader dat het voor natuurlijke personen onder meer transparant dient te zijn dat hun persoonsgegevens worden verzameld. Daarenboven vereist artikel 30 AVG dat elke verwerkingsverantwoordelijke een register van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvindt, bijhoudt. Dit register bevat onder meer een beschrijving van de verzamelde categorieën van persoonsgegevens.[244]

113. Wanneer het in de praktijk – vanwege het groot aantal actoren en/of de technologische complexiteit – voor een betrokkene moeilijk is te weten en te begrijpen welke persoonsgegevens worden verzameld, benadrukt overweging 58 AVG nog eens extra het belang van het relationele aspect van de dimensie verklaarbaarheid. De informatie omtrent de dataverzameling dient namelijk steeds beknopt, eenvoudig toegankelijk en begrijpelijk te zijn. Daarenboven dient een duidelijke en eenvoudige taal te worden gehanteerd, en eventueel, gebruik worden gemaakt van aanvullende visualisatie.

114. De transparantievereisten, zoals gestipuleerd in de AVG, met betrekking tot de dataverzameling, staan in het bijzonder op gespannen voet met de gegevensverzameling door '*Data driven Companies'*. Online zoekmachines (zoals Google), sociale mediaplatformen (zoals Facebook en Instagram) en gerichte reclamediensten maken gebruik van een "*data-driven*" businessmodel dat gebaseerd is op het op grote schaal verzamelen van persoonsgegevens.[245]

---

[243] N. BALASUBRAMANIAM, M. KAUPPINEN, K. HIEKKANEN en S. KUJALA, "Transparency and Explainability of AI Systems: Ethical Guidelines in Practice" in V. GERVASI en A. VOGELSANG (eds.), *Requirements Engineering Foundation for Software Quality*, Cham, Springer, 2022, (3) 15.
[244] Art. 30, lid 1, c) AVG.
[245] P. VAN DE WAERDT, "Information asymmetries: recognizing the limits of the GDPR on the data-driven market", *Computer Law & Security Review* 2020, (1) 1.

Dergelijke datagedreven bedrijven verzamelen via steeds complexer wordende dataverzamelingsmethoden veel meer persoonsgegevens dan de betrokkene weet of redelijkerwijze kan verwachten, waardoor de informatieasymmetrie tussen betrokkenen en deze datagedreven bedrijven aanzienlijk vergroot in de inputfase van de gegevensverwerkingscyclus.[246]

Deze bedrijven hebben toegang tot enorme hoeveelheden gegevens die aangeven wat we doen, wat we belangrijk vinden en waarnaar we zoeken in digitale ruimten. Zo verzamelen datagedreven bedrijven niet alleen gegevens die bewust door de betrokkene worden verstrekt, maar verzamelen zij ook gegevens die worden "waargenomen" tijdens het gebruik door de betrokkene van het sociale-mediaplatform, de zoekmachine of een andere onlinedienst.[247] Daarnaast bezitten ook online advertentienetwerken de mogelijkheid om grote hoeveelheden persoonsgegevens te verwerken door het plaatsen van *cookies*. Het is onwaarschijnlijk dat betrokkenen er zich van bewust zijn dat hun persoonsgegevens worden verzameld, niet alleen door de websites die zij bezoeken, maar ook door deze advertentienetwerken.[248]

115. Gelet op de omvang, alsook de wijze van gegevensverzameling door datagedreven bedrijven, is het moeilijk zicht te houden op datastromen en de wijze waarop data worden verzameld en gebruikt. Wanneer het voor individuen moeilijk is om een duidelijk beeld te krijgen van de hoeveelheid gegevens die over hen werden verzameld, uit welke bronnen en met wie ze zijn gedeeld, ontstaat een aanzienlijk gebrek aan controle van betrokkenen over hun persoonsgegevens in de inputfase van de gegevensverwerking.[249] Betrokkenen kunnen immers zelf moeilijk de volledigheid van deze informatie controleren, waardoor deze in sterke mate afhankelijk zijn van de inspanningen van de verwerkingsverantwoordelijke om volledige informatie te verstrekken.

Het huidige ecosysteem van dataverzameling is zo complex geworden, waardoor het twijfelachtig is of de artikelen 14, lid 1, d) en 15, lid 1, b) AVG in staat zijn deze informatieasymmetrie in de inputfase op de datagedreven markt te beperken.

[246] *Ibid.*
[247] *Ibid.*
[248] *Ibid.*
[249] E. SCHLEHAHN en R. WENNING, "GDPR Transparency Requirements and Data Privacy Vocabularies" in E. KOSTA, J. PIERSON, D. SLAMANIG, S. HÜBNER en S. KRENN (eds.), *Privacy and Identity Management. Fairness, Accountability and Transparency in the Age of Big Data*, Cham, Springer, 2018, (95) 96.

1.2. Informatie omtrent de kwaliteit van de aangeleverde data(sets)

116. Het beginsel van 'juistheid' ex artikel 5, lid 1, d) AVG heeft betrekking op de kwaliteit van de data voor de ontwikkeling van op AI gebaseerde systemen en stipuleert dat persoonsgegevens 'juist' moeten zijn en zo nodig, moeten worden geactualiseerd.[250] Volgens het EDPB moeten de verwerkingsverantwoordelijken de kwaliteit van persoonsgegevens in het bijzonder in het oog houden bij het verzamelen van persoonsgegevens om AI-systemen te voeden.[251] Immers, wanneer persoonsgegevens waarmee het AI-systeem wordt gevoed, inaccuraat of onjuist zijn, zullen ook de daaruit resulterende besluiten inaccuraat of onjuist zijn. Een aforisme dat in dit kader vaak wordt gebruikt, is "*garbage in, garbage out*".[252]

Met betrekking tot AI-systemen die gebruik maken van *machine learning* methoden, moet dit beginsel niet alleen gelden voor persoonsgegevens die worden verzameld om een AI-systeem te voeden in de implementatiefase ervan, maar eveneens voor persoonsgegevens in een training dataset waarmee het AI-systeem in de ontwikkelingsfase wordt gevoed.[253] Verwerkingsverantwoordelijken dienen in dit kader passende technische en organisatorische maatregelen te treffen die de kwaliteit van de data verzekert.[254]

117. Verwerkingsverantwoordelijken moeten op grond van de algemene verantwoordingsplicht kunnen bewijzen dat de nodige organisatorische en technische maatregelen genomen werden én doeltreffend zijn.[255] Zo moeten verwerkingsverantwoordelijken de eigenschappen van de datasets en de genomen maatregelen om de kwaliteit ervan te waarborgen, documenteren.[256] Dit draagt bij tot het verzekeren van transparantie met betrekking tot de kwaliteit van de aangeleverde data(sets) betreffende de inputfase van de gegevensverwerking, op voorwaarde dat deze documentatie aangepast is aan het vooropgestelde publiek. Dit laatste is belangrijk, gelet op het relationele aspect van de dimensie verklaarbaarheid.

---

[250] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf, 9.
[251] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 13.
[252] S. THIRUMURUGANATHAN, M. KUNJIR, M. OUZZANI en S. CHAWLA, "Automated Annotations for AI Data and Model Transparency", *Qatar Computing Research Institute* 2021, (1) 2.
[253] SCIENTIFIC FORESIGHT UNIT (STOA), The impact of the General Protection Regulation (GDPR) on *artificial intelligence, juni 2020*, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf, 62.
[254] Art. 25 AVG; Overw. 71 AVG.
[255] Art. 5, lid 2 AVG.
[256] T. GILS, E. WAUTERS, B. BENICHOU, J. DE BRUYNE en P. VALCKE, "Artificiële Intelligentie en gegevensbescherming: een verkennende gids", *Kenniscentrum Data en Maatschappij*, 2020, https://data-en-maatschappij.ai/publicaties/ai-en-gegevensbescherming-een-verkennende-gids, 31.

Afdeling 2: Proces

2.1. Informatie omtrent het bestaan van geautomatiseerde besluitvorming

118. Wanneer verwerkingsverantwoordelijken gebruik maken van geautomatiseerde besluitvorming bij de verwerking van persoonsgegevens, dienen zij dit aan de betrokkene mee te delen – om een behoorlijke en transparante verwerking te waarborgen – op grond van de artikelen 13, lid 2, onder f); 14, lid 2, onder g) en artikel 15, lid 1, onder h) AVG. Betrokkenen moeten op grond van deze bepalingen dus worden geïnformeerd wanneer ze persoonsgegevens meedelen aan dergelijke systemen.[257] Het is bijgevolg van belang dat verwerkingsverantwoordelijken duidelijk in kaart brengen welke verwerkingen door middel van AI-systemen geautomatiseerd verlopen.[258]

119. De vraag of geautomatiseerde besluitvorming wordt toegepast voor de verwerking van persoonsgegevens, gaat in casu over de vraag of een AI-systeem al dan niet als middel wordt gehanteerd om geautomatiseerde besluiten te genereren. Gezien de nadruk bij deze transparantieverplichting wordt gelegd op informatie omtrent het daadwerkelijke bestaan van AI-systemen als middel van geautomatiseerde besluitvorming, wordt deze transparantieverplichting gecatalogeerd onder de procesfase. Het is immers noodzakelijke informatie over het proces.

2.2. Informatie omtrent de conversie door het AI-systeem van een input tot een output

120. Om ten aanzien van de betrokkenen een behoorlijke en transparante verwerking te waarborgen, moeten verwerkingsverantwoordelijken – op grond van de artikelen 13, lid 2, onder f); 14, lid 2 onder g) en 15, lid 1 onder h) AVG – de betrokkenen eveneens 'nuttige' informatie verstrekken over de onderliggende logica van de verwerking. De inhoudelijke invulling van de notie 'nuttige informatie over de onderliggende logica' wordt in de rechtsleer op verschillende wijzen geïnterpreteerd, vermits de AVG de vraag naar welk type en soort informatie 'nuttige' informatie constitueert, onbeantwoord laat.[259]

Deze onduidelijkheid resulteerde in een fel bediscussieerd onderwerp in de academische literatuur waarover tot op heden nog geen eensgezindheid lijkt te bestaan, wanneer geautomatiseerde besluitvorming, zoals gedefinieerd in artikel 22, lid 1 AVG wordt toegepast.[260]

---

[257] *Ibid.,* 81.
[258] *Ibid.*, 75.
[259] B. CUSTERS en A. HEIJNE, "The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice", *Computer Law & Security Review* 2022, (1) 5.
[260] I. KOIVISTO, *Thinking Inside the Box: The Promise and Boundaries of Transparency in Automated Decision-Making*, Italië, European University Institute, 2020, 16.

De vraag of een zogenaamd 'recht op uitleg' ('*right to an explanation*') bestaat onder de AVG, afgeleid uit artikel 22 juncto overweging 71 AVG, alsook het gepolariseerde debat daaromtrent, is grotendeels te wijten aan de vage formulering van de transparantieverplichting om ten aanzien van betrokkenen 'nuttige informatie over de onderliggende logica' te verstrekken.[261] Transparantie en 'nuttige informatie' zouden het algemene uitgangspunt van de AVG moeten zijn, maar door dergelijke vage formuleringen, creëert de AVG onvermijdelijk rechtsonzekerheid, die in het bijzonder problematisch is wanneer het gaat om complexe geautomatiseerde besluitvormingsprocessen.[262]

121. De eerste strekking in de rechtsleer verdedigt een eerder functionele benadering en beargumenteert dat informatie slechts 'nuttig' kan zijn indien de informatie de betrokkene in staat stelt de gegenereerde specifieke output te betwisten en aan te vechten, zoals bepaald in artikel 22, lid 3 AVG.[263] Dergelijke interpretatie bevestigt de algemene doelstelling van de AVG dat de versterking van gegevensbescherming als fundamenteel recht beoogt.[264]

In deze strekking refereert 'nuttige' informatie naar een precieze toelichting over de wijze waarop het algoritme tot een specifieke output heeft geleid die de betrokkene in staat stelt te bepalen in welke mate een bepaalde input determinerend was voor de output, dan wel de output heeft beïnvloed.[265] De zinsnede in overweging 71 dat het recht stipuleert om uitleg te krijgen over het genomen besluit lijkt deze strekking te bevestigen.

Echter, de technische natuur van op machinaal lerende gebaseerde AI-systemen, bemoeilijkt het voor verwerkingsverantwoordelijken om ten aanzien van betrokkenen 'nuttige' informatie te verstrekken over de achterliggende logica die hen moet toelaten te begrijpen hoe een AI-systeem beslissingen neemt. Immers, het kwantitatieve besluitvormingsproces van veel AI-systemen wordt gekenmerkt door dynamische ontwikkeling (zelflerend karakter) en ondoorzichtige elementen (*black box*), waardoor het inherent verschilt van de menselijke besluitvormingsprocessen die meestal gebaseerd zijn op een causale en theoretische redenering.[266]

---

[261] B. CASEY, A. FARHANGI en R. VOGL, "Rethinking Explainable Machines: The GDPR's Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise", *Berkely Technology Law Journal* 2019, (145) 158.
[262] I. KOIVISTO, *Thinking Inside the Box: The Promise and Boundaries of Transparency in Automated Decision-Making*, Italië, European University Institute, 2020, 16.
[263] A. SELBST en J. POWLES, "Meaningful information and the right to an explanation", *International Data Privacy Law* 2017, (233) 235.
[264] *Ibid.*
[265] F. DOSHI-VELEZ, M. KORTZ, R. BUDISH, C. BAVITZ, S. GERSHMAN, D. O'BRIEN, K. SCOTT, S. SHIEBER, J. WALDO, D. WEINBERGER, A. WELLER en A. WOOD, "Accountability of AI Under the Law: The Role of Explanation", *Berkman Center Research Publication* 2017, (1) 4; N. WALLACE en D. CASTRO, "The Impact of the EU's New Data Protection Regulation on AI", *Center for Data Innovation* 2018, (1) 10.
[266] A. KESA en T. KERIKMÄE, "Artificial Intelligence and the GDPR: inevitable Nemeses?", *TalTech Journal of European Studies* 2020, (67) 76; EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR (EDPB-EDPS), *Gezamenlijk advies over het voorstel voor een verordening van*

Hoe meer variabelen een algoritme bevat en hoe complexer de verbanden tussen die variabelen zijn, hoe moeilijker het is voor een mens om te beoordelen hoe het algoritme tot een bepaalde beslissing is gekomen.[267] Wanneer AI-systemen leren en beslissingen nemen, doen ze dit immers zonder rekening te houden met het menselijk begrip.[268]

Sommige auteurs menen eveneens dat, indien de wetgever of een rechter de wet zo zou uitleggen dat verwerkingsverantwoordelijken precies moeten kunnen uitleggen hoe elk individueel specifiek besluit tot stand is gekomen, dit een ernstige belemmering op de werking van AI-systemen zou impliceren, omdat deze vereiste ten koste gaat van de nauwkeurigheid van de werking van het AI-systeem.[269] Dit zou op zijn beurt eveneens de ontwikkeling van AI-systemen belemmeren.

122. Een andere strekking in de rechtsleer beargumenteert daarentegen dat deze transparantieverplichting enkel informatie over de algemene functionaliteit en werking van het AI-systeem beoogt te vatten. 'Nuttige' informatie betekent in deze strekking bijgevolg geen informatie omtrent de individuele omstandigheden van een specifieke output, de factoren die in het specifieke geval in aanmerking werden genomen en hun weging.[270] Volgens deze strekking garanderen deze bepalingen in de AVG enkel algemene informatie over de werking van het algoritme en geen informatie over de wijze waarop een specifiek geautomatiseerd besluit tot stand is gekomen.[271]

Wanneer dergelijke interpretatie wordt gevolgd, rijst de vraag in welke mate de actie van een betrokkene om een bepaalde beslissing betreffende hem/haar aan te vechten (*infra* 64, nr. 150) daadwerkelijk effectief kan zijn.[272] De betrokkene zou immers naast de specifieke beslissing, eveneens de algemene functionaliteit van het algoritme en de trainingdata waarmee het AI-systeem werd gevoed moeten aanvechten, wat diepgaande technische kennis vereist.[273]

---

het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie), 18 juni 2021, nr. 5/2021, https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_nl.pdf, 23.

[267] N. WALLACE en D. CASTRO, "The Impact of the EU's New Data Protection Regulation on AI", *Center for Data Innovation* 2018, (1) 10.

[268] J. BURRELL, "How the machine 'thinks': Understanding opacity in machine learning algorithms", *Big Data & Society* 2016, (1) 10.

[269] N. WALLACE en D. CASTRO, "The Impact of the EU's New Data Protection Regulation on AI", *Center for Data Innovation* 2018, (1) 10.

[270] S. WACHTER, B. MITTELSTADT en L. FLORIDI, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation", *International Data Privacy Law* 2017, (76) 96.

[271] M. VEALE, L. EDWARDS, "Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling", *Computer Law & Security Review* 2018, (398) 399.

[272] A. KESA en T. KERIKMÄE, "Artificial Intelligence and the GDPR: inevitable Nemeses?", *TalTech Journal of European Studies* 2020, (67) 77.

[273] *Ibid.*

123. In haar Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering lijkt het EDPB de tweede strekking te volgen, maar inconsistenties in haar bewoordingen veroorzaken enige verwarring en onduidelijkheid, waardoor de verdeeldheid in de rechtsleer blijft bestaan omtrent het al dan niet bestaan van een '*right to an explanation*'.[274]

In eerste instantie dienen verwerkingsverantwoordelijken – volgens het EDPB – begrijpelijke en volledige, doch voldoende specifieke en nuttige informatie te verstrekken aan de betrokkenen, opdat deze laatsten in staat worden gesteld om te begrijpen hoe het AI-systeem een beslissing heeft gegenereerd.[275] Meer bepaald, vereist het EDPB dat verwerkingsverantwoordelijken eenvoudige manieren moeten vinden om de betrokkenen uit te leggen wat de achterliggende gedachte is of op grond van welke criteria het besluit is genomen, zonder dat verwerkingsverantwoordelijken een toelichting moeten verstrekken over een specifiek besluit.

Verderop in haar Richtsnoeren poneert het EDPB met betrekking tot de invulling van de notie 'nuttige' informatie over de onderliggende logica, dat de verwerkingsverantwoordelijke de betrokkene algemene informatie moet verstrekken (met name over de in het besluitvormingsproces in aanmerking genomen factoren en hun weging) die hem/haar in staat stelt het besluit aan te vechten.[276] De bewoording "algemene informatie" duidt op een inconsistentie met de eerder geponeerde verplichting om "specifieke" informatie te verstrekken.

