Kenniscentrum
Data & Maatschappij

ETHISCHE PRINCIPES EN (NIET-)BESTAANDE JURIDISCHE REGELS VOOR AI.

Een praktische gids.

Kenniscentrum
Data & Maatschappij

DECEMBER 2020

Deze gids citeren als:

Vranckaert, K., De Bruyne, J., Gils, T., Wauters, E., Bénichou, B. & Valcke, P. (oktober 2020). Ethische principes en (niet-)bestaande juridische regels voor AI. Een praktische gids. Kenniscentrum Data & Maatschappij, Brussel, België.

www.data-en-maatschappij.ai

Inhoudstafel

Algemene toelichting

Algemene toelichting

Context Gids – De Europese Commissie (EC) baseert haar AI-strategie op drie pijlers: (i) investering in onderzoek om de capaciteit en het gebruik van AI te bevorderen, (ii) een voorbereiding op de socio-economische veranderingen, en (iii) de ontwikkeling van een passend ethisch en juridisch kader dat aansluit op de waarden van de Europese Unie (EU).

Wat betreft het derde punt zijn de werkzaamheden van de in juni 2018 opgerichte Deskundigengroep inzake Kunstmatige Intelligentie (High-Level Expert Group on Artificial Intelligence – AI HLEG) van groot belang. In april 2019 publiceerde de AI HLEG de Ethische Richtsnoeren voor Betrouwbare AI. Het document bevat een aantal aanbevelingen voor het ontwikkelen van betrouwbare AI (Trustworthy AI). Een betrouwbaar AI-systeem leeft alle toepasselijke regelgeving na, handelt in overeenstemming met ethische waarden/principes en is robuust (zowel vanuit een sociaal als technisch perspectief). De Richtsnoeren bevatten zeven ethische eisen waaraan AI-systemen moeten voldoen om betrouwbaar te zijn:

- menselijke controle en menselijk toezicht;
- technische robuustheid en veiligheid;
- privacy en databeheer;
- transparantie;
- diversiteit, non-discriminatie en rechtvaardigheid;
- maatschappelijk en milieuwelzijn; en
- verantwoording.

ALTAI Beoordelingslijst – Deze Ethische Richtsnoeren zijn geen geldend recht. Ze geven louter een aanwijzing over hoe AI ethisch kan worden ontworpen, ontwikkeld en gebruikt (soft law). Toch kan best zoveel mogelijk rekening worden gehouden met deze vereisten en ervoor worden gezorgd dat AI-systemen conform deze principes worden ontwikkeld. Hoe deze Ethische Richtsnoeren kunnen worden nageleefd, is echter niet altijd duidelijk en/of eenvoudig. Om een en ander te vereenvoudigen, werd bij de Ethische Richtsnoeren daarom recent een Beoordelingslijst (Assessment List for Trustworthy AI – ALTAI) toegevoegd. Deze lijst bevat een aantal heel concrete vragen om te beoordelen of een bepaalde ethische vereiste wordt nageleefd.

Opbouw gids – Met deze gids wil het Kenniscentrum Data en Maatschappij nagaan in welke mate de vragen in de ALTAI Beoordelingslijst al een vertaling vinden in het bestaande wetgevende kader en of er bepaalde relevante regels zijn die aansluiten bij de ethische vereisten. Meteen geven we ook aan waar nog ruimte is voor verduidelijking, aanvulling of verfijning. Daarom gaan we in de volgende delen dieper in op elk van de zeven ethische vereisten, aan de hand van de volgende vragen:

- Wat betekent de ethische vereiste?
- Welke regels vormen reeds een vertaling van de ethische vereiste of kunnen dienen als inspiratiebron voor het aannemen van (bijkomende) regels over de vereiste?
- Waar zitten mogelijke punten van verbetering en/of aandachtspunten?
- Welke tools zijn er al/kunnen worden gebruikt om aan de ethische vereiste te voldoen?

Doel gids – De inhoud van deze gids wordt in een interactieve webpagina gegoten, met andere woorden in een soort van toegankelijke online encyclopedie: de WIKAIPEDAI. Deze gids dient als basis/kapstok voor bijkomende acties (cf. werkwijze Gids AI en AVG en bijhorende fiches). De webpagina die door het KDM zal worden aangeboden zal de structuur van deze gids volgen, met telkens een onderverdeling per ethische vereiste (eerste laag) en daaronder bijhorende uitklapmogelijkheden per vraag zoals deze hierboven werden gegeven (tweede laag).