Een tweede inconsistentie situeert zich op het niveau van de begrijpelijkheid van de informatie, vermits het EDPB stelt dat verwerkingsverantwoordelijken "niet noodzakelijkerwijs" verplicht worden een "complexe uitleg betreffende het gebruikte algoritme, dan wel een uiteenzetting van het volledige algoritme" te verstrekken. Dergelijke bewoording impliceert dat er omstandigheden kunnen zijn volgens het EDPB waarin een betrokkene zeer gedetailleerde informatie kan eisen omtrent het onderliggende algoritme, wat in strijd lijkt te zijn met de kwalitatieve voorwaarden waaraan de informatie/communicatie moet voldoen, alsook met de bescherming van de intellectuele eigendomsrechten.[277] De invulling door het EDPB biedt bijgevolg eveneens geen adequaat antwoord op de vraag welke informatie betrokkenen dienen te krijgen.

---

[274] G. MALGIERI, "Automated decision-making in the EU Member States: The right to an explanation and other "suitable safeguards" in the national legislations", *Computer Law & Security Review 2019*, (1) 5 vs. M. VEALE, L. EDWARDS, "Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling", *Computer Law & Security Review* 2018, (398) 399.
[275] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 29-30.
[276] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 32.
[277] Overw. 63 AVG.

2.3. Informatie omtrent de risico's van de verwerking

124. Met betrekking tot de procesfase, dienen betrokkenen eveneens te worden geïnformeerd over de risico's verbonden aan de gegevensverwerking door AI-systemen, alsook over de maatregelen die worden genomen om deze risico's te reduceren.[278] De verplichting om transparantie te bieden omtrent de risico's van gegevensverwerking door AI-systemen op privacy en gegevensbescherming, wordt onder meer in overweging 39 AVG benadrukt. Deze overweging stipuleert dat natuurlijke personen bewust moeten worden gemaakt van de risico's in verband met de verwerking van persoonsgegevens. Een soortgelijke bepaling is niet terug te vinden in de bindende tekst van de wet.

125. Een *Data Protection Impact Assessment*, ook wel een DPIA genoemd of een gegevensbeschermingseffectenbeoordeling ('GEB') kan een belangrijke bron zijn van informatie omtrent de risico's die verbonden zijn aan de gegevensverwerking door AI-systemen en kan bijgevolg een belangrijk aspect uitmaken van de dimensie verklaarbaarheid.[279] Een DPIA is een instrument om vóór de verwerking van de persoonsgegevens de gegevensbeschermingsrisico's van een gegevensverwerking in kaart te brengen om vervolgens maatregelen te kunnen nemen om deze geïdentificeerde risico's te reduceren. Een DPIA is in het bijzonder verplicht wanneer de voorgenomen verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.[280] Bijgevolg is een DPIA bij het gebruik van AI-systemen veelal verplicht.[281]

126. In een DPIA moeten verwerkingsverantwoordelijken dus onder meer de risico's voor de rechten en vrijheden van natuurlijke personen, alsook de vraag of deze risico's kunnen worden gemitigeerd en welke maatregelen daarvoor worden getroffen, beschrijven. Het documenteren van deze informatie maakt een belangrijk aspect uit van de verklaarbaarheidsdimensie van transparantie.[282] Echter, het publiceren van een DPIA wordt niet door de de AVG verplicht.

---

[278] H. FELZMANN, E. VILLARONGA, C. LUTZ en A. TAMO-LARRIEUX, "Towards Transparency by Design for Artificial Intelligence", *Science and Engineering Ethics* 2020, (3333) 3350.
[279] T. GILS, E. WAUTERS, B. BENICHOU, J. DE BRUYNE en P. VALCKE, "Artificiële Intelligentie en gegevensbescherming: een verkennende gids", *Kenniscentrum Data en Maatschappij*, 2020, https://data-en-maatschappij.ai/publicaties/ai-en-gegevensbescherming-een-verkennende-gids, 57.
[280] Art. 35, lid 1 AVG.
[281] Art. 35 AVG; AUTORITEIT PERSOONSGEGEVENS (AP), *Toezicht op AI & Algortimes*, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezicht_op_ai_en_algoritmes.pdf, 7.
[282] M. KAMINSKI en G. MALGIERI, "Multi-layered Explanations for Algorithmic Impact Assessments in the GDPR", *International Data Privacy Law* 2020, (68) 75.

De verwerkingsverantwoordelijke beslist zelf om de beoordeling al dan niet te publiceren.[283] Dit wordt door de rechtsleer als een leemte beschouwd.[284]

Afdeling 3: Output

3.1. Informatie omtrent de verwachte gevolgen van de verwerking

127. Vervolgens dient de verwerkingsverantwoordelijke – om een behoorlijke en transparante verwerking te waarborgen – de betrokkene te informeren over de verwachte gevolgen van de verwerking voor deze laatste.[285] Dit impliceert dat aan de betrokkene informatie moet worden verstrekt die erop gericht is duidelijkheid te verschaffen over de wijze waarop de geautomatiseerde besluitvorming de betrokkene kan beïnvloeden/welke gevolgen dit voor hem/haar kan hebben.[286] Dergelijke informatie is erop gericht om de betrokkene te informeren over de mogelijke reik- en draagwijdte van het geautomatiseerd besluit.

128. Gelet op het relationele aspect van de dimensie verklaarbaarheid, is het aangewezen echte, tastbare voorbeelden van het soort mogelijke gevolgen aan te reiken.[287] In het kader van een kredietwaardigheidsbeoordeling kunnen de verwachte gevolgen bijvoorbeeld onder meer betrekking hebben op het gebruik van het resultaat van de kredietwaardigheidsbeoordeling voor latere beoordelingen, de periode gedurende dewelke het resultaat van de kredietwaardigheidsbeoordeling geldig blijft en derden die toegang zouden hebben tot het resultaat.[288] Informatie over de verwachte gevolgen moet bijgevolg de reële gevolgen van geautomatiseerde besluiten weergeven, zodat de betrokkenen de gevolgen ervan kunnen beoordelen.[289]

---

[283] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt in de zin van Verordening 2016/679*, 4 april 2017, WP248rev.01, https://ec.europa.eu/newsroom/article29/items/611236, 22.

[284] M. KAMINSKI en G. MALGIERI, "Multi-layered Explanations for Algorithmic Impact Assessments in the GDPR", *International Data Privacy Law* 2020, (68) 75.

[285] Arts. 13, lid 2, f); 14, lid 2, g) en 15, lid 1, h) AVG.

[286] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 31.

[287] T. GILS, E. WAUTERS, B. BENICHOU, J. DE BRUYNE en P. VALCKE, "Artificiële Intelligentie en gegevensbescherming: een verkennende gids", *Kenniscentrum Data en Maatschappij*, 2020, https://data-en-maatschappij.ai/publicaties/ai-en-gegevensbescherming-een-verkennende-gids, 83.

[288] E. BAYAMLIOGLU, "The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation"", *Regulation & Governance* 2021, (1) 10.

[289] *Ibid.*

Hoofdstuk 3: Controle in de AVG

129. In dit hoofdstuk wordt de dimensie controle van betekenisvolle transparantie in de drie fasen beoordeeld. In de drie beschikbare vlakken binnen de controledimensie van het transparantiekader, worden de in de AVG geïdentificeerde controlemechanismen in elke fase van de gegevensverwerking door AI-systemen ingepast.

Afdeling 1: Input

1.1. Gegevensverwerkingsgrondslag: toestemming

130. In de AVG is er een mechanisme ingebouwd dat betrokkenen controle wil bieden over hun persoonsgegevens als input bij de gegevensverwerking door AI-systemen. In het bijzonder gaat het om het mechanisme van de geldige toestemming – een van de zes rechtsgronden voor de verwerking van persoonsgegevens, zoals beschreven in artikel 6 AVG – op grond waarvan betrokkenen verwerkingsverantwoordelijken toestemming kunnen geven om hun persoonsgegevens te verwerken. Dit moet betrokkenen in staat stellen autonoom – op basis van de verstrekte informatie – te beslissen op welke wijze zij de kosten en baten van het verzamelen en de eigenlijke verwerking van hun persoonsgegevens afwegen.

131. De geldige toestemming is gebaseerd op de onderliggende gedachte dat betrokkenen bewuste, rationele en autonome keuzes maken over de verwerking van hun persoonsgegevens.[290] Bijgevolg kan de geldige toestemming als een belangrijk controlemechanisme worden beschouwd, vermits de mogelijkheid tot het verlenen van voorafgaandelijke toestemming met betrekking tot de verwerking van persoonsgegevens door AI-systemen, bij uitstek de menselijke autonomie bevordert en respecteert.[291] In dit opzicht is toestemming een essentiële garantie van individuele controle over persoonsgegevens als input.[292]

132. Toestemming wordt in artikel 4, lid 11 AVG omschreven als "elke vrije, specifieke, op informatie berustende en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt".

---

[290] B. SCHERMER, B. CUSTERS en S. VAN DER HOF, "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection", *Ethics Inf Technol* 2014, (171) 171.
[291] S. BAROCAS en H. NISSENBAUM, "Big Data's End Run around Anonymity and Consent" in J. LANE, V. STODDEN, S. BENDER en H. NISSENBAUM (eds.), *Privacy, Big Data, and the Public Good. Frameworks for Engagement*, Cambridge, Cambridge University Press, 2014, (44) 57.
[292] E. KOSTA en C. CUIJPERS, "The Draft Data Protection Regulation and the Development of Data Processing Applications", *IFIP Advances in Information and Communication Technology* 2014, (12) 17.

133. In het kader van deze masterproef wordt de vereiste van een geïnformeerde toestemming onder de loep genomen. Deze vereiste houdt in dat – opdat de toestemming geldig zou zijn – de verwerkingsverantwoordelijke voorafgaandelijk aan de verwerkingsactiviteit waarvoor toestemming nodig is, de betrokkene informeert omtrent zaken die van essentieel belang zijn om een geïnformeerde beslissing te kunnen nemen omtrent het al dan niet aanvaarden van de voorgenomen verwerking.[293]

134. Echter, in de rechtsleer groeit het scepticisme over de efficiëntie van toestemming als rechtsgrond voor een rechtmatige verwerking.[294] Er wordt met name beargumenteerd dat de vereiste van geïnformeerde toestemming moeilijk verenigbaar is met de realiteit van AI, aangezien het impliceert dat de betrokkene alle relevante aspecten van de voorgenomen verwerking begrijpt. In dit opzicht lijkt geïnformeerde toestemming onmogelijk omdat ze uitgaat van de veronderstelling dat betrokkenen datgene waartoe ze hun toestemming verlenen, weten én begrijpen. De *black box*-problematiek, het zelflerend karakter en de technologische complexiteit van de verwerking van persoonsgegevens door AI-systemen – gebaseerd op *machine learning* methoden – verzwakken het vermogen van betrokkenen om geldige toestemming te geven.[295]

135. Ten slotte moet worden opgemerkt dat toestemming slechts een van de zes grondslagen vormt voor de verwerking van persoonsgegevens. Dit controlemechanisme is bijgevolg niet toepasbaar in alle gevallen van verwerking van persoonsgegevens door AI-systemen.

---

[293] EUROPEAN DATA PROTECTION BOARD (EDPB), *Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679,* 4 mei 2020, versie 1.1, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_nl.pdf, 17.

[294] N. MARNAU, "Stakeholders' Consultation. Comments on the "Draft Ethics Guidelines for Trustworthy AI" by the High-Level Expert Group on Artificial Intelligence", *Helmholtz Center For Information Security* 2019, (1) 3.

[295] J. VAN HOBOKEN, "The Privacy Disconnect" in R. JØRGENSEN (ed.), *Human Rights in the Age of Platforms*, Cambridge, The MIT Press, 2019, (255) 266.

Afdeling 2: Proces

2.1. Verbod om te worden onderworpen aan uitsluitend geautomatiseerde besluitvorming

136. Krachtens artikel 22, lid 1 AVG heeft de betrokkene het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft. In wezen gaat het niet zozeer om een recht dat aan de betrokkene wordt toegekend, maar wel om een principieel algemeen verbod dat aan verwerkingsverantwoordelijken wordt opgelegd betreffende het nemen van besluiten waaraan rechtsgevolgen verbonden zijn of dat een individu in aanmerkelijke mate treft dat uitsluitend op geautomatiseerde verwerking is gebaseerd.[296] Dergelijk besluit kan bestaan uit een automatische weigering van een online ingediende kredietaanvraag of van verwerking van sollicitaties via het internet zonder menselijke tussenkomst.[297]

137. Dit verbod is van toepassing, ongeacht of de betrokkene al dan niet actie onderneemt met betrekking tot de verwerking van zijn/haar persoonsgegevens.[298] Verwerkingsverantwoordelijken hebben bijgevolg een actieve onthoudingsverplichting op dit punt. De formulering van artikel 22 AVG onder de vorm van een verbodsbepaling versterkt de positie van betrokkenen, aangezien verwerkingsverantwoordelijken in beginsel verplicht zijn om betrokkenen niet te onderwerpen aan uitsluitend geautomatiseerde besluitvorming. Dit versterkt de idee dat betrokkenen controle hebben over hun persoonsgegevens, aangezien personen automatisch worden beschermd tegen de mogelijke negatieve gevolgen die uitsluitend geautomatiseerde verwerking kan hebben.[299]

138. Niettemin kunnen op dit beginsel uitzonderingen worden voorzien in welk kader de AVG bepaalde waarborgen (artikel 22, lid 3 AVG) en specifieke transparantieverplichtingen (artikelen 13-15 AVG) voorziet ten aanzien van de betrokkene.

---

[296] D. DE BOT, *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Mechelen, Wolters Kluwer, 2020, 673; I. MENDOZA en L. BYGRAVE, "The Right Not te be Subject to Automated Decisions Based on Profiling" in T. SYNODINOU, P. JOUGLEUX, C. MARKOU en T. PRASTITOU (eds.), *EU Internet Law. Regulation and Enforcement*, Cham, Springer, 2017, (77) 87.

[297] Overw. 71 AVG

[298] P. WOLTERS, "De rechten van de betrokkene onder de AVG", *Tijdschrift voor Consumentenrecht en handelspraktijken* 2018, (130) 136.

[299] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 23.

Het verbod ex artikel 22, lid 1 AVG is echter alleen van toepassing in specifieke omstandigheden, met name wanneer het gaat om een besluit dat 1) gebaseerd is op uitsluitend geautomatiseerde verwerking of profilering en 2) rechtsgevolgen voor iemand heeft of de persoon anderszins in aanmerkelijke mate treft.[300] Geautomatiseerde besluiten die niet voldoen aan de definitie van artikel 22, lid 1 AVG, worden bijgevolg niet gevat door deze bepaling.[301]

139. In de rechtsleer wordt door een aantal auteurs kritiek geuit op het – volgens hen – gelimiteerd en vaag toepassingsgebied en de (bijgevolg volgens hen) beperkte reikwijdte van artikel 22, lid 1 AVG, alsook de hiermee geassocieerde waarborgen en specifieke transparantievereisten.[302] Deze auteurs zijn van mening dat artikel 22 AVG de betrokkene op deze manier een vals gevoel van veiligheid geeft.

Vooreerst vereist artikel 22, lid 1 AVG dat het besluit uitsluitend geautomatiseerd werd gegenereerd. Deze formulering impliceert dat er geen sprake mag zijn van enige menselijke tussenkomst tijdens het besluitvormingsproces. Aangezien de mate van menselijke tussenkomst niet werd verduidelijkt door de Europese wetgever, werd dergelijke restrictieve interpretatie door veel verwerkingsverantwoordelijken gehandhaafd om te ontsnappen aan de toepassing van artikel 22 AVG.[303] Immers, door de toevoeging van slechts een minimale, niet substantiële vorm van menselijke tussenkomst in het besluitvormingsproces, zouden verwerkingsverantwoordelijken relatief gemakkelijk de – in het kader van artikel 22 AVG – gestelde waarborgen en specifieke transparantieverplichtingen kunnen omzeilen.[304] Dit zou de gewenste rechtsbescherming voor betrokkenen sterk reduceren.

De interpretatie van het EDPB over de notie 'uitsluitend geautomatiseerd besluit' in de zin van artikel 22, lid 1 AVG biedt betrokkenen een sterkere rechtsbeschermende component, aangezien de notie ruimer wordt opgevat dan zoals de formulering in eerste instantie doet vermoeden. Vooreerst merkt het EDPB op dat een menselijke tussenpersoon meer dan een louter symbolische rol moet vervullen om de verplichtingen ex artikel 22, lid 1 AVG te omzeilen.[305]

---

[300] S. BARROS VALE en G. ZANFIR-FORTUNA, "Automated Decision-Making Under the GDPR: Practical Cases form Courts and Data Protection Authorities", *Future of Privacy Forum* 2022, (1) 8.
[301] *Ibid.*, (1) 28.
[302] G. MALGIERI en G. COMANDÉ, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law* 2017, (1) 6; A. SELBST en J. POWLES, "Meaningful information and the right to an explanation", *International Data Privacy Law* 2017, (233) 235.
[303] E. BAYAMLIOGLU, "The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation"", *Regulation & Governance* 2021, (1058) 1061.
[304] B. GREEN en A. KAK, "The False Comfort of Human Oversight as an Antidote to A.I. Harm", *Slate* 2021, (1) 3; G. MALGIERI en G. COMANDÉ, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law* 2017, (1) 6.
[305] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 24.

Dit impliceert dat het routinematig toepassen van automatisch gegenereerde besluiten, zonder dat een menselijke tussenpersoon hierop enige invloed heeft of kan uitoefenen, nog steeds een uitsluitend op geautomatiseerde verwerking gebaseerd besluit is.[306] Pas wanneer de menselijke tussenpersoon substantieel het gegenereerde besluit kan veranderen, is er geen sprake meer van een 'uitsluitend geautomatiseerd besluit'.

De interpretatie van deze eerste voorwaarde is ook een van de meest omstreden kwesties in zaken voor rechtbanken van lidstaten van de EU en een van de belangrijkste aandachtspunten in besluiten van gegevensbeschermingsautoriteiten.[307] Uit een analyse van de rechtspraak van rechtbanken in de hele EU blijkt dat een vaak beperkte mate van menselijke tussenkomst voldoende is om de toepassing van artikel 22 AVG terzijde te schuiven.[308]

140. Vervolgens moet het besluit rechtsgevolgen creëren voor de betrokkene of hem/haar anderszins in aanmerkelijke mate treffen. Volgens het EDPB heeft een besluit rechtsgevolgen voor een persoon wanneer het besluit zijn/haar rechtspositie of rechten krachtens de wet of uit hoofde van een overeenkomst aantast.[309] Voorbeelden die in dit kader worden gegeven, zijn geautomatiseerde besluiten over onder meer het beëindigen van een overeenkomst, de weigering van een sociale uitkering of de weigering van de toekenning van een nationaliteit.