Het doel van deze gids en de interactieve website is drievoudig. Ten eerste willen we een overzicht geven van de toepasselijke ethische vereisten met een beknopte inhoudelijke omkadering en duiding. We identificeren daarbij ook de relevante wetgeving. We analyseren deze niet tot in detail, maar geven de essentie weer en integreren hyperlinks naar de vindplaats. Ten tweede willen we voor elke ethische vereiste een aantal leemtes identificeren en enkele aanbevelingen voor beleidsmakers formuleren. Op basis hiervan kunnen in de toekomst dan gerichte(re) acties worden ondernomen. Ten derde is het de bedoeling om opnieuw een levend document (working document) te ontwikkelen, waarin de informatie op regelmatige tijdstippen zal worden geactualiseerd en waarop stakeholders steeds feedback of aanbevelingen kunnen geven.

Totstandkoming gids – Deze gids kwam tot stand door middel van overleg met en input door belanghebbenden en met steun van het Vlaams Departement Economie, Wetenschap & Innovatie (EWI). Na intern overleg werd een algemeen overzicht van de ethische vereisten opgesteld. Dit werd aan de belanghebbenden bezorgd voor feedback. Onderzoekers aan het KU Leuven Centre for IT & IP Law (CiTiP) zijn verantwoordelijk voor de coördinatie van deze gids. De betrokken stakeholders en het onderzoeksluik van het Vlaams AI-plan kregen ook de mogelijkheid om feedback te geven op een draft versie van deze gids. Bijkomende feedback, aanvullingen, vragen en input op/over deze gids kan te alle tijden aan hun worden overgemaakt.

Over het KDM – Het Kenniscentrum Data & Maatschappij is een samenwerking tussen drie universitaire onderzoeksgroepen: imec-SMIT-VUB, KU Leuven CiTiP en imec-MICT-UGent. Het maakt deel uit van het Vlaams Beleidsplan Artificiële Intelligentie en krijgt steun van de Vlaamse overheid (EWI). Het KDM is de centrale hub voor de juridische, maatschappelijke en ethische aspecten van data-gedreven applicaties en AI-toepassingen. Het KDM wenst bij te dragen aan het debat en het creëren van een maatschappelijk draagvlak voor AI en data-gedreven toepassingen. De door het KDM verschafte informatie, zoals deze gids, is algemeen en kan niet beschouwd worden als individueel juridisch advies. Ze kan niet worden gebruikt ter vervanging van advies door een juridisch expert. Hoewel het KDM ernaar streeft om onze documenten correct en accuraat op te stellen, is het mogelijk dat de daarin vervatte positie niet toepasbaar is op uw specifieke situatie, niet volledig, juist of actueel is, of niet overeenkomt met de positie die een rechtbank of toezichthoudende autoriteit zou kunnen innemen. Het KDM draagt dan ook geen enkele verantwoordelijkheid voor de naleving van de toepasselijke wettelijke voorschriften door een organisatie.

Hoofdstuk 1: Ethische vereiste 1 - menselijke controle en menselijk toezicht

1. Ethische vereiste 1: menselijke controle en menselijk toezicht

1.1. Wat betekent de ethische vereiste?

Met deze eerste ethische vereiste wordt gedoeld op het feit dat AI-systemen de **menselijke autonomie** en het **menselijk beslissingsproces moeten ondersteunen**, zoals volgt uit het beginsel van respect voor de menselijke autonomie. Daarvoor is het nodig dat AI-systemen zowel een democratische en gelijkwaardige samenleving mogelijk maken door de gebruikersautonomie te garanderen, als fundamentele rechten respecteren, wat dient te worden afgedwongen door middel van menselijk toezicht.

Onder deze vereiste worden AI-systemen beoordeeld op basis van **twee sub-componenten**, namelijk de mate waarin zij de (1) menselijke autonomie respecteren en (2) menselijk toezicht toelaten.

Menselijke autonomie behandelt het effect dat AI-systemen kunnen hebben op menselijk gedrag in de breedste zin van het woord. Het omvat de effecten van AI-systemen die gericht zijn op het sturen, beïnvloeden of ondersteunen van personen in hun besluitvormingsprocessen zoals algoritmische beslissingsondersteunende systemen, risicoanalyse/voorspellingssystemen (bv. recommender systems, predictive policing, financial risk analysis). Het omvat ook het effect op de menselijke perceptie en de verwachtingen wanneer men geconfronteerd wordt met AI-systemen die 'handelen' zoals mensen. Tot slot behandelt dit deelvereiste het effect van AI-systemen op menselijke affectie, vertrouwen en (on) afhankelijkheid.

De vereiste van **menselijk toezicht** helpt om zelf de vereiste toezichtsmechanismen te beoordelen. Dergelijk toezicht kan worden verwezenlijkt via beheersmechanismen, zoals een benadering met human-in-the-loop (HITL), human-on-the-loop (HOTL) of human-in-command (HIC).