Vaststellen of een besluit de betrokkene anderszins in aanmerkelijke mate treft, is moeilijker aangezien dit criterium niet eenvoudig te meten is. Om vast te stellen of een besluit de betrokkene anderszins in aanmerkelijke mate treft, moet volgens het EDPB het besluit het potentieel hebben om de omstandigheden, het gedrag of de keuzen van de betrokken personen in aanmerkelijke mate te treffen, een langdurig of blijvend effect op de betrokkenen te hebben of (in het uiterste geval) tot uitsluiting of discriminatie van personen te leiden.[310]

---

[306] N. JAK en S. BASTIAANS, "De betekenis van de AVG voor geautomatiseerde besluitvorming door de overheid. Een black box voor een black box", *Nederlands Juristenblad* 2018, (3018) 3020; GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 24.
[307] S. BARROS VALE en G. ZANFIR-FORTUNA, "Automated Decision-Making Under the GDPR: Practical Cases form Courts and Data Protection Authorities", *Future of Privacy Forum* 2022, (1) 8.
[308] *Ibid.,* (1) 29-34.
[309] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 25.
[310] *Ibid.,* 26.

Het EDPB erkent de moeilijkheid om de precieze grens en reikwijdte van de notie 'in aanmerkelijke mate' te bepalen, aangezien de gevolgen van een geautomatiseerde beslissing zeer subjectief kunnen worden opgevat.[311] Het toepassingsgebied van artikel 22 AVG blijft bijgevolg vaag op dit punt.

2.2. Passende beschermingsmaatregelen

141. Op het verbod bestaan drie mogelijke uitzonderingsgronden op basis waarvan uitsluitend geautomatiseerde individuele besluiten mogelijk zijn. Concreet zijn uitsluitend geautomatiseerde individuele besluiten mogelijk indien ze 1) noodzakelijk zijn voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke, 2) toegestaan zijn bij wetgeving, mits passende maatregelen of 3) berusten op de uitdrukkelijke toestemming van de betrokkene.[312]

142. In elk van deze gevallen dient, hetzij de verwerkingsverantwoordelijke, hetzij de wetgever, passende maatregelen te voorzien ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkenen.[313] Dit betreft – voor wat betreft de eerste en derde uitzondering – ten minste het recht op menselijke tussenkomst, het recht van de betrokkene om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten.[314]

De wijze waarop de drie beschermingsmaatregelen/rechten uit artikel 22, lid 3 AVG zich ten opzichte van elkaar verhouden, alsook de praktische implementatie ervan, is onduidelijk.[315] Daarenboven zijn de in artikel 22, lid 3 AVG opgesomde maatregelen geen exhaustieve voorbeelden van passende maatregelen, maar een lijst van minimumvereisten. Bijgevolg rijst de vraag op welke andere rechten betrokkenen zich in dit verband kunnen beroepen.[316]

143. In dit kader worden enkel het recht op menselijke tussenkomst en het recht om het besluit aan te vechten besproken, gezien dit de twee belangrijkste controlemechanismen uitmaken.

---

[311] G. MALGIERI en G. COMANDÉ, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law* 2017, (1) 6; GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 26.
[312] Art. 22, lid 2 AVG.
[313] Art. 22, lid 2 b) AVG en lid 3 AVG.
[314] Art. 22, lid 3 AVG.
[315] E. BAYAMLIOGLU, "The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation"", *Regulation & Governance* 2021, (1058) 1062; E. KAMINSKI en J. URBAN, "The right to contest AI", Columbia Law Review 2021, (1957) (1979).
[316] I. MENDOZA en L. BYGRAVE, "The Right Not te be Subject to Automated Decisions Baded on Profiling" in T. SYNODINOU, P. JOUGLEUX, C. MARKOU en T. PRASTITOU (eds.), *EU Internet Law. Regulation and Enforcement*, Cham, Springer, 2017, (77) 92.

2.2.1. Recht op menselijke tussenkomst

144. Indien beroep kan worden gedaan op een van de uitzonderingsgronden in artikel 22, lid 2 AVG, voorziet artikel 22, lid 3 AVG in eerste instantie een recht op menselijke tussenkomst als minimum te treffen beschermingsmaatregel. Menselijke tussenkomst vindt pas plaats nadat een output werd gegenereerd. [317] Dit is ook logisch, aangezien een verwerking maar onder het toepassingsgebied van artikel 22, lid 1 AVG zal ressorteren wanneer substantiële/zinvolle menselijke tussenkomst afwezig blijft in het besluitvormingsproces.

145. Het recht op menselijke tussenkomst wordt in de AVG voorgesteld als een middel om de rechten, vrijheden en gerechtvaardigde belangen van betrokkenen te beschermen wanneer de verwerking uitsluitend geautomatiseerd verloopt. In dit opzicht kan het recht op menselijke tussenkomst worden beschouwd als een middel om betrokkenen tegen de risico's, verbonden aan individuele geautomatiseerde besluitvorming, te beschermen door hen de mogelijkheid te bieden om het geautomatiseerd besluit te laten herbeoordelen.[318]

Deze vorm van controle benadrukt de noodzaak van menselijke autonomie en is bijgevolg gericht op de doelstelling van veiligheid en precisie. Immers, het recht op menselijke tussenkomst houdt het recht in voor de betrokkene om een herbeoordeling/heroverweging te verzoeken van besluiten die zijn legitieme belangen en rechten onnodig beperken, en indien nodig het besluit kan worden aangepast.[319]

146. Opdat betrokkenen dit recht zouden kunnen uitoefenen, moeten ze beschikken over informatie over de verwerking van de persoonsgegevens door het AI-systeem die hen toelaat het verzoek tot menselijke tussenkomst te rechtvaardigen. In dit kader zijn de artikelen 13-15 AVG die werden opgenomen in de dimensie verklaarbaarheid (over de drie fasen heen) van het transparantiekader, erop gericht om het recht op menselijke tussenkomst te faciliteren.[320]

147. Hoewel het recht op menselijke tussenkomst, zoals gereguleerd door de AVG, een wezenlijk controle mogelijk maakt voor betrokkenen, kunnen een aantal bedenkingen bij dit recht worden geformuleerd.

---

[317] M. ALMADA, "Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems", *Forthcoming, 17th International Conference on Artificial Intelligence and Law* 2018, (1) 11.
[318] P. WOLTERS, "De rechten van de betrokkene onder de AVG", *Tijdschrift voor Consumentenrecht en handelspraktijken* 2018, (130) 137.
[319] M. ALMADA, "Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems", *Forthcoming, 17th International Conference on Artificial Intelligence and Law* 2018, (1) 2 en 5.
[320] *Ibid.,* (1) 6.

Een eerste nadeel dat in de rechtsleer wordt geïdentificeerd met betrekking tot het recht op menselijke tussenkomst, is het gegeven dat het recht op menselijke tussenkomst pas plaatsvindt nadat een besluit werd gegenereerd en de gevolgen al merkbaar zijn voor de betrokkene.[321] Deze gevolgen kunnen – afhankelijk van de situatie – al dan niet eenvoudig worden teruggedraaid. Zelfs wanneer de gevolgen makkelijk kunnen worden teruggedraaid, kan het geautomatiseerd besluit al een blijvende impact tot stand hebben gebracht voor de betrokkene.[322]

148. Vervolgens toont onderzoek eveneens aan dat mensen over het algemeen slecht presteren bij het in heroverweging nemen van geautomatiseerde besluiten.[323] Zo kunnen deze menselijke tussenpersonen – net als AI-systemen – vertekeningen (*bias*) en fouten in hun besluitvormingsproces introduceren, waardoor betrokkenen zich misschien zelfs in een nog slechtere positie bevinden dan ze waren onder het geautomatiseerd besluit.[324] Indien in een bepaald geval de kans groot is dat de menselijke tussenpersonen niet neutraal (*biased*) zullen optreden, zou de betrokkene er waarschijnlijk geen baat bij hebben zijn recht op menselijke tussenkomst uit te oefenen.[325]

149. Ten slotte kan eveneens de vraag rijzen of de menselijke tussenpersoon het geautomatiseerd besluit daadwerkelijk heroverweegt en niet blindelings overneemt.[326] Immers, mensen kunnen de mogelijke neiging hebben om te veel te vertrouwen op de output van een AI-systeem waardoor ze onbewust geneigd zijn om het geautomatiseerde besluit over te nemen (*automation bias*). Om dit risico zoveel als mogelijk te reduceren, kunnen evenwel waarborgen worden ingebouwd. Zo kunnen bijvoorbeeld meerdere tussenpersonen hetzelfde besluit herzien, waarna ze hun resultaten vergelijken. Deze maatregelen zijn echter afhankelijk van de middelen waarover de verwerkingsverantwoordelijke beschikt.[327] Dergelijke kwaliteitswaarborgen ontbreken in de bindende tekst van de wet.

---

[321] G. SMELTING, *Geautomatiseerde besluitvorming: van human in-the-loop naar human out-the-loop*, onuitg. masterproef Rechten UvA, 2020, https://scripties.uba.uva.nl/download?fid=c2025980, 30.
[322] *Ibid.*
[323] R. KOULU, "Proceduralizing control and discretion: Human oversight in artificial intelligence policy", *Maastricht Journal of European and Comparative Law* 2020, (720) 219.
[324] M. ALMADA, "Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems", *Forthcoming, 17th International Conference on Artificial Intelligence and Law* 2018, (1) 8.
[325] *Ibid.*
[326] G. SMELTING, *Geautomatiseerde besluitvorming: van human in-the-loop naar human out-the-loop*, onuitg. masterproef Rechten UvA, 2020, https://scripties.uba.uva.nl/download?fid=c2025980, 31.
[327] *Ibid.*

2.2.2. Recht om het uitsluitend geautomatiseerd individueel besluit aan te vechten

150. In dit onderdeel wordt een essentieel aspect van de controledimensie, met name het recht om geautomatiseerde besluiten aan te vechten ex artikel 22, lid 3 AVG, nader bekeken. Artikel 22 AVG betrekking heeft op een specifiek resultaat, namelijk een volledig geautomatiseerd besluit waaraan voor de betrokkene rechtsgevolgen zijn verbonden of die hem/haar anderszins in aanmerkelijke mate treft.[328]

151. Deze vorm van controle is gericht op het bereiken van procedurele rechtvaardigheid en eerlijkheid. De dimensie verklaarbaarheid, over de drie horizontale fasen heen, is erop gericht de aanvechtbaarheid van geautomatiseerde besluiten te faciliteren, dan wel te verbeteren.[329] De betrokkene kan immers alleen een besluit aanvechten als hij bewust is van het bestaan van geautomatiseerde besluitvorming, volledig begrijpt hoe en op grond waarvan dat besluit tot stand is gekomen.[330]

152. Dit recht wordt beschouwd als de "ruggengraat" van de beschermingsmaatregelen waarin de AVG voorziet.[331] Echter, hoewel het recht om uitsluitend geautomatiseerde besluiten aan te vechten wordt beschouwd als een belangrijk aspect van de controledimensie in de AVG, wordt dit recht noch in de bindende wettekst van de AVG, noch in de overwegingen ervan nader omschreven. Ook in de Richtsnoeren van het EDPB wordt hieromtrent weinig aandacht besteed.

153. Een van de kritieken die vanuit de rechtsleer worden geuit met betrekking tot het recht om uitsluitend geautomatiseerde besluiten aan te vechten, is het gegeven dat de betrokkene afhankelijk is van de inspanningen van de verwerkingsverantwoordelijke om aanspraak te kunnen maken op deze beschermingsmaatregel.[332] Wanneer een verwerkingsverantwoordelijke zich niet houdt aan zijn verplichting om de betrokkene te informeren, omdat hij bijvoorbeeld denkt dat de voorgenomen verwerking niet onder artikel 22, lid 1 AVG ressorteert, dan weet de betrokkene niet eens dat hij wordt onderworpen aan geautomatiseerde besluitvorming.[333] Deze bemerking geldt eveneens voor wat betreft het recht op menselijke tussenkomst.

---

[328] E. BAYAMLIOGLU, "The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation"", *Regulation & Governance* 2021, (1058) 1060.
[329] GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 26.
[330] A. ROIG, "Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR)", *European Journal of Law and Technology* 2017, (1) 6.
[331] M. KAMINSKI en J. URBAN, "The right to contest AI", *Columbia Law Review* 2021, (1957) 1979.
[332] G. SMELTING, *Geautomatiseerde besluitvorming: van human in-the-loop naar human out-the-loop*, onuitg. masterproef Rechten UvA, 2020, https://scripties.uba.uva.nl/download?fid=c2025980, 31.
[333] *Ibid.*

Afdeling 3: Output

154. In de AVG kon geen controlemechanisme worden geïdentificeerd die de betrokkene de mogelijkheid biedt om controle over zijn persoonsgegevens te behouden in de outputfase van de gegevensverwerking. Controle over persoonsgegevens in de outputfase van de gegevensverwerking gaat specifiek over de vraag of de betrokkene enige instrumenten in handen heeft om zich te verzetten in de outputfase (dus nadat een output werd gegenereerd) tegen de specifieke gevolgen die verbonden zijn aan de gegenereerde output. De controlemechanismen die controle toelaten over de persoonsgegevens moeten worden aangewend in de inputfase en procesfase van de gegevensverwerking.

Hoofdstuk 4: Conclusie

155. Op grond van de voorgaande paragrafen, wordt in deze conclusie een antwoord geformuleerd op de eerste deelvraag, met name: "zijn er grenzen aan de definiëring van de transparantievereisten in de AVG bij de toepassing van AI-systemen?".

156. De AVG is erop gericht de positie van de betrokkene in het gegevensbeschermingsrecht maximaal te versterken. Deze doelstelling komt onder meer tot uiting in de wezenlijke transparantievereisten in de verklaarbaarheidsdimensie die de controledimensie dienen te versterken. Echter, de keuze van de Europese wetgever om de AVG als een technologisch neutraal wettelijk kader te introduceren, lijkt op grenzen te stuiten wanneer AI-systemen persoonsgegevens verwerken.

157. Vooreerst zijn de transparantievereisten omtrent het proces van conversie in de verklaarbaarheidsdimensie zeer vaag en open geformuleerd, waardoor rechtsonzekerheid bestaat omtrent de precieze invulling van deze transparantievereisten. Daarenboven creëren de verschillende invullingen van deze vereisten eveneens problemen inzake de praktische toepassing ervan in AI-context.[334] Immers, door het niet erkennen van de specifieke en unieke kenmerken van AI-systemen, zoals haar *black box*-karakter en de mogelijkheid tot *self learning*, is de AVG niet volledig aangepast aan deze kenmerken, waardoor de toepassing ervan tot problemen leidt en onvolmaaktheden vertoont.[335]

158. Een specifieke technologie vereist duidelijke en precieze regels die, door rekening te houden met de typische kenmerken van AI-systemen, een regime creëren dat de volledige eerbiediging van de door het wetgevingsinstrument geponeerde rechten garandeert (*i.e.* controledimensie).[336]

---

[334] J. DE BRUYNE en T. GILS, "Wat brengt de toekomst: de regulering van artificiële intelligentie" in P. VAN EECKE (ed.), *Recht & Elektronische handel*, Mortsel, Intersentia, 2021, (581) 600.
[335] J. DE BRUYNE, "Artificiële Intelligentie in 2021: veel wetgevende en beleidsinitiatieven, maar meer focus nodig op digitale geletterdheid, *De Juristenkrant* 2021, (8) 8.
[336] A. KESA en T. KERIKMÄE, "Artificial Intelligence and the GDPR: inevitable Nemeses?", *TalTech Journal of European Studies* 2020, (67) 71.

Gezien de transparantieverplichtingen wel degelijk als wezenlijk worden beschouwd, impliceren de bestaande transparantieverplichtingen geen onverenigbaarheid bij de toepassing van AI-systemen inzake gegevensverwerking, maar vereisen ze bijkomende verduidelijking en concretisering. Dit, om enerzijds de nodige rechtszekerheid te creëren voor alle actoren, en anderzijds de praktische toepassing van de vereisten te vergemakkelijken .[337]

Dit is belangrijk, gezien de transparantieverplichtingen in de verklaarbaarheidsdimensie implicaties hebben voor de controledimensie. Zo kan de controledimensie slechts doeltreffend zijn als de informatieverplichtingen in de verklaarbaarheidsdimensie optimaal (geformuleerd) zijn. Zoals hierboven uiteengezet, lijkt dit niet steeds het geval te zijn.

159. Een laatste beperking van de AVG betreft het gegeven dat de betrokkene, zowel in de verklaarbaarheidsdimensie als in de controledimensie, in hoge mate afhankelijk is van de inspanningen die de verwerkingsverantwoordelijke wil en kan leveren. In de verklaarbaarheidsdimensie komt dit in het bijzonder tot uiting met betrekking tot de inputfase waarin *Data Driven Companies* gegevens verzamelen en met betrekking tot de procesfase. In de controledimensie heeft deze problematiek voornamelijk betrekking op het recht op menselijke tussenkomst.

[337] J. DE BRUYNE en T. GILS, "Wat brengt de toekomst: de regulering van artificiële intelligentie" in P. VAN EECKE (ed.), *Recht & Elektronische handel*, Mortsel, Intersentia, 2021, (581) 606.

DEEL V. TOEPASSING VAN HET TRANSPARANTIEKADER OP HET VOORSTEL

Hoofdstuk 1: Verklaarbaarheid in het Voorstel

160. In dit hoofdstuk wordt de verklaarbaarheid met betrekking tot de drie fasen in het Voorstel beoordeeld. Bij de invulling van de drie beschikbare vlakken binnen de dimensie verklaarbaarheid van het ontwikkelde transparantiekader, wordt de – in de artikelen 10 tot en met 14 en 52 van het Voorstel – relevante informatie in verband met de verwerking van (persoons)gegevens door AI-systemen ingepast (zie bijlage B). In tegenstelling tot de AVG, is er in het Voorstel geen sprake van een overkoepelende transparantieverplichting die de modaliteiten van transparantie reguleert. Bijgevolg wordt weinig tot geen aandacht besteed in het Voorstel aan het relationele aspect van de dimensie verklaarbaarheid.

161. Deel V poogt in het bijzonder een antwoord te formuleren op de tweede deelvraag die luidt als volgt: "waarin verschilt de invulling van de transparantievereisten in de AVG ten opzichte van de transparantievereisten in het Voorstel?".