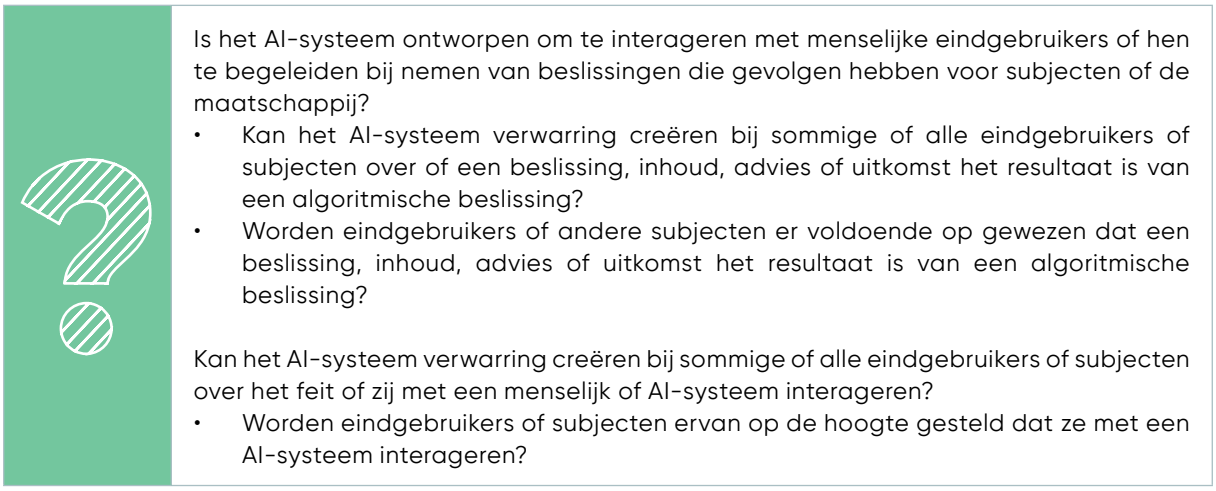
- HITL verwijst naar de mogelijkheid tot menselijke interventie in elke besluitcyclus van het systeem.
- HOTL verwijst naar de mogelijkheid tot menselijke interventie gedurende de ontwerpcyclus van het systeem en het monitoren van de werking van het systeem.
- HIC verwijst naar de mogelijkheid om de algemene werking van het AI-systeem te overzien (inclusief de ruimere economische, maatschappelijke, juridische en ethische impact) en de mogelijkheid om te kiezen wanneer en hoe het systeem in een specifieke situatie wordt gebruikt. Daarbij kan het bijvoorbeeld gaan om de keuze om een AI-systeem in een bepaalde situatie niet te gebruiken, om een bepaald niveau van menselijke beoordelingsvrijheid te garanderen tijdens het gebruik van het systeem of om te garanderen dat een door het AI-systeem genomen beslissing kan worden herroepen.

Hou hierbij rekening met het feit dat, afhankelijk van het toepassingsgebied van het AI-systeem en het potentiële risico, er **meer of minder verregaande toezichtmechanismen** nodig kunnen zijn om andere veiligheids- en controlemaatregelen te ondersteunen. Indien alle andere omstandigheden gelijk blijven, moet een AI-systeem uitgebreider worden getest en kunnen er best strengere beheers-mechanismen worden geïmplementeerd naarmate er minder menselijk toezicht op het systeem mogelijk is.

1.2. Welke regels zijn een uitdrukking van de ethische vereiste of kunnen dienen als inspiratiebron?

De ALTAI lijst voorziet per aangehaald element verschillende vragen. We geven hieronder een overzicht van de vragen per sub-component en de wetgeving die reeds een uitdrukking vormt van deze vragen of kan worden gebruikt als inspiratie.

1.2.A. Menselijke autonomie



Is het AI-systeem ontworpen om te interageren met menselijke eindgebruikers of hen te begeleiden bij nemen van beslissingen die gevolgen hebben voor subjecten of de maatschappij?

- Kan het AI-systeem verwarring creëren bij sommige of alle eindgebruikers of subjecten over of een beslissing, inhoud, advies of uitkomst het resultaat is van een algoritmische beslissing?
- Worden eindgebruikers of andere subjecten er voldoende op gewezen dat een beslissing, inhoud, advies of uitkomst het resultaat is van een algoritmische beslissing?

Kan het AI-systeem verwarring creëren bij sommige of alle eindgebruikers of subjecten over het feit of zij met een menselijk of AI-systeem interageren?

- Worden eindgebruikers of subjecten ervan op de hoogte gesteld dat ze met een AI-systeem interageren?

GEGEVENSBESCHERMING

Onder art. 13 en 14 van de Algemene Verordening Gegevensbescherming (AVG) moeten verwerkingsverantwoordelijken bepaalde informatie meedelen aan de personen van wie zij de persoonsgegevens verwerken. Indien er sprake is van **geautomatiseerde besluitvorming of profilering** moet het bestaan daarvan worden erkend en moet er nuttige informatie verstrekt worden over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Het spiegelbeeld hiervan is art. 22 AVG dat verwerkingsverantwoordelijken verplicht om betrokkenen ten minste volgende **rechten te verlenen**: het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, het recht om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten. Om betrokkenen werkelijk en voldoende in staat te stellen om dergelijke automatische beslissing aan te vechten, kan het vereist zijn dat zij geïnformeerd worden over het feit dat de beslissing gegeneerd werd door een AI-systeem en/of dat zij interageerden met dergelijk systeem.