Afdeling 1: Input

1.1. Informatie omtrent de dataverzameling en kwaliteit van de aangeleverde data (implementatiefase van het AI-systeem)

162. De transparantievereisten inzake dataverzameling (*i.e.* informatie omtrent hoe en welke data worden verzameld) in de implementatiefase van het AI-systeem, zoals gestipuleerd in de AVG, vinden geen expliciete weerklank in de tekst van het Voorstel. Deze informatie ontbreekt zowel voor AI-systemen met een beperkt risico, als voor AI-systemen met een hoog risico. Dit is het gevolg van het gegeven dat het Voorstel in se productregulering is.[338]

163. Informatie omtrent de kwaliteit van de aangeleverde data in de implementatiefase van het AI-systeem wordt eveneens niet door het Voorstel gereguleerd. Artikel 29, lid 3 van het Voorstel bepaalt enkel dat de gebruiker ervoor zorgt dat – voor zover hij controle heeft over de inputdata – de inputdata relevant zijn voor het beoogde doel van het AI-systeem met een hoog risico.

[338] AUTORITEIT PERSOONSGEGEVENS (AP), *AP Inzet Artificial Iintelligence Act,* 15 maart 2022, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_inzet_ai_act.pdf, 4.

1.2. Informatie omtrent de dataverzameling en kwaliteit van de aangeleverde datasets (ontwikkelingsfase van het AI-systeem)

164. Aanbieders van AI-systemen met een hoog risico moeten informatie omtrent de gebruikte datareeksen waarmee het systeem werd gevoed – voor de ontwikkeling ervan – opnemen in de technische documentatie. Zo moet onder meer informatie omtrent de herkomst en de belangrijkste kenmerken van deze datareeksen daarin worden opgenomen.[339]

165. Met betrekking tot de kwaliteit van de aangeleverde datasets voor het trainen, valideren en testen, bepalen de leden 3 en 4 van artikel 10 van het Voorstel de kwaliteitscriteria waaraan deze datasets moeten voldoen.[340] Deze kwaliteitscriteria gelden specifiek voor AI-systemen met een hoog risico die gebruik maken van technieken waarbij hun modellen met data getraind worden (*i.e. machine learning* modellen). Deze kwaliteitscriteria ontbreken voor AI-systemen met een beperkt risico.

Vooreerst dienen de datareeksen voor training, validatie en tests relevant, representatief, foutenvrij en volledig te zijn.[341] De vereisten van "volledig" en "foutenvrij" stuiten in de rechtsleer op kritiek, gezien de praktische onhaalbaarheid ervan in de realiteit.[342] Bovendien rijst de vraag wie de kwaliteit van de data zal beoordelen, alsook aan de hand van welke criteria. De verplichtingen laten bijgevolg eveneens ruimte voor ambiguïteit.

Vervolgens dienen de datareeksen bovendien de passende statistische kenmerken te hebben met betrekking tot de personen waarvoor de AI-systemen met een hoog risico moeten worden gebruikt.[343] Ten slotte wordt ook het representativiteitscriterium ingeschreven en gepreciseerd in artikel 10, lid 4 van het Voorstel dat bepaalt dat de datareeksen rekening moeten houden met de eigenschappen of elementen die specifiek zijn voor een bepaalde geografische, functionele of gedragsomgeving waarin het AI-systeem moet worden gebruikt.

---

[339] Bijlage IV, lid 2, g) Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[340] Art. 10, lid 1 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[341] Art. 10, lid 3 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[342] L. FLORIDI, "The European Legislation on AI: A Brief Analysis of Its Philosophical Approach" in J. MÖKANDER en M. ZIOSI (eds.), *The 2021 Yearbook of the Digital Ethics Lab*, Cham, Springer, 2022, (1) 6; N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI en K. YEUNG, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", *SSRN* 2021, (1) 34.
[343] Art. 10, lid 3 Voorstel voor een Verordening betreffende Artificiële Intelligentie.

166. De kwaliteitsvereisten met betrekking tot de datasets ex artikel 10 van het Voorstel, moeten samen gelezen worden met de informatie die verplicht moet worden opgenomen in de technische documentatie ex artikel 11 van het Voorstel. Zo moet onder meer informatie worden opgenomen omtrent de datavereisten en de methoden voor dataopschoning.[344]

167. De verschillende informatie-elementen die de technische documentatie ten minste moet bevatten, moeten ervoor zorgen dat het systeem zodanig 'transparant' is dat de aanbieder in eerste instantie en, indien nodig, de toezichthoudende autoriteiten na het in de handel brengen van het AI-systeem, de conformiteit ervan kunnen beoordelen.

Het lijkt het nuttig de informatie omtrent de gebruikte trainings-, validerings- en testgegevens (en hun kwaliteit) op te nemen in de EU-databank (*infra* 78, nr. 195). Immers, de werking (proces) van AI-systemen, alsook de mogelijke vertekeningen ervan, worden onder meer bepaald door de aangeleverde data(sets) en hun kwaliteit.[345] Door transparantie hieromtrent te bieden, wordt het mogelijk de redenen te identificeren waarom het AI-systeem foutieve beslissingen heeft gegenereerd en de output van het systeem te betwisten. Het Voorstel voorziet echter niet in deze mogelijkheid.

168. Wanneer aanbieders van AI-systemen met een hoog risico als verwerkingsverantwoordelijken kunnen worden beschouwd, kan de informatie met betrekking tot de gebruikte trainings-, validerings- en testgegevens die in de technische documentatie is opgenomen, wel worden verstrekt ten aanzien van de aan het AI-systeem onderworpen personen (in casu: de betrokkenen). De verstrekking van deze informatie aan de betrokkene kan immers de naleving van zijn transparantieverplichtingen die volgen uit de artikelen 14, lid 1, d) en 15, lid 1, b) AVG vergemakkelijken.

Bovendien laat de informatie omtrent de kwaliteit van de aangeleverde datasets de verwerkingsverantwoordelijke toe een meer volledige en gedetailleerde documentatie op te stellen van maatregelen die de kwaliteit van de data verzekeren, wat de naleving van zijn verantwoordingsplicht versterkt.

169. Ingevolge artikel 13, lid 3, b), v) van het Voorstel dienen aanbieders van AI-systemen met een hoog risico deze AI-systemen te vergezellen van gebruiksinstructies voor de gebruikers ervan (*infra* 75, nr. 188).

344

345 P. HACKER, "A legal framework for AI training data – from first principles to the Artificial Intelligence Act", *Law, Innovation and Technology* 2021, (257) 260; GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf, 13 en 33.

Deze gebruiksinstructies moeten – conform artikel 13 van het Voorstel – onder meer relevante informatie omvatten met betrekking tot de gebruikte datareeksen voor training, validatie en tests. Dit impliceert dat wanneer gebruikers van deze AI-systemen als verwerkingsverantwoordelijken kunnen worden beschouwd, deze informatie eveneens verstrekt kan worden aan de aan het AI-systeem onderworpen personen (in casu: de betrokkenen).

170. Met betrekking tot AI-systemen met een beperkt risico, voorziet de Europese wetgever geen transparantieverplichtingen omtrent de gebruikte trainings-, validerings- en testgegevens.

Afdeling 2: Proces

2.1. Informatie omtrent het bestaan van AI-systemen

2.1.1. Chatbots

171. Voor AI-systemen met een beperkt risico, moeten aanbieders van AI-systemen die bedoeld zijn voor interactie met natuurlijke personen, (*i.e.* chatbots) ervoor zorgen – conform artikel 52, lid 1 van het Voorstel – dat natuurlijke personen worden geïnformeerd dat zij interageren met een dergelijk AI-systeem en niet met een mens, tenzij de omstandigheden en de gebruikscontext dit reeds duidelijk maken, of indien het gebruik van dergelijke AI-systemen bij wet is toegestaan voor het opsporen, onderzoeken en vervolgen van strafbare feiten.

172. Transparantie refereert in deze bepaling naar menselijk bewustzijn van communicatie met AI-systemen. Door de bekendmaking van de artificiële aard van het systeem ten aanzien van de natuurlijke personen die eraan worden blootgesteld, verplicht te stellen, poogt het Voorstel het risico op imitatie of misleiding te reduceren.[346] Niettemin blijft de informatie beperkt tot het kunstmatig karakter van het systeem, zodat de aanbieders een grote vrijheid behouden voor wat betreft de informatie die zij over het systeem zelf wensen mede te delen.[347] Dit lijkt onvoldoende te zijn, in die gevallen waar dergelijke systemen potentieel hoge risico's kunnen genereren.[348]

[346] Overw. 70 Voorstel voor een Verordening betreffende Artificiële Intelligentie
[347] M. BUSUIOC, D. CURTIN en M. ALMADA, "Reclaiming transparency: contesting the logics of secrecy within the AI Act", *European Law Open* 2022, (1) 15.
[348] I. VAROSANEC, "On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI", *International Review of Law, Computers & Technology* 2022, (95) 104.

2.1.2. Deep fakes

173. Het Voorstel categoriseert *deep fakes* onder de categorie van AI-systemen met een beperkt risico waarvoor specifieke transparantieverplichtingen gelden. Artikel 52, lid 3 van het Voorstel stipuleert dat gebruikers van AI-systemen die beeld-, audio-, of videomateriaal genereren of bewerken die aanzienlijk lijkt op bestaande personen, objecten, plaatsen of andere entiteiten of gebeurtenissen en die voor een persoon ten onrechte als authentiek of waarheidsgetrouw zou overkomen, de kunstmatige aard van de resulterende inhoud moeten bekendmaken. Deze verplichting geldt niet wanneer het gebruik wettelijk is toegestaan om strafbare feiten op te sporen, te voorkomen of te vervolgen, of wanneer het noodzakelijk is voor de uitoefening van het recht op vrijheid van meningsuiting en het recht op vrijheid van kunsten en wetenschappen.

174. Hoewel deep fakes inherent misschien niet schadelijk zijn, hebben ze het vermogen om onder meer steeds meer realistische vervalsingen van geluids- en beeldfragmenten mogelijk te maken en desinformatie te verspreiden, waardoor het krachtige middelen kunnen zijn die de geest en het gedrag van een persoon kunnen manipuleren.[349] Denk in dit kader bijvoorbeeld aan de ophef die in Duitsland is ontstaan over een "interview" met Michael Schumacher.

Een studie, gemaakt in opdracht van het Europees Parlement, identificeerde het psychologisch, financieel en maatschappelijk destructief potentieel van *deep fakes* op individueel en maatschappelijk niveau.[350] Uit deze studie bleek dat dergelijke technologie aanleiding kan geven tot een breed scala aan maatschappelijke en financiële schade, waaronder reputatie- en merkschade, fraude, manipulatie van democratische processen en financiële, justitiële en wetenschappelijke systemen, laster, intimidatie en afpersing.

175. Gelet op de aard van de risico's die *deep fake*-technologieën met zich kunnen meebrengen, lijkt de categorisering van *deep fakes* als AI-systemen met een beperkt risico te leiden tot een inconsistentie met de erkenning door de Europese Commissie van andere AI-systemen als systemen met een hoog risico.[351] Dergelijke categorisering lijkt bijgevolg onvoldoende waarborgen te bieden voor de bescherming van de grondrechten van natuurlijke personen met betrekking tot bepaalde *deep fakes*.

---

[349] Res. (EP) inzake artificiële intelligentie: kwesties betreffende de interpretatie en toepassing van het internationaal recht, voor zover dit van toepassing is op de EU, op het gebied van civiel en militair gebruik en staatsgezag buiten de werkingssfeer van het strafrecht, 20 januari 2021, 2020/2013(INI), 76; R. NEUWIRTH, "Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)", *Computer Law & Security Review* 2023, (1) 6.

[350] PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (STOA), *Tackling deepfakes in European policy*, juli 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf.

[351] MESARÍC, M., SOLÁROVÁ, S., PODROUZEK, J. en BIELIKOVA, M., "Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence – Artificial Intelligence act", Kempele Institute of Intelligent Technologies 2021, (1) 8.

176. Artikel 52, lid 2 van het Voorstel bevat geen enkele verplichting om daadwerkelijk informatie over de innerlijke werking van een AI-systeem te verstrekken die relevant en bruikbaar is voor de natuurlijke persoon die eraan blootgesteld wordt.[352] Deze bepaling veronderstelt dat deze transparantieverplichting de informatieasymmetrie zou reduceren en natuurlijke personen in staat zou stellen de effecten van *deep fakes* te bestrijden.[353] Bijgevolg laat de openbaarmaking van het enkele feit dat een AI-systeem betrokken is, geen controle over de rechtmatigheid van de verwerking door de aan het AI-systeem onderworpen personen toe.[354]

177. Vervolgens bestaat ambiguïteit op welke wijze dergelijke informatie moet worden verstrekt.[355] Het Voorstel zou deze onduidelijkheid kunnen remediëren door bijkomende toelichting te verstrekken omtrent de wijze waarop de informatie moet worden verstrekt. Ten slotte wordt vanuit de rechtsleer geargumenteerd dat de gestipuleerde uitzonderingen te ruim worden geformuleerd. Enkele organisaties pleiten zelf voor een volledige schrapping van de uitzondering met betrekking tot het opsporen, voorkomen en vervolgen van strafbare feiten.[356]

2.2. Informatie omtrent de conversie door het AI-systeem van een input tot een output

2.2.1. Emotieherkenningssystemen en biometrische indelingssystemen

178. Met betrekking tot emotieherkenningssystemen of biometrische indelingssystemen, stipuleert artikel 52, lid 2 van het Voorstel dat gebruikers van dergelijke AI-systemen met een beperkt risico de daaraan blootgestelde natuurlijke personen moeten informeren over de werking van het systeem, tenzij het gevallen betreft van biometrische indeling die wettelijk zijn toegestaan om strafbare feiten op te sporen, te voorkomen en te onderzoeken. Deze uitzondering geldt niet voor emotieherkenningssystemen, op grond waarvan de openbaarmaking van hun gebruik en werking steeds verplicht is, bijvoorbeeld wanneer de politie of rechtbanken verdachten ondervragen.[357]

---

[352] P. HACKER en J. PASSOTH, "Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond" in A. HOLZINGER, R. GOEBEL, R. FONG, T. MOON, K. MÜLLER en W. SAMEK (eds.), *xxAI – Beyond Explainable AI*, Lecture Notes in Computer Science, 2022, (343) 361.
[353] MESARÍC, M., SOLÁROVÁ, S., PODROUZEK, J. en BIELIKOVA, M., "Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence – Artificial Intelligence act", Kempele Institute of Intelligent Technologies 2021, (1)7.
[354] PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (STOA), *Regulatory divergences in the draft AI act – Differences in public and private sector obligations*, mei 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU(2022)729507_EN.pdf, 30.
[355] PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (STOA), *Tackling deepfakes in European policy*, juli 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf, 60.
[356] A Civil Society Statement, An EU Artificial Intelligence Act for Fundamental Rights, 30 november 2021, https://www.accessnow.org/wp-content/uploads/2021/11/joint-statement-EU-AIA.pdf, 4.
[357] V. RAPOSO, "Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence", *International Journal of Law and Information Technology* 2022, (88) 104.

179. De wijze waarop natuurlijke personen moeten worden geïnformeerd, zal variëren in functie van de omstandigheden en de context.[358] Met betrekking tot de emotieherkenningssystemen zijn het EDPB en de EDPS echter van oordeel dat het gebruik van AI om emoties van een natuurlijke persoon af te leiden als zeer onwenselijk moet worden beschouwd en bijgevolg moet worden verboden, behalve in bepaalde welomschreven gevallen van gebruik, zoals voor gezondheids- of onderzoeksdoeleinden, mits inachtneming van passende waarborgen en alle andere gegevensbeschermingsvoorwaarden en –beperkingen.[359]

180. Ten slotte wordt opgemerkt dat artikel 52 van het Voorstel een nieuwe categorie van rechtssubjecten introduceert die betrokken zijn in de levenscyclus van AI-systemen, namelijk 'natuurlijke personen' ten aanzien waarvan de specifieke transparantieverplichtingen moeten worden gewaarborgd. Om verwarring met de andere gehanteerde termen te voorkomen, zoals 'gebruiker' en 'aanbieder' lijkt het aangewezen om in het Voorstel eveneens de notie 'natuurlijke personen'die worden onderworpen aan het AI-systeem te definiëren en de verschillen tussen de categorieën van rechtssubjecten te verduidelijken.[360]

2.2.2. Technische documentatie

181. De vereiste die aan aanbieders van AI-systemen met een hoog risico wordt opgelegd om technische documentatie op te stellen voordat dergelijke systemen in de handel worden gebracht of in gebruik worden gesteld, veruiterlijkt de idee van de op naleving gerichte transparantie.[361] De technische documentatie wordt immers op zodanige wijze opgesteld dat wordt aangetoond aan de nationale bevoegde autoriteiten en aangemelde instanties dat het AI-systeem met een hoog risico in overeenstemming is met de voorschriften voor AI-systemen met een hoog risico.[362]

---

[358] M. DUROVIC en J. WATSON, "Nothing to Be Happy about: Consumer Emotions and AI", *Multidisciplinary Scientific Journal* 2021, (784) 790.
[359] EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR (EDPB-EDPS), *Gezamenlijk advies over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie)*, 18 juni 2021, nr. 5/2021, https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_nl.pdf, 14.
[360] M. EBERS, V. HOCH, F. ROSENKRANZ, H. RUSCHEMEIER en B. STEINRÖTTER, "The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)", *Multidisciplinary Scientific Journal* 2021, (489) 598.
[361] F. SOVRANO, S. SAPIENZA, M. PALMIRANI en F. VITALI, "Metrics, Explainability and the European AI Act Proposal", *Multidisciplinary Scientific Journal* 2022, (126) 132.
[362] Art. 11, lid 1 Voorstel voor een Verordening betreffende Artificiële Intelligentie.

182. Bijlage IV bevat de verschillende informatie-elementen die de technische documentatie ten minste moet bevatten opdat het systeem zodanig 'transparant' is dat de aanbieder in eerste instantie en, indien nodig, de nationale bevoegde autoriteiten na het in de handel brengen van het AI-systeem, de conformiteit ervan kunnen beoordelen.[363] Conform Bijlage IV, dient deze technische documentatie onder meer gedetailleerde informatie te bevatten omtrent de algemene logica van het AI-systeem, het algoritme, en de werking ervan.[364]

183. Wanneer aanbieders van AI-systemen met een hoog risico als verwerkingsverantwoordelijken kunnen worden beschouwd, kan informatie met betrekking tot de algemene logica, het algoritme en de werking ervan die in de technische documentatie is opgenomen worden verstrekt ten aanzien van de aan het AI-systeem onderworpen personen (in casu: de betrokkenen). De verstrekking van deze informatie aan de betrokkene kan immers de naleving van zijn transparantieverplichting die volgt uit de artikelen 13, lid 2, onder f); 14, lid 2, onder g) en 15, lid 1, onder h) AVG vergemakkelijken. [365]

2.2.3. Registratie

184. Krachtens artikel 12 van het Voorstel worden AI-systemen met een hoog risico ontworpen en ontwikkeld met capaciteiten die de automatische registratie van gebeurtenissen ('logs' genaamd) tijdens de werking van het AI-systeem mogelijk maken. Deze loggingscapaciteiten maken de monitoring van de werking van het AI-systeem mogelijk en beogen een mate van traceerbaarheid van de werking van het AI-systeem tijdens de levensduur ervan te waarborgen.[366] Traceerbaarheid betekent dat AI-systemen zodanig zijn ontworpen dat hun besluitvorming kan worden getraceerd, op grond waarvan een betrouwbare reconstructie van de relevante processen en besluitvormingsfactoren mogelijk wordt gemaakt.[367]

185. Gezien de nadruk wordt gelegd op de traceerbaarheid van de werking van het AI-systeem, werd ervoor geopteerd om deze verplichting onder de procesfase te categoriseren.

---

[363] F. SOVRANO, S. SAPIENZA, M. PALMIRANI en F. VITALI, "Metrics, Explainability and the European AI Act Proposal", *Multidisciplinary Scientific Journal* 2022, (126) 132.
[364] Bijlage IV, lid 2, b Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[365] C. LAWSON-HETCHELY, The Potential Impact of the Future AI Act on the GDPR, onuitg. masterproef rechten University of Oslo, 2022, 21.
[366] Art. 12, lid 2 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[367] H. FELZMANN, E. FOSCH-VILLARONGA, C. LUTZ en A. TAMO-LARRIEUX, "Towards Transparency by Design for Artificial Intelligence", *Science and Engineering Ethics* 2020, (3333) 3351.

186. Traceerbaarheid wordt door de HLEG AI eveneens als een belangrijke component van transparantie beschouwd.[368] In haar ethische Richtsnoeren voor betrouwbare AI stipuleert de HLEG AI dat onder meer de processen – waaruit een bepaalde output door het AI-systeem wordt gegenereerd – zo goed mogelijk moeten worden gedocumenteerd om ze traceerbaar te maken en de transparantie te vergroten. Hierdoor wordt het immers mogelijk vast te stellen waarom een bepaalde output onjuist was, waardoor vervolgens ook toekomstige fouten kunnen worden voorkomen.

187. Traceerbaarheid – als onderdeel van de dimensie verklaarbaarheid – faciliteert controle (doelstelling: procedurele rechtvaardigheid en eerlijkheid) door de aan het AI-systeem onderworpen personen.[369] Wanneer immers tijdens de implementatiefase van het AI-systeem, de gebruiker kan worden beschouwd als een verwerkingsverantwoordelijke, kan deze ervoor opteren om de informatie die voortvloeit uit de registratie van de werking van het AI-systeem, mee te delen aan de betrokkene om de naleving van zijn transparantieverplichting ex artikelen 13, lid 2, onder f); 14, lid 2, onder g) en 15, lid 1, onder h) AVG te vergemakkelijken.

2.2.4. Transparantie en informatieverstrekking aan gebruikers

188. Artikel 13, lid 1 van het Voorstel bepaalt dat AI-systemen met een hoog risico op zodanige wijze moeten ontworpen en ontwikkeld worden dat de werking ervan voldoende transparant is om de gebruikers in staat te stellen de output van het systeem te interpreteren en dienovereenkomstig op passende wijze te gebruiken (*i.e.* interne transparantie, *infra* 32, nr. 78). Daarbij moet een "passende soort en mate van transparantie" worden gewaarborgd met het oog op het faciliteren van de naleving van de verplichtingen van gebruikers en aanbieders in het kader van het Voorstel.[370] Daarenboven dienen AI-systemen met een hoog risico vergezeld te gaan van gebruiksinstructies die beknopte, volledige, juiste en duidelijke informatie bevat die relevant, toegankelijk en begrijpelijk is voor gebruikers (*i.e.* het relationele aspect van de dimensie verklaarbaarheid).[371]

189. De precieze reikwijdte en inhoud van de transparantieverplichting wordt verder gepreciseerd in artikel 13, lid 3 van het Voorstel. De relevante informatie met betrekking tot het proces van conversie van een input tot een output moet onder meer de technische specificaties en details over de kenmerken, capaciteiten en prestaties van het AI-systeem omvatten.

---

[368] THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (HLEG AI), *Ethische Richtsnoeren voor Betrouwbare KI,* 8 april 2019, https://op.europa.eu/nl/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1#, 49.
[369] A. KISELEVA, D. KOTZINOS en P. DE HERT, "Transparency of AI in Healthcare as a Multilayered System of Accountabilities: Between Legal Requirements and Technical Limitations", *Frontiers in Artificial Intelligence* 2022, (1) 5.
[370] Arts. 16 – 29 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[371] Art. 13, lid 2 en 3 Voorstel voor een Verordening betreffende Artificiële Intelligentie.

190. Er kunnen enkele beperkingen geïdentificeerd worden met betrekking tot de inhoudelijke invulling van de transparantieverplichting in artikel 13 van het Voorstel. Vooreerst is artikel 13 van het Voorstel specifiek gericht op het bieden van transparantie ten aanzien van de gebruikers van AI-systemen en niet ten aanzien van de individuen die eraan zijn onderworpen (*i.e.* externe transparantie).[372] Dit blijkt eveneens uit de zinsnede van artikel 13, lid 1 van het Voorstel die de specifieke doelstelling van "een passende soort en mate van transparantie" omschrijft als het faciliteren van de naleving van de verplichtingen van gebruikers en aanbieders die ze hebben in hoofde van het Voorstel. Bijgevolg lijkt transparantie in het Voorstel in eerste plaats gericht te zijn op de naleving van het Voorstel zelf, en niet op de uitoefening van de rechten die de aan het AI-systeem onderworpen personen zouden kunnen hebben.[373]

Dit impliceert dat de geponeerde transparantieverplichting primair ten aanzien van de aan het AI-systeem onderworpen natuurlijke personen weinig effect lijkt te hebben, daar artikel 13 geen wezenlijke bijdrage levert aan de aanvulling of aanscherping van de inhoud om 'nuttige' informatie te verstrekken over de achterliggende logica aan betrokkenen onder de AVG, en bijgevolg niet leidt tot een versterking van de bescherming en uitoefening van hun (grond)rechten.[374] Dit gegeven staat op gespannen voet met een van de door het Voorstel vooropgestelde doelstellingen, namelijk de versterking en bevordering van de door het Handvest van de Grondrechten van de EU beschermde grondrechten, zoals onder meer de bescherming van persoonsgegevens.[375]

191. Ter versterking van de rechtspositie van de aan het AI-systeem onderworpen personen, lijkt het bijgevolg aangewezen de begunstigden van de informatieverplichtingen die in titel III aan de aanbieders van AI-systemen worden opgelegd, uit te breiden tot personen die aan het AI-systeem onderworpen worden, en niet alleen aan de gebruikers ervan.[376] Het ontbreken van enige verwijzing in de bindende tekst van het Voorstel naar betrokkenen of andere personen die aan het AI-systeem worden onderworpen, lijkt een dode hoek te zijn, aldus het EDPB en de EDPS.[377]

---

[372] M. FINK, "The EU Artificial Intelligence Act and Access to Justice", *EU Law Live* 2021, (1) 2; N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI en K. YEUNG, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", *SSRN* 2021, (1) 35.
[373] P. HACKER en J. PASSOTH, "Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond" in A. HOLZINGER, R. GOEBEL, R. FONG, T. MOON, K. MÜLLER en W. SAMEK (eds.), *xxAI – Beyond Explainable AI*, Lecture Notes in Computer Science, 2022, (343) 359.
[374] *Ibid.,* (343) 361.
[375] Titel 3.5. Memorie van ToelichtingVoorstel voor een Verordening betreffende Artificiële
[376] A. KISELEVA, "Comments on the EU Proposal for the Artificial Intelligence Act", *SSRN* 2021, (1) 2; N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI en K. YEUNG, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", *SSRN* 2021, (1) 52.
[377] EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR (EDPB-EDPS), *Gezamenlijk advies over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie)*,

De verplichtingen die aan de betrokken actoren worden opgelegd, moeten immers concreter voortvloeien uit de bescherming van het individu en zijn of haar rechten.[378]

192. Vervolgens creëert het gebruik van termen als "passende" en "voldoende", respectievelijk soort en mate van transparantie, ambiguïteit omtrent de reikwijdte van de transparantieverplichtingen en laat bijgevolg veel interpretatieruimte aan de aanbieders van AI-systemen bij het bepalen van het transparantieniveau.[379] De norm formuleert immers algemene eisen zonder deze te specificeren.

2.2.5. Menselijk Toezicht

193. Transparantie is nauw verbonden met de eisen inzake menselijk toezicht ex artikel 14 (*infra* 80, nr. 200), omdat deze eisen inzake menselijk toezicht onrechtstreeks ten aanzien van natuurlijke personen die worden onderworpen aan AI-systemen met een hoog risico bijkomende transparantie – als onderdeel van de dimensie verklaarbaarheid – kunnen bieden omtrent de werking van het AI-systeem en de gegenereerde output.[380]

194. Wanneer immers een gebruiker kan worden beschouwd als een verwerkingsverantwoordelijke in de zin van de AVG, kan deze laatste ervoor opteren om de informatie die voortvloeit uit het uitoefenen van het menselijk toezicht, te verstrekken aan de natuurlijke persoon wiens persoonsgegevens door het AI-systeem met een hoog risico werden verwerkt teneinde de naleving van zijn verplichtingen uit hoofde van de AVG te vergemakkelijken. In deze optiek kan menselijk toezicht worden gelieerd aan transparantie ten aanzien van betrokkenen (*i.e.* externe transparantie).[381]

---

18 juni 2021, nr. 5/2021, https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_nl.pdf, 10.

[378] *Ibid.*

[379] M. BUSUIOC, D. CURTIN en M. ALMADA, "Reclaiming transparency: contesting the logics of secrecy within the AI Act", *European Law Open* 2022, (1) 20.

[380] P. HACKER en J. PASSOTH, "Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond" in A. HOLZINGER, R. GOEBEL, R. FONG, T. MOON, K. MÜLLER en W. SAMEK (eds.), *xxAI – Beyond Explainable AI*, Lecture Notes in Computer Science, 2022, (343) 360.

[381] K. BRENNAN-MARQUEZ, K. LEVY en D. SUSSER, "Strange Loops: apparent versus actual human involvement in automated decision making", *Berkely Technology Law Journal* 2019, (745) 745.

Echter, de tekst van het Voorstel blijft onduidelijk betreffende de vraag of menselijk toezicht moet worden uitgeoefend door de gebruiker of door iemand die onafhankelijk is van de gebruiker.[382] De Raad heeft in zijn Gemeenschappelijk Standpunt deze onduidelijkheid geremedieerd en verduidelijkt dat menselijk toezicht moet worden uitgeoefend door de gebruiker.[383]

2.2.6. Europese Databank

195. Het Voorstel introduceert een door de Europese Commissie beheerde Europese databank waarin essentiële informatie over alle in de EU gebruikte autonome AI-systemen met een hoog risico moeten worden geregistreerd met het oog op het vergroten van de publieke transparantie en het publieke toezicht. [384] Dit wordt zowel in de rechtsleer, als door het EDPB en de EDPS (*European Data Protection Supervisor*) toegejuicht. Dergelijke databank betreft immers een potentieel nuttig instrument om ten aanzien van natuurlijke personen de noodzakelijke transparantie met betrekking tot de gegevensverwerking door autonome hoog risico AI-systemen te kunnen garanderen.

196. Echter, de in bijlage VIII opgenomen informatie die door de aanbieders van dergelijke geregistreerde AI-systemen in de Europese databank moet worden opgenomen, lijkt vrij beperkt te zijn en lijkt bijgevolg niet te beantwoorden aan de informatiebehoeften van de natuurlijke personen die onderworpen worden aan deze AI-systemen om de rechtmatigheid van de gegevensverwerking te kunnen begrijpen en onderzoeken (*i.e.* controle: procedurele rechtvaardigheid).[385]

In de rechtsleer, alsook in het gezamenlijk advies van het EDPB en de EDPS, wordt gepleit om een meer exhaustieve lijst van informatie op te nemen in de databank opdat de natuurlijke personen wiens persoonsgegevens worden verwerkt door autonome hoog risico AI-systemen toegang kunnen krijgen tot informatie die hen daadwerkelijk helpt de verwerking te begrijpen, zodoende de rechtmatigheid ervan te kunnen controleren.

---

[382] M.EBERS, V. HOCH, F. ROSENKRANZ, H. RUSCHEMEIER en B. STEINRÖTTER, "The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)", *Multidisciplinary Scientific Journal* 2021, (589) 596; N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI en K. YEUNG, *How the EU can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act*, Leads Lab, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991#, 35.

[383] Art. 14, lid 4 Gemeensch.Standp. Raad

[384] Art. 51 en 60 Voorstel voor een Verordening betreffende Artificiële Intelligentie; Overw. 69 Voorstel voor een Verordening betreffende Artificiële Intelligentie; Titel 5.2.3. Memorie van Toelichting Voorstel voor een Verordening betreffende Artificiële Intelligentie

[385] N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI en K. YEUNG, *How the EU can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act*, LEADS Lab, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991#, 52.

Die informatie kan betrekking hebben op de kenmerken, mogelijkheden, beperkingen van de prestaties van het AI-systeem en het type of model van *machine learning*.[386]

2.3. Informatie omtrent de risico's van het gebruik van AI-systemen

197. Overweging 47 stipuleert dat gebruikers de output van AI-systemen met een hoog risico moeten kunnen interpreteren en dienovereenkomstig gebruiken. Om dit mogelijk te maken moeten deze AI-systemen vergezeld gaan van relevante documentatie en gebruiksaanwijzigingen die beknopte en duidelijke informatie moet bevatten, waar passend ook met betrekking tot de mogelijke risico's voor de grondrechten en risico's op discriminatie.

Informatie omtrent de mogelijke risico's voor de grondrechten en risico's op discriminatie worden evenwel niet opgenomen in de bindende tekst van het Voorstel. Bijgevolg ontbreekt essentiële informatie omtrent de wijze waarop degene die aan het AI-systeem worden onderworpen nadelige gevolgen van het AI-systeem kunnen ondervinden.

Afdeling 3: Output

198. In het Voorstel kon geen informatie worden geïdentificeerd die in de dimensie verklaarbaarheid zou kunnen worden opgenomen over de output van de gegevensverwerking door een AI-systeem. Immers, in het Voorstel wordt geen gewag gemaakt van de specifieke gevolgen die verbonden worden aan de door het AI-systeem gegenereerde output.

[386] M.EBERS, V. HOCH, F. ROSENKRANZ, H. RUSCHEMEIER en B. STEINRÖTTER, "The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)", *Multidisciplinary Scientific Journal* 2021, (589) 597; N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI en K. YEUNG, *How the EU can achieve legally trustworthy AI: a response to the European Commission's Proposal for an Artificial Intelligence Act*, Leads Lab, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991#, 53; EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR (EDPB-EDPS), *Gezamenlijk advies over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie)*, 18 juni 2021, nr. 5/2021, https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_nl.pdf, 22.

Hoofdstuk 2: Controle in het Voorstel
Afdeling 1: Input

199. In het Voorstel wordt, in tegenstelling tot de AVG, geen specifiek controlemechanisme geïntroduceerd in de inputfase van de gegevensverwerking.

Afdeling 2: Proces
2.1. Menselijk toezicht

200. Op grond van artikel 14, lid 1 van het Voorstel moeten AI-systemen met een hoog risico zodanig worden ontworpen en ontwikkeld dat hierop tijdens de periode dat het AI-systeem wordt gebruikt, op doeltreffende wijze toezicht kan worden uitgeoefend door natuurlijke personen. Artikel 14, lid 1 van het Voorstel vereist uitdrukkelijk dat 'doeltreffend' menselijk toezicht vereist is. In tegenstelling tot de AVG wordt dus een duidelijke kwaliteitsvereiste inzake het menselijk toezicht opgelegd. Echter, artikel 14 van het Voorstel blijft vaag over wat menselijk toezicht nu precies 'doeltreffend' maakt.[387]

201. De eisen inzake menselijk toezicht nemen – naast hun plaats in de dimensie verklaarbaarheid, waar ze een belangrijke faciliterende rol spelen ter voldoening van de tweede vorm van controle – eveneens een belangrijke rol op in de controledimensie ten voordele van de veiligheid en precisie. Immers, menselijk toezicht is erop gericht de menselijke autonomie te ondersteunen wanneer geautomatiseerde besluitvorming plaatsvindt, op grond waarvan menselijk toezicht als een belangrijk middel kan worden beschouwd om de risico's voor de grondrechten te voorkomen of tot een minimum te beperken.[388]

202. Het EDPB en de EDPS juichen de prominente plaats van de notie 'menselijk toezicht' in het Voorstel toe, omdat het Voorstel de reële centrale rol van de mens erkent, alsook het recht eerbiedigt om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit ex artikel 22 AVG.[389]

---

[387] J. LAUX, "Institutionalised Distrust and Human Oversight of Artificial intelligence: Toward a Democratic Design of AI Governance under the European Union Act", *Oxford Internet Institute* 2023, (1) 7.
[388] Art. 14, lid 2 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[389] EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR (EDPB-EDPS), *Gezamenlijk advies over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie)*, 18 juni 2021, nr. 5/2021, https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_nl.pdf, 7.

203. Aanbieders van AI-systemen met een hoog risico moeten verzekeren dat deze AI-systemen in overeenstemming zijn met de eisen inzake menselijke toezicht.[390] Alvorens het AI-systeem in de handel wordt gebracht of in gebruik wordt gesteld, moeten de aanbieders hetzij passende maatregelen vaststellen die door de gebruiker moeten worden uitgevoerd, hetzij maatregelen vaststellen en inbouwen in het AI-systeem indien dit technisch haalbaar is om het menselijk toezicht te waarborgen.[391] De natuurlijke personen aan wie de taak van het menselijk toezicht is toegewezen, moeten beschikken over de noodzakelijke competenties, opleiding en autoriteit om deze taak uit te voeren.[392]

204. Controle over het proces van conversie van een input tot een output vindt weerklank in de eisen inzake menselijk toezicht. In eerste instantie stipuleert artikel 14, lid 4, a) van het Voorstel dat het AI-systeem op dergelijke wijze ontworpen en ontwikkeld moet worden, dat de natuurlijke persoon die belast wordt met het menselijk toezicht, in staat is om de capaciteiten en beperkingen van het AI-systeem volledig te begrijpen en de werking ervan naar behoren te kunnen monitoren, zodat tekenen van onregelmatigheden, storingen en onverwachte prestaties zo snel mogelijk kunnen worden gedetecteerd. Deze invulling van menselijk toezicht stuit in de rechtsleer op kritiek. Zo zou deze verplichting voor *black box* AI-systemen niet haalbaar zijn, daar *black boxes* niet volledig te begrijpen zijn.[393] De praktische haalbaarheid van deze invulling van menselijk toezicht is bijgevolg twijfelachtig.