Meer informatie kan hierover worden gevonden in het deel over "Hoofdstuk 4: Ethische vereiste 4 - transparantie".

CONSUMENTENRECHT

Ook in het consumentrecht bestaan er **informatieverplichtingen** die er nu reeds kunnen toe leiden dat de verkopers van AI-systemen de eindgebruikers moeten informeren omtrent het feit dat een beslissing of uitkomst het resultaat is van een algoritmische beslissing of dat zij interageren met een AI-systeem.

Zo moet onder de algemene informatieverplichting in artikel VI.2 Wetboek Economisch Recht

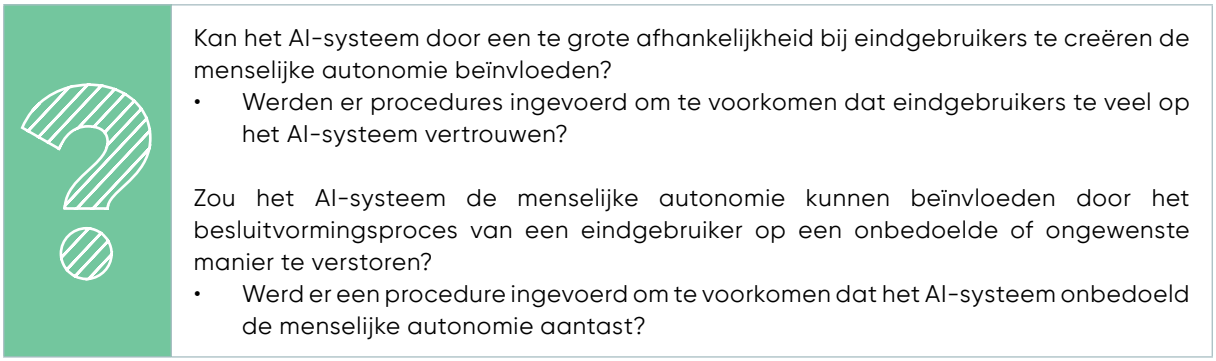
(WER) de consument geïnformeerd worden omtrent de **voornaamste kenmerken** van de producten, desgevallend, de **functionaliteit** van digitale inhoud (met inbegrip van toepasselijke technische beveiligingsvoorzieningen) en de relevante **interoperabiliteit** van digitale inhoud met hardware en software en andere diensten waarvan de onderneming op de hoogte is of redelijkerwijs kan worden verondersteld op de hoogte te zijn. Gelijkaardige bepalingen breiden dit ook uit naar diensten (artikels VI.45 en VI.64 WER) en financiële diensten (artikel VI. 55 WER).

ALGEMEEN VERBINTENISSENRECHT

Indien een eindgebruiker of consument niet afdoende werd geïnformeerd omtrent het feit dat een beslissing of uitkomst het resultaat is van een algoritmische beslissing of dat zij interageren met een AI-systeem én het AI-systeem wordt gebruikt in een situatie waarbij er een contract wordt gesloten, kan het zijn dat dit leidt tot **dwaling** in hoofde van de gebruiker of consument (art. 1110 BW).

Dwaling is een wilsgebrek waardoor er, in principe, geen geldige overeenkomst wordt gevormd. In essentie komt dwaling erop neer dat een contractpartij er een verkeerde voorstelling van de werkelijkheid heeft op nagehouden op het ogenblik van de contractsluiting. Verder moet het ook gaan om een 'substantiële dwaling', wat wil zeggen dat het contract zonder die dwaling niet zou zijn gesloten. Eenvoudige illustratie: stel dat iemand een kunstwerk bestelt bij een online dienst die kunstwerken aanbiedt van een bekende kunstenaar (bv. Rinus Van De Velde), waarbij in praktijk deze kunstwerken gegenereerd worden door een AI-systeem. Indien de koper erop vertrouwt dat deze kunstwerken gemaakt worden door de kunstenaar zelf en daarom een schilderij bestelt, zal die zich op dwaling kunnen beroepen indien die er later op uitkomt dat zijn/haar schilderij blijkt door een AI-systeem te zijn gemaakt.

Dergelijke dwaling moet wel 'verschoonbaar' zijn. Deze vereiste houdt in dat een redelijk persoon in gelijkaardige omstandigheden ook zou hebben gedwaald. Toegepast op bovenstaande illustratie, betekent dit dat de koper niet zou hebben kunnen opmaken uit de door de dienstverlener verschafte informatie, noch op basis van eventueel eigen onderzoek, dat de kunstwerken AI-creaties waren en geen authentieke creaties.