205. Vervolgens moet het AI-systeem op zo'n wijze worden ontwikkeld en ontworpen dat de natuurlijke toezichtspersoon in staat is om zich bewust te blijven van de mogelijke neiging om automatisch (te veel) te vertrouwen op de output van het AI-systeem. Enkele bedenkingen kunnen in dit kader worden gemaakt. Vooreerst lijkt het onwaarschijnlijk dat het probleem van *'automation bias'*, namelijk het psychologisch verschijnsel om geneigd te zijn de output van het AI-systeem blindelings te vertrouwen en automatisch te aanvaarden, door deze bepaling kan worden geremedieerd.[394] Daarenboven lijkt het niet voldoende om te vereisen dat deze personen zich voldoende bewust zijn van de mogelijkheid van *automation bias*, maar moet op transparante wijze ook effectief worden aangetoond dat beslissingen niet worden genomen door te veel te vertrouwen op de output van een AI-systeem.[395]

---

[390] Art. 16 (a) Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[391] Art. 14, lid 3 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[392] Overw. 48 Voorstel voor een Verordening betreffende Artificiële Intelligentie.
[393] M. EBERS, V. HOCH, F. ROSENKRANZ, H. RUSCHEMEIER en B. STEINRÖTTER, "The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)", *Multidisciplinary Scientific Journal* 2021, (489) 596.
[394] N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI en K. YEUNG, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", *LEADS Lab* 2021, (1) 35.
[395] *Ibid.*

206. Bovendien moet het AI-systeem zodanig ontwikkeld en ontworpen worden dat de natuurlijke toezichtspersoon in staat wordt gesteld om de output van het AI-systeem met een hoog risico juist te interpreteren. Het lijkt aangewezen dat de Europese wetgever de invulling verduidelijkt van de notie 'interpreteerbaarheid'. Immers, rechtsgeleerden en beleidsmakers uit verschillende disciplines hebben verschillende opvattingen over de invulling van de notie 'interpreteerbaarheid', waardoor ambiguïteit én rechtsonzekerheid bestaat omtrent de precieze betekenis van deze notie.

Sommige auteurs definiëren interpreteerbaarheid als het feit dat het AI-model van nature begrijpelijk is.[396] Echter, AI-systemen die gebruik maken van *machine learning* methoden worden gekenmerkt door ondoorgrondelijkheid/ondoorzichtigheid en de mogelijkheid tot *self learning*, waardoor ze niet interpreteerbaar zijn (volgens deze definitie). Dit zou impliceren dat de Europese wetgever deze *black box*-modellen (die een van de meest geavanceerde en veelbelovende AI-systemen uitmaken) zou uitsluiten van het toepassingsgebied van de regelgeving.[397] Dit lijkt niet de bedoeling te zijn. Het lijkt dan ook aangewezen dat het Voorstel duidelijkheid creëert omtrent de invulling van deze notie.

207. Voorts moet het AI-systeem ontwikkeld en ontworpen worden op een wijze dat de natuurlijke toezichtspersoon in staat stelt om te kunnen besluiten het AI-systeem niet te gebruiken of de output van het AI-systeem op andere wijze te negeren, terzijde te schuiven of terug te draaien.[398]

208. Vervolgens moet het AI-systeem op dergelijke wijze ontworpen en ontwikkeld te worden, dat de natuurlijke toezichtspersonen in staat zijn om in te grijpen in de werking van het AI-systeem of het systeem kunnen onderbreken door middel van een stopknop of een vergelijkbare procedure.

209. Ten slotte introduceert artikel 14, lid 5 van het Voorstel het zgn. vier ogen-principe voor AI-systemen die worden gebruikt voor biometrische identificatie op afstand van natuurlijke personen. Menselijk toezicht houdt in casu in dat de gebruiker van deze AI-systemen geen actie of beslissingen kan nemen op basis van het door het systeem gegenereerde identificatie, tenzij wanneer deze door minstens twee natuurlijke personen zijn geverifieerd en bevestigd. Dit is een bijkomende toezichtsvereiste wanneer biometrische identificatiesystemen worden gebruikt.

---

[396] A. BIBAL, M. LOGNOUL, A. DE STREEL en B. FRENAY, "Legal requirements on explainability in machine learning", *Artificial Intelligence & Law* 2021, (149) 150.
[397] A. KISELEVA, "Making AI's Transparency Transparent: notes on the EU Proposal", European Law Blog 2021 (blog), https://europeanlawblog.eu/2021/07/29/making-ais-transparency-transparent-notes-on-the-eu-proposal-for-the-ai-act/.
[398] Art. 14, lid 4, d) Voorstel voor een Verordening betreffende Artificiële Intelligentie.

Opdat dit menselijk toezicht doeltreffend zou zijn, is het vereist dat de bevestiging door twee natuurlijke personen gebaseerd dient te zijn op een door beiden afzonderlijk gemaakte beoordeling.[399] Daarenboven moet menselijk toezicht beschouwd worden als een laatste redmiddel wanneer is aangetoond dat het gebruik van dergelijke indringende systemen noodzakelijk en evenredig is in een democratische samenleving.[400] Het mag bijgevolg niet worden gebruikt als legitimatie/excuus voor het gebruik van AI-systemen die in feite niet zouden mogen worden gebruikt.

Afdeling 3: Output

210. In het Voorstel kon geen controlemechanisme worden geïdentificeerd die de aan het AI-systeem onderworpen persoon de mogelijkheid biedt om controle over zijn (persoons)gegevens te behouden in de outputfase van de gegevensverwerking. In deze fase in de controledimensie gaat het specifiek over de vraag of de aan het AI-systeem onderworpen persoon enige instrumenten in handen heeft om zich te verzetten in de outputfase tegen de specifieke gevolgen die verbonden zijn aan de gegenereerde output.

Hoofdstuk 3: Conclusie

211. Op grond van de voorgaande paragrafen, wordt in deze conclusie een antwoord geformuleerd op de tweede deelvraag, met name: "waarin verschilt de invulling van de transparantievereisten in de AVG ten opzichte van de transparantievereisten in het Voorstel?".

212. Het Voorstel beoogt de ontwikkeling en het gebruik van AI te reguleren, met specifieke aandacht voor de unieke kenmerken die deze technologie omhelst. Hoewel een van de door het Voorstel vooropgestelde doelstellingen erin bestaat de bescherming van persoonsgegevens te versterken en bevorderen, lijken de aan het AI-systeem onderworpen personen en de instrumenten die hen betekenisvolle transparantie beogen te bieden, geen prominente plaats in te nemen in het Voorstel.

Ten opzichte van de AVG wordt immers vastgesteld dat het Voorstel geen aanvulling/versterking impliceert in de verklaarbaarheidsdimensie met betrekking tot de output, alsook niet in de input- en outputfase van de controledimensie. De aanvulling in de procesfase in de controledimensie is slechts minimaal. Zo bevat het Voorstel bijvoorbeeld geen enkel mechanisme om personen die worden

[399] N. SMUHA, E. AHMED-RENGERS, A. HARKENS, W. LI, J. MACLAREN, R. PISELLI en K. YEUNG, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", *LEADS Lab* 2021, (1) 36.
[400] *Ibid.*

onderworpen aan AI-systemen in staat te stellen de AI-gestuurde besluitvorming aan te vechten (procesfase) of te weigeren (inputfase).[401]

Dit is te verklaren door de verschillende benaderingen op grond waarvan de AVG, dan wel het Voorstel is geconstrueerd. Daar waar de AVG een belangrijk kader representeert om de eerbiediging van het gegevensbeschermingsrecht als grondrecht maximaal te eerbiedigen, maakt het Voorstel eerder het voorwerp uit van productregulering dat de productveiligheid van AI-systemen centraal stelt.[402]

213. Het Voorstel focust zich voornamelijk op de procesfase; de fase waarin het *black box*- en zelflerend karakter van AI-systemen op de voorgrond treden. Echter, de in het Voorstel opgenomen transparantievereisten zullen heel vaak maar indirect transparantie verzekeren ten aanzien van de aan het AI-systeem onderworpen personen. Zij zijn immers in hoge mate afhankelijk van het gegeven of de aanbieder, dan wel de gebruiker van een AI-systeem als verwerkingsverantwoordelijke kan worden beschouwd.

Bovendien gelden de bepalingen die bijkomende transparantie kunnen verzekeren ten opzichte van de AVG heel vaak enkel wanneer het gaat om AI-systemen met een hoog risico. Met betrekking tot AI-systemen met een beperkt risico worden slechts minimale transparantieverplichtingen opgelegd. Voorts worden in het Voorstel eveneens vage en open normen gehanteerd, waardoor men blijft worstelen met normen die niet eenduidig te interpreteren zijn. Ten slotte wordt, in tegenstelling tot de AVG, weinig tot geen aandacht besteed aan het relationele aspect van de dimensie verklaarbaarheid.

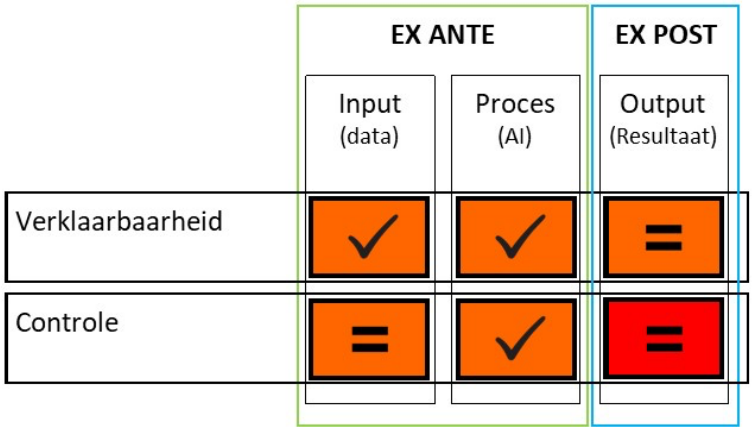
[401] M. MLADENOV, "Human vs. Artificial Intelligence – EU's legal response", *LAW – theory and practice* 2023, (32) 39.
[402] AUTORITEIT PERSOONSGEGEVENS (AP), *AP Inzet Artificial Iintelligence Act,* 15 maart 2022, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_inzet_ai_act.pdf, 4.

DEEL VI. CONCLUSIE OP BASIS VAN HET GEÏNTEGREERD TRANSPARANTIEKADER

Hoofdstuk 1: Visualisering van de conclusie

214. In deel III werd de zelf ontwikkelde definiëring van betekenisvolle transparantie in AI-context vertaald in een transparantiekader. Deel IV analyseert de manier waarop de transparantievereisten gedefinieerd zijn in de AVG en identificeert grenzen met betrekking tot de wijze waarop ze daarin omschreven worden. In deel V werden de transparantievereisten in het Voorstel gescreend en nagegaan hoe deze verschillen met de AVG. Deze twee analyses worden in dit laatste deel geïntegreerd in een samenvattend transparantiekader om zo tot een antwoord te komen op de centrale onderzoeksvraag, met name: "zorgen de AVG en het Voorstel voor betekenisvolle transparantie bij de toepassing van AI-systemen ten aanzien van de aan het AI-systeem onderworpen personen?".

Figuur 7 visualiseert de conclusie met betrekking tot de centrale onderzoeksvraag.



Figuur 7: Geïntegreerd transparantiekader

In deel VI wordt dus in het bijzonder nagegaan in welke mate de informatieasymmetrie maximaal gereduceerd wordt in de verschillende fasen van de gegevensverwerking en in welke mate de controle over (persoons)gegevens doeltreffend is.

215. In het bovenstaand transparantiekader worden twee componenten geïntegreerd. De eerste component omvat de symbolen ('v' of '=') en visualiseert of het Voorstel al dan niet aanvullend werkt op de AVG. Werkt het aanvullend, en dus versterkend, wordt gewerkt met een vinkje ('v'). Werkt het Voorstel niet aanvullend, maar doet het er geen afbreuk aan, dan wordt deze *status quo* aangeduid met een gelijkheidsteken ('=').

216. De tweede component is een kleurcode (groen, oranje, rood). De kleur visualiseert de mate waarin beide Europese rechtsinstrumenten samen in staat zijn tot maximale reductie van de informatieasymmetrie (verklaarbaarheidsdimensie), respectievelijk doeltreffende controle (controledimensie).

Groen in de verklaarbaarheidsdimensie impliceert dat de transparantieverplichtingen in beide Europese rechtsinstrumenten in staat zijn de informatieasymmetrie maximaal te reduceren waarbij het relationele aspect van de verklaarbaarheidsdimensie volledig eerbiedigd wordt. Rood betekent dat de transparantieverplichtingen in de rechtsinstrumenten daartoe niet in staat zijn. Oranje representeert de voorwaardelijke maximale reductie van de informatieasymmetrie, in die zin dat de informatieasymmetrie slechts maximaal gereduceerd kan worden als belangrijke randvoorwaarden vervuld zijn.

Groen in de controledimensie impliceert doeltreffende controle. Rood betekent dat er geen sprake is van doeltreffende controle. Oranje ten slotte, representeert doeltreffende controle in theorie, maar de praktische haalbaarheid ervan blijft twijfelachtig.

217. In hoofdstuk 2 wordt een toelichting gegeven bij de keuze voor het een of het andere symbool, respectievelijk kleur.

Hoofdstuk 2: Toelichting van de conclusie

Afdeling 1: Verklaarbaarheid

1.1. Input

218. Met betrekking tot transparantie over de input vormt het Voorstel algemeen een versterking ten opzichte van de AVG (‘v’). De informatieasymmetrie kan maximaal gereduceerd worden op voorwaarde dat een aantal belangrijke randvoorwaarden vervuld zijn. Vandaar de keuze voor de kleur oranje.

1.1.1. Informatie omtrent de dataverzameling

219. Inzake de dataverzameling, poneert de AVG een duidelijke transparantieverplichting: de verwerkingsverantwoordelijke moet de betrokkene informeren omtrent welke persoonsgegevens van hem/haar worden verzameld om het AI-systeem te voeden (zowel in de ontwikkelingsfase, als in de implementatiefase van het AI-systeem).

Dit is een belangrijke transparantieverplichting die ervoor zorgt dat betrokkenen een beter begrip hebben van welke persoonsgegevens worden gebruikt en verwerkt door het AI-systeem, waardoor de

informatieasymmetrie met betrekking tot de input van het AI-systeem in belangrijke mate tussen de betrokkene en de verwerkingsverantwoordelijke wordt gereduceerd. Echter, deze transparantievereiste staat op gespannen voet met de complexiteit van de gegevensverzameling door *Data Driven Companies*. Hoewel deze transparantieverplichting wezenlijk is om de informatieasymmetrie tussen de betrokkene en een verwerkingsverantwoordelijke te reduceren, stelt de complexiteit van de gegevensverzameling door *Data Driven Companies* de doeltreffendheid van deze verplichting in vraag.

220. Het Voorstel kan op de AVG wel een belangrijke aanvulling vormen, maar enkel uitsluitend met betrekking tot de ontwikkelingsfase van het AI-systeem. Er is namelijk in het Voorstel geen enkele transparantieverplichting voorzien met betrekking tot de dataverzameling in de implementatiefase van een AI-systeem. Dit impliceert meteen ook dat het Voorstel geen antwoord biedt op de problematiek inzake de gegevensverzameling door *Data Driven Companies*. Wil het Voorstel daadwerkelijk meer transparantie bieden omtrent de ontwikkelingsfase van het AI-systeem (en dus een versterking betekenen), dan moeten twee voorwaarden vervuld zijn.

Vooreerst moeten persoonsgegevens worden verwerkt. Immers, de gebruikte datareeksen waarmee het AI-systeem in de ontwikkelingsfase werd gevoed, is een informatie-element dat moet worden opgenomen in de technische documentatie. De aan het AI-systeem onderworpen personen kunnen omtrent dit element slechts worden geïnformeerd op indirecte wijze, namelijk wanneer de aanbieder als verwerkingsverantwoordelijke kan worden beschouwd. In de implementatiefase van het AI-systeem is dit eerder onwaarschijnlijk.[403] Ten tweede moet het gaan om een AI-systeem met een hoog risico. Voor AI-systemen met een beperkt risico biedt het Voorstel dus sowieso geen versterking.

1.1.2. Informatie omtrent de kwaliteit van de aangeleverde data(sets)

221. In het Voorstel wordt de kwaliteit van de aangeleverde datasets in de ontwikkelingsfase van het AI-systeem met hoog risico uitdrukkelijk gereguleerd. Dit aspect lijkt een grote meerwaarde te zijn ten aanzien van de AVG.

De AVG bepaalt immers enkel dat de aangeleverde data(sets) 'juist' moeten zijn. Dit is een uiterst vage norm en verlangt precisering in AI-context. Daarnaast vereist de AVG eveneens dat passende maatregelen worden genomen om de kwaliteit van deze data te verzekeren. Termen als 'passende' maatregelen duiden opnieuw op vage en open normen die een belangenafweging vergen.

[403] S. BARROS VALE, "GDPR and the AI Act interplay: lessons from FPF's ADM case-law report", Future of Privacy Forum 2022 (blog), https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/;

In het Voorstel moet informatie omtrent de kwaliteitsvereisten en de methoden voor de data-opschoning worden opgenomen in de technische documentatie en gebruiksinstructies bij het AI-systeem. De uitdrukkelijke erkenning van het belang van kwaliteitsvolle data en een poging tot definiëring van wat dit inhoudt voor de ontwikkeling van AI-systemen, wordt ten zeerste geapprecieerd.

222. Gezien dit gegeven, kunnen de bepalingen uit het Voorstel een versterking impliceren ten opzichte van de AVG – en bijgevolg samen de informatieasymmetrie maximaal reduceren – mits enkele voorwaarden vervuld zijn.

Vooreerst moeten persoonsgegevens worden verwerkt. De aan het AI-systeem onderworpen personen kunnen immers slechts omtrent de kwaliteit van de trainingdata worden geïnformeerd op indirecte wijze, namelijk wanneer de aanbieder, respectievelijk de gebruiker als verwerkingsverantwoordelijke kan worden beschouwd. In de implementatiefase van het AI-systeem, is het waarschijnlijk dat de gebruiker als verwerkingsverantwoordelijke wordt beschouwd.

Bovendien worden deze datavereisten, alsook de documentatie ervan in de technische documentatie, dan wel in de gebruiksinstructies enkel opgelegd met betrekking tot AI-systemen met een hoog risico. Voor AI-systemen met een beperkt risico ontbreken dergelijke kwaliteitsvereisten en de documentatie ervan.

1.2. Proces

223. Met betrekking tot transparantie over het proces wordt algemeen een versterking ('v') geïdentificeerd ten opzichte van de AVG. De transparantieverplichtingen worden geacht samen de informatieasymmetrie maximaal te kunnen reduceren, mits een aantal randvoorwaarden vervuld zijn. Vandaar de keuze voor de kleur oranje.

1.2.1. Informatie omtrent het bestaan van AI-systemen

224. Met betrekking tot het eerste aspect van transparantie, merkt de AVG op dat de betrokkene moet worden geïnformeerd omtrent het gegeven dat zijn/haar persoonsgegevens geautomatiseerd worden verwerkt. Het Voorstel voegt in dit kader toe dat wanneer personen interageren met chatbots zij hieromtrent moeten worden geïnformeerd. Dit is een belangrijke toevoeging, want heel vaak interageren mensen met chatbots zonder dat deze persoonsgegevens verwerken. Gezien het risico op misleiding (dat eraan verbonden kan worden) is het noodzakelijk dat personen die ermee interageren hierover worden geïnformeerd.

225. Met betrekking tot *deep fakes*, voorziet het Voorstel dat de gebruikers van dergelijk AI-systemen, de kunstmatige aard van de resulterende inhoud moeten bekendmaken. Ook dit is – vanuit de idee om misleiding te reduceren – een wezenlijke versterking ten aanzien van de AVG.

1.2.2. Informatie omtrent de conversie door het AI-systeem van een input tot een output

226. Verwerkingsverantwoordelijken moeten de betrokkene 'nuttige' informatie verstrekken over de onderliggende logica van de verwerking. Dit is een uiterst vage norm waaromtrent de AVG geen duidelijkheid biedt over welke soort informatie in dit kader moet worden geboden. De Richtsnoeren van het EDPB bieden eveneens geen duidelijkheid. Dit creëert onvermijdelijk rechtsonzekerheid.

227. Het Voorstel heeft een aantal mechanismen in het leven geroepen die bijkomende transparantie kunnen verzekeren met betrekking tot het conversieproces, waardoor de bepalingen uit het Voorstel een versterking kunnen impliceren ten opzichte van de AVG – en bijgevolg samen de informatieasymmetrie maximaal kunnen reduceren – mits enkele voorwaarden vervuld zijn.

Voor emotieherkenningssystemen of biometrische indelingssystemen (AI-systemen met een beperkt risico) moeten de gebruikers de daaraan blootgestelde natuurlijke personen informeren over de werking van het systeem. Positief aan deze transparantieverplichting is het gegeven dat dit een transparantieverplichting is die rechtstreeks gericht is op de aan het AI-systeem onderworpen personen. Echter, deze bepaling verschaft geen duidelijkheid over de inhoudelijke invulling van "de werking". In dit opzicht is er opnieuw onduidelijkheid over welke soort informatie hier precies moet worden verstrekt. Wil deze transparantieverplichting daadwerkelijk de informatieasymmetrie maximaal reduceren, moet het Voorstel preciseren welke soort informatie hier precies moet worden verstrekt.

De in de artikelen 11 tot en met 14 van het Voorstel opgenomen informatie kan in combinatie met de relevante transparantieverplichtingen in de AVG slechts ten aanzien van de aan het AI-systeem onderworpen personen een versterking uitmaken – en de informatieasymmetrie maximaal reduceren – wanneer twee voorwaarden zijn voldaan.

Vooreerst moeten de aanbieders, respectievelijk de gebruikers van het AI-systeem beschouwd worden als verwerkingsverantwoordelijken. Deze laatste zouden ervoor kunnen opteren om de informatie te verstrekken aan de aan het AI-systeem onderworpen personen wiens persoonsgegevens worden verwerkt, teneinde de naleving van zijn verplichtingen uit hoofde van de AVG te vergemakkelijken. De aan het AI-systeem onderworpen personen hebben immers geen rechtstreekse toegang tot deze informatie. Vervolgens moet het telkens gaan om AI-systemen met een hoog risico. Dergelijke informatie ontbreekt bijgevolg voor AI-systemen met een beperkt risico.

1.2.3. Informatie omtrent de risico's van de verwerking

228. Met betrekking tot dit aspect van transparantie in de procesfase, kan geen versterking worden geïdentificeerd. Het gebrek aan een algemene verplichting in de bindende tekst van de AVG om de betrokkene te informeren omtrent de risico's verbonden aan de gegevensverwerking door AI-systemen, wordt niet door het Voorstel opgevangen. Bijgevolg ontbreekt essentiële informatie omtrent de wijze waarop degene die aan het AI-systeem worden onderworpen nadelige gevolgen van het AI-systeem kunnen ondervinden (tenzij een DPIA wordt opgemaakt die eveneens gepubliceerd wordt).

1.3. Output

229. Krachtens de AVG moeten verwerkingsverantwoordelijken de betrokkene informeren over de verwachte gevolgen van de verwerking voor deze laatste. Informatie betreffende de te verwachte gevolgen, is erop gericht om de betrokkene te informeren over de mogelijke reik- en draagwijdte van het geautomatiseerd besluit.

230. In het Voorstel kon geen informatie worden geïdentificeerd die in de dimensie verklaarbaarheid zou kunnen worden opgenomen over de outputfase van de gegevensverwerking door een AI-systeem. Immers, in het Voorstel wordt geen gewag gemaakt van de specifieke gevolgen die verbonden worden aan de door het AI-systeem gegenereerde output. In dit opzicht kan bijgevolg een *status quo* worden genoteerd. De kleur oranje werd gekozen omdat deze informatie pas zal worden verstrekt als de AVG van toepassing is. Wanneer geen persoonsgegevens zouden worden verwerkt, beschikt de aan het AI-systeem onderworpen persoon over geen enkele informatie over de output.

Afdeling 2: Controle

2.1. Input

231. De AVG voorziet in een controlemechanisme in de inputfase van de gegevensverwerking door AI-systemen, namelijk de keuze om al dan niet toe te stemmen met de voorgenomen verwerking. Het Voorstel voorziet daarentegen geen (gelijkaardig) controlemechanisme, waardoor op dit punt een *status quo* ('=') wordt waargenomen. Uit de voorgaande analyse bleek daarenboven dat de doeltreffendheid van dit controlemechanisme in vraag kon worden gesteld wanneer AI-systemen persoonsgegevens verwerken, gezien de praktische moeilijkheden die in dit verband rijzen. Vandaar de kleur oranje.

2.2. Proces

232. De AVG voorziet in de procesfase verschillende controlemechanisme, namelijk een verbod, menselijke tussenkomst en het recht om bezwaar te maken. Het Voorstel voegt in dit kader eveneens een belangrijk controlemechanisme toe, met name menselijk toezicht voor AI-systemen met een hoog risico. Dit wordt beschouwd als een versterking ('v'). De controlemechanismen in de AVG en het Voorstel worden in theorie samen doeltreffend beschouwd, maar de praktische haalbaarheid van de mechanismen kan in twijfel worden getrokken. Vandaar de kleur oranje.

2.3. Output

233. In de AVG kon geen controlemechanisme worden geïdentificeerd die de betrokkene de mogelijkheid biedt om controle over zijn persoonsgegevens te behouden in de outputfase van de gegevensverwerking. In deze fase gaat het specifiek over de vraag of de betrokkene enige instrumenten in handen heeft om zich te verzetten in de outputfase (dus nadat een output werd gegenereerd) tegen de specifieke gevolgen die verbonden zijn aan de gegenereerde output. De controlemechanismen die controle toelaten over de persoonsgegevens in de inputfase en procesfase van de gegevensverwerking moeten worden aangewend.

234. In het Voorstel kon eveneens geen controlemechanisme in deze fase worden geïdentificeerd. Er kan op dit punt bijgevolg een *status quo* worden geïdentificeerd. Gezien in beide rechtsinstrumenten een controlemechanisme ontbreekt, werd voor de kleur rood geopteerd.

Hoofdstuk 3: Eindconclusie

Betekenisvolle transparantie impliceert enerzijds maximale reductie van de informatieasymmetrie in de verschillende fasen van de gegevensverwerking – mits respect voor het relationele aspect van de verklaarbaarheidsdimensie – en anderzijds doeltreffende controle over de (persoons)gegevens. Algemeen kan worden geconcludeerd dat beide rechtsinstrumenten over de verschillende fasen heen in staat zijn om de informatieasymmetrie maximaal te reduceren. Echter, daarbij wordt vastgesteld dat dit maar voorwaardelijk is. Er moeten immers steeds noodzakelijke randvoorwaarden vervuld zijn. Met betrekking tot de controlemechanismen in beide rechtsinstrumenten, wordt algemeen vastgesteld dat zij samen doeltreffende controle in theorie mogelijk maken (met uitzondering in de outputfase). De praktische haalbaarheid blijft echter twijfelachtig.

LIJST VAN FIGUREN

BIBLIOGRAFIE

Wetgeving

Richtl. EP. Raad nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *Pb.L.* 23 november 1995, afl. 281, 31.

Verord.Raad nr. (EU) 2016/679, 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb.L.* 4 mei 2016, afl. 119, 7.

Voorstel (Comm.) voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie, 21 april 2021, COM'2021) def – 2021/0106 (COD).

Preambule Verord.Raad nr. (EU) 2016/679, 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *Pb.L.* 4 mei 2016, afl. 119, 7.

Res. (EP) inzake artificiële intelligentie: kwesties betreffende de interpretatie en toepassing van het internationaal recht, voor zover dit van toepassing is op de EU, op het gebied van civiel en militair gebruik en staatsgezag buiten de werkingssfeer van het strafrecht, 20 januari 2021, 2020/2013(INI).

Concl.Raad nr. 11481/20, 21 oktober 2020 over het Handvest van de Grondrechten in de context van artificiële intelligentie en digitale verandering, https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/nl/pdf.

Rechtsleer

AHMAD, N., HAMID, M., ZAINAL, A., RAUF, M. en ADNAN, Z., "Review of Chatbots Design Techniques", *International Journal of Computer Applications* 2018, 7-10.

ALMADA, M., "Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems", *Forthcoming, 17th International Conference on Artificial Intelligence and Law* 2018, 1-10.

BALASUBRAMANIAM, N., KAUPPINEN, M., HIEKKANEN, K. en KUJALA, S., "Transparency and Explainability of AI Systems: Ethical Guidelines in Practice" in GERVASI, V. en VOGELSANG, A. (eds.), *Requirements Engineering Foundation for Software Quality*, Cham, Springer, 2022, 3-18.

BAROCAS, S. en NISSENBAUM, H., "Big Data's End Run around Anonymity and Consent" in LANE, J., STODDEN, V., BENDER, S. en NISSENBAUM, H. (eds.), *Privacy, Big Data, and the Public Good. Frameworks for Engagement*, Cambridge, Cambridge University Press, 2014, 44-75.

BARROS VALE, S. en ZANFIR-FORTUNA, G., "Automated Decision-Making Under the GDPR: Practical Cases form Courts and Data Protection Authorities", *Future of Privacy Forum* 2022, 1-60.

BAYAMLIOGLU, E., "The right to contest automated decisions under the General Data Protection Regulation: Beyond the so-called "right to explanation"", *Regulation & Governance* 2021, 1-21.

BENICHOU, B., KINDT, J. en BEUDELS, M., "Informatieverplichtingen in het gegevensbeschermingsrecht: *much ado about nothing?*" in S. VAN AGGELEN (ed.), *Informatie en recht*, Mortsel, Intersentia, 2021, 197-234.

BERTINO, E., "The Quest for Data Transparency", *IEEE Computer Society* 2020, 67-68.

BIBAL, A., LOGNOUL, M., DE STREEL, A. en FRENAY, B., "Legal requirements on explainability in machine learning", *Artificial Intelligence & Law* 2021, 149-169.

BRENNAN-MARQUEZ, K., LEVY, K. en SUSSER, D., "Strange Loops: apparent versus actual human involvement in automated decision making", *Berkely Technology Law Journal* 2019, 745-771.

BURRELL, J., "How the machine 'thinks': Understanding opacity in machine learning algorithms", *Big Data & Society* 2016, 1-12.

BUSUIOC, M., CURTIN, D. en ALMADA, M., "Reclaiming transparency: contesting the logics of secrecy within the AI Act", *European Law Open* 2022, 1-27.

CASEY, B., FARHANGI, A. en VOGL, R., "Rethinking Explainable Machines: The GDPR's Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise", *Berkely Technology Law Journal* 2019, 145-188.

CUSTERS, B. en HEIJNE, A., The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice", *Computer Law & Security Review* 2022, 1-17.

DAVIDOVIC, J., "On the purpose of meaningful human control of AI", *SSRN* 2022, 1-6.

DE BOT, D., (ed.), *De toepassing van de Algemene Verordening Gegevensbescherming in de Belgische context. Commentaar op de AVG, de Gegevensbeschermingswet en de Wet Gegevensbeschermingsautoriteit*, Mechelen, Wolters Kluwer, 2020, 1314.

DE BRUYNE, J., "Artificiële Intelligentie in 2021: veel wetgevende en beleidsinitiatieven, maar meer focus nodig op digitale geletterdheid, *De Juristenkrant* 2021, 8-9.

DE BRUYNE, J. en GILS, T., "Wat brengt de toekomst: de regulering van artificiële intelligentie" in VAN EECKE, P. (ed.), *Recht & Elektronische handel*, Mortsel, Intersentia, 2021, 581-606.

DE RAEDT, S., MARTENS, D. en BRUGHMANS, D., "Waarom krijg ik fiscale controle? Naar meer transparantie bij de geautomatiseerde besluitvorming door de fiscale overheid", *TFR* 2021, nr. 604, 607-612.

DEVILLE, R., SERGEYSSELS, N. en MIDDAG, C., "Basic Concepts of AI for Legal Scholars" in DE BRUYNE, J. en VANLEENHOVE, C. (eds.), *Artificial Intelligence and the Law*, Mortsel, Intersentia, 2021, 1-22.

DOSHI-VELEZ, F., KORTZ, M., BUDISH, R., BAVITZ, C., GERSHMAN, S., O'BRIEN, D., SCOTT, K., SHIEBER, S., WALDO, J., WEINBERGER, D., WELLER, A. en WOOD, A., "Accountability of AI Under the Law: The Role of Explanation", *Berkman Center Research Publication* 2017, 1-15.

DUROVIC, M. en WATSON, J., "Nothing to Be Happy about: Consumer Emotions and AI", *Multidisciplinary Scientific Journal* 2021, 784-793.

EBERS, M., HOCH, V., ROSENKRANZ, F., RUSCHEMEIER, H. en STEINRÖTTER, B., "The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)", *Multidisciplinary Scientific Journal* 2021, 589-603.

FELZMANN, H., VILLARONGA, E., LUTZ, C. en TAMO-LARRIEUX, A., "Transparency you can trust: transparency requirements for artificial intelligence between legal norms and contextual concerns", *Big Data & Society* 2019, 1-14.

FELZMANN, H., VILLARONGA, E., LUTZ, C. en TAMO-LARRIEUX, A., "Towards Transparency by Design for Artificial Intelligence", *Science and Engineering Ethics* 2020, 3333-3361.

FIERENS, M., VAN GOOL, E. en DE BRUYNE, J., "De regulering van artificiële intelligentie (deel 1) - Een algemene stand van zaken en een analyse van enkele vraagstukken inzake consumentenbescherming", *RW* 2021, 962-980.

FINK, M., "The EU Artificial Intelligence Act and Access to Justice", *EU Law Live* 2021, 1-4.

FLORIDI, L., "The European Legislation on AI: A Brief Analysis of Its Philosophical Approach" in MÖKANDER, J. en ZIOSI, M. (eds.), *The 2021 Yearbook of the Digital Ethics Lab*, Cham, Springer, 2022, 1-8.

GABRIELS, K., *Regels voor robots. Ethiek in tijden van AI*, Brussel, VUBPRESS, 2019, 172.

GIAKOUMOPOULOS, C., BUTTARELLI, G. en O'FLAHERTY, M., *Handboek Europese gegevensbeschermingswetgeving*, Luxemburg, Bureau voor publicaties van de Europese Unie, 2021, 466.

GREEN, B. en KAK, A.,"The False Comfort of Human Oversight as an Antidote to A.I. Harm", *Slate* 2021, 1-6.

HACKER, P., "A legal framework for AI training data – from first principles to the Artificial Intelligence Act", *Law, Innovation and Technology* 2021, 257-301.

HACKER, P. en PASSOTH, J., "Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond" in HOLZINGER, A., GOEBEL, R., FONG, R., MOON, T., MÜLLER, K. en SAMEK, W. (eds.), *xxAI – Beyond Explainable AI*, Lecture Notes in Computer Science, 2022, 343-373.

JAK, N. en BASTIAANS, S., "De betekenis van de AVG voor geautomatiseerde besluitvorming door de overheid. Een black box voor een black box", *Nederlands Juristenblad* 2018, 3018-3025.

KAMINSKI, E. en MALGIERI, G., “Multi-layered Explanations from Algorithmic Impact Assessments in the GDPR”, *International Data Privacy Law* 2020, 68-79.

KAMINSKI, E. en URBAN, J., “The right to contest AI”, *Columbia Law Review* 2021, 1957-2047.

KESA, A. en KERIKMÄE, T., “Artificial Intelligence and the GDPR: inevitable Nemeses?”, *TalTech Journal of European Studies* 2020, 67-90.

KEMPER, J. en KOLKMAN, K., “Transparent to whom? No algorithmic accountability without a critical audience”, *Information, communication & society* 2019, 2081-2096.

KISELEVA, A., “Comments on the EU Proposal for the Artificial Intelligence Act”, *VUB* 2021, 1-8.

KISELEVA, A., KOTZINOS, D. en DE HERT, P., “Transparency of AI in Healthcare as a Multilayered System of Accountabilities: Between Legal Requirements and Technical Limitations”, *Frontiers in Artificial Intelligence* 2022, 1-21.

KOSTA, E. en CUIJPERS, C., “The Draft Data Protection Regulation and the Development of Data Processing Applications”, *IFIP Advances in Information and Communication Technology* 2014, 12-32.

KOIVISTO, I., *Thinking Inside the Box: The Promise and Boundaries of Transparency in Automated Decision-Making*, San Domenico di Fiesole, European University Institute, 2020, 1-22.

KOULU, R., “Proceduralizing control and discretion: Human oversight in artificial intelligence policy”, *Maastricht Journal of European and Comparative Law* 2020, 720-735.

LARSSON, S. en HEINTZ, F., “Transparency in artificial intelligence”, *Internet Policy Review* 2020, 1-16.

LAUX, J., “Institutionalised Distrust and Human Oversight of Artificial Intelligence: Toward a Democratic Design of AI Governance under the European Union AI Act”, *Oxford Internet Institute* 2023, 1-30.