Kan het AI-systeem door een te grote afhankelijkheid bij eindgebruikers te creëren de menselijke autonomie beïnvloeden?

- Werden er procedures ingevoerd om te voorkomen dat eindgebruikers te veel op het AI-systeem vertrouwen?

Zou het AI-systeem de menselijke autonomie kunnen beïnvloeden door het besluitvormingsproces van een eindgebruiker op een onbedoelde of ongewenste manier te verstoren?

- Werd er een procedure ingevoerd om te voorkomen dat het AI-systeem onbedoeld de menselijke autonomie aantast?

CONSUMENTENRECHT

In deze context kan er op worden gewezen dat het consumentenrecht zogenaamde **oneerlijke misleidende praktijken** verbiedt (art. VI.97-100 WER). Een handelspraktijk wordt als misleidend beschouwd als die op onwaarheden berust of, zelfs als de informatie feitelijk correct is, de gemiddelde consument op enigerlei wijze, inclusief door de algemene presentatie, bedriegt of kan bedriegen met betrekking tot bepaalde elementen en de gemiddelde consument er zowel in het ene als in het andere geval toe brengt of kan brengen een besluit over een transactie te nemen dat hij anders niet had genomen. De elementen waaromtrent bedrieglijke informatie kan worden verschaft, zijn o.a.:

- het bestaan of de aard van het product;
- de voornaamste kenmerken van het product (incl. risico's, samenstelling, geschiktheid voor het gebruik, gebruiksmogelijkheden,…)

Verder kan er ook sprake zijn van **misleidende omissies**. Dit is het geval indien er – samengevat - essentiële informatie welke de gemiddelde consument, naargelang de context, nodig heeft om een geïnformeerd besluit over een transactie te nemen, weg wordt gelaten en die de gemiddelde consument er toe brengt of kan brengen een besluit over een transactie te nemen dat hij anders niet had genomen. Hier is eveneens sprake van indien de essentiële informatie op onduidelijke, onbegrijpelijke of dubbelzinnige wijze dan wel laattijdig werd verstrekt, of het commerciële oogmerk, indien dit niet reeds duidelijk uit de context blijkt, niet werd duidelijk gemaakt, en de gemiddelde consument er zowel in het ene als in het andere geval toe wordt of kan worden gebracht een besluit over een transactie te nemen dat hij anders niet had genomen

Indien een AI-systeem (bv. chatbot) dus zou worden gebruikt om producten of diensten te verkopen, moet er op worden gewaakt dat het systeem geen bedrieglijke informatie zou (beginnen te) gebruiken, maar een consument steeds de juiste informatie verschaft of er, minstens, naar verwijst. Zo niet, zou het besluitvormingsproces van een eindgebruiker op onbedoelde of ongewenste manier kunnen worden verstoord.

ALGEMEEN VERBINTENISSENRECHT

Hoewel het wat verder gezocht is, zullen organisaties die een AI-systeem gebruiken in de loop van een contractsluiting, er ook voor moeten zorgen dat het AI-systeem geen 'geweld' of 'dwang' veroorzaakt (art. 1111-1115 BW). **Dwang** is, net zoals dwaling, een wilsgebrek en staat in de weg van een geldige contractsluiting. Dit komt in praktijk eerder uitzonderlijk voor.

Meer bepaald bestaat dwang uit het uitoefenen van een fysieke of morele dwang, minstens uit de dreiging ermee, ten aanzien van de persoon van de medecontractant, zijn eer of zijn vermogen.

Er moet dus over gewaakt worden dat een AI-systeem dat bepaalde producten verkoopt niet doorslaat en ter vervulling van diens functie ongeoorloofde dwang zou (beginnen) uitoefenen op potentiële kopers. Hier kan bijvoorbeeld sprake van zijn indien het systeem zou dreigen de digitale toestellen van de koper of diens dierbaren te hacken. Zodoende wordt vermeden dat het besluitvormingsproces van een eindgebruiker op een onbedoelde of ongewenste manier zou worden verstoord.

STRAFRECHT

In deze context kan ook worden gedacht aan het risico dat een AI-systeem zich zou bezondigen aan of aangewend zou worden in het kader van mogelijke strafbare **misdrijven** als informaticabedrog, afpersing, oplichting en bedriegerij of misbruik van vertrouwen. Deze komen verder aan bod bij de bespreking van de "Hoofdstuk 2: Ethische vereiste 2 - technische robuustheid en veiligheid".