LAWSON-HETCHELY, C., The Potential Impact of the Future AI Act on the GDPR, onuitg. masterproef rechten University of Oslo, 2022, 31.

LAZCOZ, G. en DE HERT, P., "Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities", *Brussels Privacy Hub* 2022, 1-31.

MALGIERI, G., "Automated decision-making in the EU Member States: The right to an explanation and other "suitable safeguards" in the national legislations", *Computer Law & Security Review 2019,* 1-26.

MALGIERI, G. en COMANDÉ, G., "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", *International Data Privacy Law* 2017, 1-36.

MENDOZA, I. en BYGRAVE, L., "The Right Not te be Subject to Automated Decisions Based on Profiling" in SYNODINOU, T., JOUGLEUX, P., MARKOU, C. en PRASTITOU, T. (eds.), *EU Internet Law. Regulation and Enforcement*, Cham, Springer, 2017, 77-98.

MENGES, F., LATZO, T., VIELBERTH, M., SOBOLA, S., PÖHLS, H., TAUBMANN, B., KÖSTLER, J., PUCHTA, A., FREILING, F., REISER, H. en PERNUL, G., "Towards GDPR-compliant data processing in modern SIEM systems", *Computers & Security* 2021, 1-19.

MESARÍC, M., SOLÁROVÁ, S., PODROUZEK, J. en BIELIKOVA, M., "Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence – Artificial Intelligence act", Kempele Institute of Intelligent Technologies 2021, 1-16.

MITROU, L., *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection (GDPR) 'Artificial Intelligence-Proof'?,* Athene, University of Economics and Business, 2018, 90.

MLADENOV, M., "Human vs. Artificial Intelligence – EU's legal response", *LAW – theory and practice* 2023, 32-43.

NEUWIRTH, R., "Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)", *Computer Law & Security Review* 2023, 1-14.

PALMIOTTO, F., "The Black Box on Trial: The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings" in M. EBERS en M. CANTERO GAMITO (eds.), *Algorithmic Governance and Governance of Algorithms,* Zwitserland, Springer, 2021, 49-70.

RAMOSAJ, B. en BERISHA, G., "Systems Theory and Systems Approach to Leadership", *ILIRIA International Review* 2014, 59-76.

RAPOSO, V., "Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence", *International Journal of Law and Information Technology* 2022, 88-109.

ROIG, A., "Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR)", *European Journal of Law and Technology* 2017, 1-17.

RUBIN, V., BURKELL, J., CORNWELL, S., ASUBIARO, T., CHEN, Y., POTTS, D. en BROGLY, C., "AI Opaqueness: What Makes AI Systems More Transparent?", *Proceedings of the Annual Conference of CAIS* 2020, 1-6.

SCHERMER, B., CUSTERS, B. en VAN DER HOF, S., "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection", *Ethics Inf Technol* 2014, 171-182.

SCHLEHAHN, E. en WENNING, R., "GDPR Transparency Requirements and Data Privacy Vocabularies" in KOSTA, E., PIERSON, J., SLAMANIG, D., HÜBNER, S. en KRENN, S. (eds.), *Privacy and Identity Management. Fairness, Accountability and Transparency in the Age of Big Data*, Cham, Springer, 2018, 95-113.

SELBST, A. en POWLES, J., "Meaningful information and the right to explanation", *International data Privacy Law* 2017, 233-242.

SMELTING, G., *Geautomatiseerde besluitvorming: van human in-the-loop naar human out-the-loop*, onuitg. masterproef Rechten UvA, 2020, https://scripties.uba.uva.nl/download?fid=c2025980, 41.

SMITS, J., "What is Legal Doctrine? On The Aims and Methods of Legal-Dogmatic Research" in VAN GESTEL, R., MICKLITZ, H. en RUBIN, E. (eds.), *Rethinking Legal Scholarship: A Transatlantic Dialogue*, New York, Cambridge University Press, 2017, 207-228.

SMUHA, N., "Beyond a Human rights-based approach to AI Governance: Promise, Pitfalls, Plea", *Philosophy & Technology* 2020, 1-14.

SMUHA, N., "From a 'Race to AI' to a 'Race to AI regulation': Regulatory Competition for Artificial Intelligence", *Law, Innovation & Technology* 2021, 1-26.

SMUHA, N., AHMED-RENGERS, E., HARKENS, A., LI, W., MACLAREN, J., PISELLI, R. en YEUNG, K., "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", *LEADS Lab* 2021, 1-59

SOVRANO, F., SAPIENZA, S., PALMIRANI, M. en VITALI, F., "Metrics, Explainability and the European AI Act Proposal", *Multidisciplinary Scientific Journal* 2022, 126-138.

THIRUMURUGANATHAN, S., MAYURESH, K., OUZZANI, M. en CHAWLA, S., "Automated Annotations for AI Data and Model Transparency", *Qatar Computing Research Institute* 2021, 1-9.

TIMAN, T. en GROMME, F., "Wat is rechtvaardige AI? Een kader voor het ontwikkelen en toepassen van algoritmes voor automatische besluitvorming", *Beleid en Maatschappij* 2020, 425-438.

URBAN, T., TATANG, D., DEGELING, M., HOLZ, T. en POHLMANN, N., The Unwanted Sharing Economy: An Analysis of Cookie Syncing and User Transparency under the GDPR", *Cornell University* 2018, 1-26.

VAN DE WAERDT, P., "Information asymmetries: recognizing the limits of the GDPR on the data-driven market", *Computer Law & Security Review* 2020, 1-18.

VAN HOBOKEN, J., "The Privacy Disconnect" in R. JØRGENSEN (ed.), *Human Rights in the Age of Platforms*, Cambridge, The MIT Press, 2019, 255-284.

VAROSANEC, I., "On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI", *International Review of Law, Computers & Technology* 2022, 95- 117.

VEALE, M. en EDWARDS, L., "Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling", *Computer Law & Security Review* 2018, 398-404.

VEALE, M. en ZUIDERVEEN BORGESIUS, F., "Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach", *Computer Law Review International* 2021, 97-112.

WACHTER, S., MITTELSTADT, B. en FLORIDI, L., "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation", *International Data Privacy Law* 2017, 76-99.

WACHTER, S., MITTELSTADT, B. en RUSSEL, C., "Counterfactual explanations without opening the black box: automated decisions and the GDPR", *Harvard Journal of Law & Technology* 2018, 842-887.

WALLACE, N. en CASTRO, D., "The Impact of the EU's New Data Protection Regulation on AI", *Center for Data Innovation* 2018, 1-37.

WALMSLEY, J., "Artificial Intelligence and the value of transparency", *AI & society* 2021, 585-595.

WOLTERS, P., "De rechten van de betrokkene onder de AVG", *Tijdschrift voor Consumentenrecht en handelspraktijken* 2018, 130-140.

ZARSKY, T., "Transparent Predictions", *University of Illinois Law Review* 2013, 1503-1569.

Onlinebronnen

A Civil Society Statement, An EU Artificial Intelligence Act for Fundamental Rights, 30 november 2021, https://www.accessnow.org/cms/assets/uploads/2021/11/joint-statement-EU-AIA.pdf.

AUTORITEIT PERSOONSGEGEVENS (AP), *Toezicht op AI & Algortimes*, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezicht_op_ai_en_algoritmes.pdf.

AWS. What is data labeling for machine learning? *AWS*. Geraadpleegd op 3 oktober 2022, van https://aws.amazon.com/sagemaker/data-labeling/what-is-data-labeling/#:~:text=In%20machine%20learning%2C%20data%20labeling,model%20can%20learn%20from%20it

BARROS VALE, S., "GDPR and the AI Act interplay: lessons from FPF's ADM case-law report", Future of Privacy Forum 2022 (blog), https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/.

Europese Commissie, *Regulatory framework proposal on artificial intelligence*, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (consultatie 6 maart 2023).

GILS, T., WAUTERS, E., BENICHOU, B., DE BRUYNE J. en VALCKE, P., "Artificiële Intelligentie en gegevensbescherming: een verkennende gids", *Kenniscentrum Data en Maatschappij*, 2020, https://data-en-maatschappij.ai/publicaties/ai-en-gegevensbescherming-een-verkennende-gids.

Kenniscentrum Data & Maatschappij. (z.d.). *Artificial Intelligence*. Geraadpleegd op 23 augustus 2022, van https://data-en-maatschappij.ai/woordenlijst#artificial-intelligence.

KISELEVA, A., "Making AI's Transparency Transparent: notes on the EU Proposal", European Law Blog 2021 (blog), https://europeanlawblog.eu/2021/07/29/making-ais-transparency-transparent-notes-on-the-eu-proposal-for-the-ai-act/.

Scholarpedia. (z.d.). *Chinese room argument*. Geraadpleegd op 28 september 2022, van http://www.scholarpedia.org/article/Chinese_room_argument.

Van Zwol, T. (2017, 22 oktober). Kunstmatige intelligentie: omarmen of wantrouwen? *Scientias*. Geraadpleegd op 29 september 2022, van https://scientias.nl/kunstmatige-intelligentie-omarmen-wantrouwen/.

Overige bronnen

BAQAIS, A., BAIG, Z. en GROBLER, M., "Transparency and Opacity in AI Systems: An Overview", Interaction Design for explainable AI", 12-15.

BODEN, M., *Its Nature and Future*, Oxford, Oxford University Press, 2016, 197.

BUYSE, T., "Frankenstein de baas blijven. Artificiële intelligentie in Vlaanderen", Gids op Maatschappelijk Gebied, 2021, 46-54.

COECKELBERGH, M., *AI Ethics*, Cambridge, The MIT Press, 2020, 229.

COPELAND, B.J., *The Essential Turing. Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life plus The Secrets of Enigma*, New York, Oxford University Press, 2004, 613.

DE KETELAERE, G.M., *Mens versus machine*, Kalmthout, Pelckmans, 2020, 204.

DE PRETER, W., SERRURE, B. en LEGRAND, R., "De techtrends van 2023:iPhone-moment breekt aan voor AI", De Tijd 27 december 2022, https://www.tijd.be/dossiers/de-vooruitblik/de-techtrends-van-2023-iphone-moment-breekt-aan-voor-ai/10437322.html.

DE SMEDT, S., "'Vragen hoe slim ChatGPT is, is als vragen hoe sportief mijn stofzuiger is'", De Tijd, 10 maart 2023, https://www.tijd.be/content/tijd/nl/mme-articles/10/45/32/33/10453233.

EUROPEAN DATA PROTECTION BOARD (EDPB), *Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679,* 4 mei 2020, versie 1.1, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_nl.pdf.

EUROPEAN DATA PROTECTION BOARD – EUROPEAN DATA PROTECTION SUPERVISOR (EDPB-EDPS), *Gezamenlijk advies over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie)*, 18 juni 2021, nr. 5/2021, https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_nl.pdf.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights*, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf.

GEGEVENSBESCHERMINGSAUTORITEIT (GBA), *Aanbeveling betreffende de verwerking van persoonsgegevens voor direct marketingdoeleinden*, 17 januari 2020, nr. 01/2020, https://www.gegevensbeschermingsautoriteit.be/publications/aanbeveling-nr.-01-2020.pdf.

GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt in de zin van Verordening 2016/679*, 4 april 2017, WP248rev.01, https://ec.europa.eu/newsroom/article29/items/611236.

GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679*, 3 oktober 2017, WP251rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp251rev01_nl.pdf.

GROEP GEGEVENSBESCHERMING ARTIKEL 29, *Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679*, 11 april 2018, WP260rev.01, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp260rev01_nl.pdf.

HAZENBERG, J., *Technologie de baas*, Amsterdam, Spectrum, 2019, 253.

ILKOU, E. en KOUTRAKI, M., "Symbolic Vs Sub-symbolic AI Methods: Friends or Enemies?", CEUR WS 2020, 1-7.

JANSEN, P., BROADHEAD, S., RODRIGUES, R., WRIGHT, D. BREY, P., FOX A. en WANG, N., "State of the art review", 2018. Draft of the D4.1 deliverable submitted to the European Commission on April 13, 2018. A report for The SIENNA Project, an EU H2020 research and innovation program under grant agreement no. 741716.

KIM, P., *MATLAB Deep Learning*, Seoul, Apress, 2017, xvii + 162.

LAUWAERT, L., *Wij, Robots*, Tielt, Lannoo Campus, 2021, 305.

LEGRAND, R., "Overheden moeten zich sneller voorbereiden op de bedreigingen van AI", De Tijd, 7 maart 2023, https://www.tijd.be/ondernemen/technologie/cisco-topman-overheden-moeten-zich-sneller-voorbereiden-op-bedreigingen-van-ai/10451824.html.

MARNAU, N., "Stakeholders' Consultation. Comments on the "Draft Ethics Guidelines for Trustworthy AI" by the High-Level Expert Group on Artificial Intelligence", *Helmholtz Center For Information Security* 2019, 1-3.

Mededeling (Comm.) van de Commissie aan het Europees Parlement, de Europese Raad, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de regio's betreffende Kunstmatige Intelligentie voor Europa, 25 april 2018, COM(2018)237.

MUELLER, J. P. en MASSARON, L., *Kunstmatige intelligentie voor dummies*, Amersfoort, BBNC uitgevers, 2018, 347.

PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (STOA), *Tackling deepfakes in European policy*, juli 2021,

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf.

PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY (STOA), *Regulatory divergences in the draft AI act – Differences in public and private sector obligations*, mei 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU(2022)729507_EN.pdf.

SCIENTIFIC FORESIGHT UNIT (STOA), *Artificial intelligence: How does it work, why does it matter, and what can we do about it?, juni 2020*, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf.

SCIENTIFIC FORESIGHT UNIT (STOA), The impact of the General Protection Regulation (GDPR) on *artificial intelligence, juni 2020*, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

SEARLE, J., "Minds, Brains and Programs", The Behavioral and Brain Sciences 1980, 417-424.

SERRURE, B., "Microsoft profiteert mee van AI-hype", De Tijd, 26 april 2023, https://www.tijd.be/ondernemen/technologie/microsoft-profiteert-mee-van-ai-hype/10463654.html.

SNAPHAAN, T. en HARDYNS, W., "Artificiële Intelligentie en big data in het veiligheidsdomein", *Veiligheidsnieuws* 2021, 1- 9.

STEELS, L. (ed.), *Artificiële intelligentie. Naar een vierde industriële revolutie?,* Brussel, KVAB Press, 2017, 43.

THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE, A Definition of AI: *Main capabilities and scientific disciplines*, 18 december 2018, https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf.

THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (HLEG AI), *Ethische Richtsnoeren voor Betrouwbare KI,* 8 april 2019, https://op.europa.eu/nl/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1#.

The European Consumer Organisation (BEUC), *Regulating AI to protect the consumer,* Bureau Européen des Unions de Consommateurs AISBL, 2021, https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf.

TIELENBURG, D., *The 'Dark Sides' of Transparency: Rethinking Information Disclosure as a Social Praxis*, onuitg. masterproef Filosofie Universiteit Utrecht, 2018, 57.

URSIN, F., TIMMERMANN, C., ORZECHOWSKI, M. en STEGER, F., "Diagnostic Diabetic Retinopathy With Artificial Intelligence: What Information Should Be Included to Ensure Ethical Informed Consent?", *Frontiers in Medicine* 2021, 1-6.

VALCKE, P. en ROSSELLO, S., "The artificial lawyer. Reflecties over de impact van AI op het recht en de rechtspraktijk" in DE BRUYNE, J. en BOUTECA, N. (eds.), *Artificiële intelligentie en maatschappij*, Oud-Turnhout, Gompel&Svacina, 2021, 175-206.

VAN BIESEN, W., VEYS, N., DECRUYENAERE, J., PELEMAN, R. en STERCKX, S., "Hoe artificiële intelligentie, digitalisering en big data ons kunnen helpen bij verantwoordbare zorg", *tvgg* 2021, 1-16.

WANG , W. en SIAU, K., "Artificial Intelligence, Machine Learning, Automation, Robotics, Future of of Work and Future of Humanity: A Review and Research Agenda", Journal of Database Management 2019, 61- 79.

BIJLAGEN

BIJLAGE A. Ingevuld transparantiekader - Algemene Verordening Gegevensbescherming

	Input (data)	Proces (AI)	Output (resultaat)
Verklaarbaarheid	- Informatie omtrent de betrokken categorieën van persoonsgegevens die werden verzameld o Art. 14, lid 1, d) o Art. 15, lid 1, b) o Overw. 39 + 58 - Informatie omtrent de kwaliteit van de aangeleverde data(sets) o Art. 5, lid 1, d) o Art. 5, lid 2 o Art. 25 o Overw. 71	- Informatie omtrent het bestaan van geautomatiseerde besluitvorming o Art. 13, lid 2, f) o Art. 14, lid 2, g) o Art. 15, lid 1, h) - Informatie omtrent de conversie door het AI-systeem van een input tot een output o Art. 13, lid 2, f) o Art. 14, lid 2, g) o Art. 15, lid 1, h) - Informatie omtrent de risico's van de verwerking o Art. 35 o Overw. 39	- Informatie omtrent te verstrekken over de verwachte gevolgen o Art. 13, lid 2, f) o Art. 14, lid 2, g) o Art. 15, lid 1, h)
Controle	- Grondslag rechtmatige verwerking: toestemming o Art. 6	- Recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit o Art. 22, lid 1 - Beschermingsmaatregelen indien uitzondering op verbod art. 22 AVG o Art. 22, lid 3	

Artikel 12 AVG bepaalt in dit kader de kwaliteit van de informatieverstrekking en communicatie
- Duidelijke en eenvoudige taal
- Gemakkelijk toegankelijk
- Beknopt, transparant en begrijpelijk

Artikel 12 AVG bepaalt eveneens:
- Het kosteloos karakter van informatieverstrekking
- Manier van informatieverstrekking

BIJLAGE B. Ingevuld transparantiekader - Voorstel voor een Verordening betreffende Artificiële Intelligentie

	Input (data)	Proces (AI)	Output (resultaat)
Verklaarbaarheid	- Informatie omtrent de betrokken categorieën van gegevens die werden verzameld (ontwikkelingsfase) o Art. 11 (+ bijlage IV, lid 2, d) - Informatie omtrent de kwaliteit van de aangeleverde datasets (ontwikkelingsfase) o Art. 10 o Art. 11 (+ bijlage IV, lid 2, g) o Art. 13, lid 3, b), v)	- Informatie omtrent het gebruik van AI-systemen o Art. 52, lid 1 o Art. 52, lid 3 - Informatie omtrent de conversie door het AI-systeem van een input tot een output o Art. 11 (+ bijlage IV, lid 2, b) o Art. 12 o Art. 13 o Art. 14 o Art. 52, lid 2 - Informatie omtrent de risico's van het gebruik van AI-systemen o Overw. 47	
Controle		- Menselijk toezicht o Art. 14	