Simuleert het AI-systeem sociale interactie met of tussen eindgebruikers of subjecten? Dreigt het AI-systeem te leiden tot menselijke aanhankelijkheid, het stimuleren van verslavend gedrag of het manipuleren van gebruikersgedrag? Afhankelijk van welke risico's mogelijk of waarschijnlijk zijn, kunt u de onderstaande vragen beantwoorden:

- Werden er maatregelen genomen om mogelijke negatieve gevolgen voor eindgebruikers of subjecten aan te pakken in het geval zij een buitensporige aanhankelijkheid aan het AI-systeem ontwikkelen?
- Werden er maatregelen genomen om het risico op verslaving te beperken?
- Werden er maatregelen genomen om het risico op manipulatie te beperken?

CONSUMENTRECHT

Wat betreft het risico op buitensporige aanhankelijkheid en manipulatie, kan men deze vraag in zekere vorm terugvinden in de bepalingen omtrent de **misleidende en agressieve handelspraktijken**.

Zo bepaalt artikel VI.100 WER dat het een **misleidende handelspraktijk** is om te beweren dat producten het winnen bij kansspelen vergemakkelijken of in de context van een handelspraktijk te beweren dat er een wedstrijd wordt georganiseerd of prijzen worden uitgeloofd zonder de aangekondigde prijzen of een redelijk alternatief daadwerkelijk toe te kennen. Een AI-systeem dat producten of diensten verkoopt mag dus geen dergelijke beweringen stellen en het moet vermeden worden dat het systeem ter vervulling van diens functie dergelijke bewerkingen zou beginnen te stellen.

Verder bepaalt artikel VI.103 WER dat het een **agressieve handelspraktijk** is om als onderneming hardnekkig en ongewenst aan te dringen bij een consument per telefoon, fax, e-mail of andere afstandsmedia. Ook dit kan een risico tot manipulatie omvatten en het dient daarom te worden vermeden dat AI-systemen dergelijke handelingen zouden stellen.

ALGEMEEN VERBINTENISSENRECHT

Ook onder het algemeen verbintenissenrecht wordt manipulatie, in de vorm van **bedrog**, niet aanvaard. Bedrog is een derde wilsgebrek en staat in de weg van een geldige contractsluiting (art. 1116 BW).

Om van bedrog te spreken, moet een partij ter kwader trouw **kunstgrepen** aanwenden om bewust de andere partij te doen dwalen zodat zij een overeenkomst zou sluiten. Er moet dus opzettelijk een dwaling worden uitgelokt zonder welke het contract niet zou zijn gesloten. Met andere woorden, de kunstgrepen moeten doorslaggevend voor het sluiten van de overeenkomst zijn geweest. Dergelijke kunstgrepen kunnen zowel positieve handelingen (bv. liegen) zijn, het verschaffen van onjuiste/onvolledige informatie of het bedrieglijk stilzwijgen of verzwijgen van informatie.

GOKWETGEVING

In deze context kan ook gedacht worden aan de **inzetbeperking** die de Belgische gokwetgeving in bepaalde situaties oplegt, waardoor het inzetverlies wordt beperkt maar die ook het risico op verslaving tracht te beperken. Mochten er dus kansspelen worden aangeboden die gebruik maken van AI, moet er eveneens gezorgd voor worden dat zij de eventueel toepasselijke inzetbeperkingen respecteren.

1.2.B. Menselijk toezicht

Bepaal of het AI-systeem (kies er zoveel als nodig is):
- een zelflerend oftewel autonoom systeem is;
- gecontroleerd wordt door een Human-in-the-Loop;
- gecontroleerd wordt door een Human-on-the-Loop;
- gecontroleerd wordt door een Human-in-Command.

Kregen gebruikers (HITL, HOTL, HIC) specifieke training over hoe ze de controle of toezicht kunnen uitoefenen?

ARBEIDSRECHT

In deze context kan er in de eerste plaats gedacht worden aan werkgevers die AI-systemen gebruiken in hun productieprocessen of dienstverlening. Zij dienen immers enerzijds de arbeidsveiligheid van hun werknemers te verzekeren, en anderzijds hen in de mogelijkheid te stellen om hun beroep uit te oefenen, o.a. door middel van instructies. Het is dus van belang dat zij werknemers de juiste training geven mochten zij in contact komen met AI-systemen.

Meer bepaald legt artikel 4 van de **Welzijnswet** op dat het welzijn van de werknemers moet worden bevorderd door middel van maatregelen op het vlak van o.a. arbeidsveiligheid en de psychosociale aspecten van het werk. Artikels 5 en 6 concretiseren dit verder.

Zo somt artikel 5 enkele preventiebeginselen op die een werkgever dient toe te passen. Deze omvatten o.a. **risico's voorkomen**, de risico's op ernstig letsel inperken door het nemen van materiële maatregelen, de werknemer **voorlichten** over de aard van zijn werkzaamheden, de daaraan verboden risico's en bijhorende maatregelen; en het verschaffen van **passende instructies** aan de werknemers en het vaststellen van begeleidingsmaatregelen voor een redelijke garantie op de naleving van deze instructies. Vice versa bepaalt artikel 6 dat iedere werknemer op de arbeidsplaats, overeenkomstig zijn opleiding en de door de werkgever gegeven instructies, naar zijn beste vermogen zorg moet dragen voor zijn eigen veiligheid en gezondheid en deze van de andere betrokken personen.

Meer informatie kan ook worden gevonden bij de bespreking van de "Hoofdstuk 6: Ethische vereiste 6 - maatschappelijk en milieuwelzijn".

ALGEMENE EN SPECIFIEKE PRODUCTVEILIGHEIDSREGELS

In deze context kan men ook denken aan de verplichting voor producenten tot het **verschaffen van instructies of informatie** in het kader van de productveiligheid. Zo bepaalt art. IX.8 WER dat producenten aan gebruikers informatie moeten verschaffen omtrent de aan een product inherente risico's gedurende de normale of redelijkerwijs te verwachten gebruiksduur, indien deze risico's zonder passende waarschuwing niet onmiddellijk herkenbaar zijn.

De verplichting tot het geven van informatie en instructies wordt ook behandeld in meer **sectorale wetgeving**. Onder de speelgoedwetgeving bijvoorbeeld wordt vereist dat fabrikanten het door hun gemaakte speelgoed vergezellen van instructies en informatie aangaande de veiligheid. Informatieplichten bestaan ook voor medische hulpmiddelen.

Rekening houdende met het zelflerende karakter van AI-producten, lijkt dergelijke bepaling mogelijk een hernieuwde relevantie te krijgen. Meer informatie kan hierover worden gevonden in het deel over "Hoofdstuk 4: Ethische vereiste 4 - transparantie".

Werden er waarschuwings- en reactiemethodologieën opgesteld voor het geval dat het AI-systeem ongewenste schadelijke effecten op de eindgebruiker of het subject zou hebben?
Werd er een 'stopknop' of procedure om een handeling veilig af te breken wanneer dat nodig is, voorzien?
Werden er specifieke toezichts- en controlemaatregelen genomen, rekening houdende met het zelflerende of autonome karakter van het AI-systeem?

GEGEVENSBESCHERMING

De AVG verplicht de verwerkingsverantwoordelijke om in bepaalde gevallen een **gegevensbeschermings-effectbeoordeling** (GEB) te doen. Een GEB moet op voorhand uitgevoerd worden bij elke verwerking waarbij vermoedelijk een hoog risico bestaat voor de betrokkenen en is een concrete verplichting om vooraf na te denken over de risico's die het verwerken van persoonsgegevens kan hebben voor de rechten en vrijheden van natuurlijke personen (art. 35).

Voor een uitvoerige bespreking verwijzen we naar "Hoofdstuk 3: Ethische vereiste 3 - privacy en databeheer".

ARBEIDSVEILIGHEID

Ook in deze context kan er op worden gewezen dat een werkgever het **welzijn van werknemers** moet bevorderen door middel van maatregelen op het vlak van o.a. arbeidsveiligheid en de psychosociale aspecten van het werk. Een werkgever moet immers bepaalde preventiebeginselen toepassen. Werkgevers die AI-systemen gebruiken in hun productieprocessen of dienstverlening kunnen dus dergelijke waarschuwings- en reactiemethodologieën, stopknop-procedures of controlemaatregelen opstellen om te voldoen aan deze verplichting.

Meer informatie kan ook worden gevonden bij de bespreking van de "Hoofdstuk 6: Ethische vereiste 6 - maatschappelijk en milieuwelzijn".

VEILIGHEIDSNORMEN

Er zijn verschillende veiligheidsnormen die reeds nu al bepaalde **risicobeoordelingen** opleggen, vereisen dat producten aan bepaalde minimale gezondheids- en veiligheidseisen voldoen en daarom relevant kunnen zijn in deze context.

Zo is er de **Machinerichtlijn** die werd omgezet door het koninklijk besluit van 12 augustus 2008. Het toepassingsgebied van de Machinerichtlijn is zeer specifiek (art. 1). Deze bepaalt dat de fabrikant van een machine een risicobeoordeling moet uitvoeren om na te gaan welke veiligheids- en gezondheidseisen op die machine van toepassing zijn. Bij het ontwerp en de bouw van de machine moet vervolgens rekening worden gehouden met de resultaten van deze risicobeoordeling. Dit heeft ook betrekking op de besturingssystemen (bv. AI-software) van machines die o.a. zodanig moeten worden ontwikkeld dat fouten in de besturingslogica niet tot een gevaarlijke situatie kunnen leiden. Daarenboven bepaalt de machinerichtlijn ook dat een machine in bepaalde gevallen voorzien moet zijn van één of meer **noodstopinrichtingen** waarmee reële of dreigende gevaarlijke situaties kunnen worden afgewend.

Ook de **Europese Laagspanningsrichtlijn** die werd omgezet door het koninklijk besluit van 21 april 2016 legt aan fabrikanten van elektrisch materiaal op dat zij technische documentatie moeten opstellen, waaronder een risicoanalyse en-beoordeling. Deze beoordeling moet rekening houden met de algemene

vereiste dat elektrisch materiaal slechts op de markt van de EU kan worden aangeboden indien het bij correcte installatie en onderhoud en bij gebruik overeenkomstig de bestemming, de gezondheid en veiligheid van mensen en huisdieren of goederen niet in gevaar brengt. Zo dient dergelijk elektrisch materiaal o.a. erop voorzien te zijn dat er bescherming is tegen gevaren die kunnen ontstaan door invloeden van buitenaf.

Andere specifieke veiligheidsregels die in deze context relevant kunnen zijn, zijn bv. de regels van toepassing op **speelgoed**.

Algemener zijn er dan ook nog de **productveiligheidsregels** die zijn opgenomen in Boek IX WER. Zo legt art. IX.8 WER op dat producenten (eventueel ondersteund door distributeurs) maatregelen moeten nemen om op de hoogte te kunnen blijven van de risico's van hun producten en/of diensten en de passende acties te kunnen ondernemen om deze risico's te voorkomen. Tot deze maatregelen behoren o.a. de vermelding, op het product of op de verpakking ervan, van de identiteit en de contactinformatie van de producent om klachten mogelijk te maken of het uitvoeren van steekproeven op de in de handel gebrachte producten.

1.3. Waar zitten mogelijke punten van verbetering of aandachtspunten?

Verduidelijking (toepasbaarheid) concepten

De huidige regelgeving is niet voorzien op systemen die kunnen 'leren' of door de ontwerper/gebruiker onvoorziene handelingen kunnen stellen. Doorgaans wordt er immers van uitgegaan dat de onderneming of natuurlijk persoon die bepaalde hulpmiddelen hanteert daar de controle, en dus eindverantwoordelijkheid, over heeft. Werkelijk autonome AI-systemen botsen met deze stilzwijgende veronderstelling.

Het lijkt daarom van belang dat beleidsmakers **duidelijkheid scheppen** over de mate waarin ontwerpers en gebruikers van AI-systemen **maatregelen moeten treffen of procedures voorzien met het oog op het vermijden van ongewenste gevolgen** als gevolg van het zelflerende/autonome karakter van AI-systemen.

Anderzijds hebben deze vragen ook betrekking op juridisch minder aflijnbare onderwerpen als **'afhankelijkheid'** en **'aanhankelijkheid'** die nog geen weerklank vinden in het huidige recht. Vraag is hier of, en in welke mate, de (Europese of Belgische) wetgever kan of moet optreden om dergelijke **concepten in wettelijke vereisten om te zetten** en dit niet alleen voor AI-systemen, maar ook voor andere producten.

Veiligheidstandaarden

Het is aangeraden om veiligheidsstandaarden met betrekking tot AI-producten te (blijven) **ontwikkelen en verfijnen** die rekening houden met zelflerende karakter van dergelijke producten.

1.4. Welke tools kunnen worden gebruikt om aan de ethische vereiste te voldoen?

- Tarot Cards of Tech zijn bedoeld om tijdens vergaderingen een informele impact assessment te doen via een brainstormsessie.
- De Artificiële Intelligentie Impact Assessment (AIIA) is een gestructureerde methode om de (maatschappelijke) baten van een AI-toepassing duidelijk in kaart te brengen. Daarnaast is er ook aandacht voor het analyseren van de betrouwbaarheid, veiligheid en transparantie van het AI-systeem. De AIIA is een workshop die in de eerste fase van een project kan plaatsvinden, met nadien een regelmatige terugkoppeling naar de uitkomsten van de workshop.
- Data Ethics Decision Aid (DEDA) is gemaakt door de Utrecht Data School in samenwerking met data-analisten van de Gemeente Utrecht. Ze bestaat uit verschillende methodes die kunnen worden ingezet bij het begin van een project. Het doel is om de ethische kwesties en beslissingen daaromtrent te documenteren, bijvoorbeeld ter verantwoording naar de betrokken belanghebbenden.
- De aanpak begeleidingsethiek heeft als doel om door middel van een workshop een dialoog aan te gaan over het verband tussen ethiek en technologie om een duidelijker beeld te krijgen van mogelijke ethische knelpunten bij de ontwikkelde technologie.
- De Ethical Explorer pack biedt een gratis tool aan met een checklist in de vorm van een kaartenset. Hierdoor kan mee worden gedacht aan/over aspecten bij het ontwikkelen van ethische technologie.
- De Product Impact Tool zet ontwikkelaars aan het denken over de verhouding tussen mens en techniek en geeft een handvat over hoe met nieuwe technologieën kan worden omgegaan.

Hoofdstuk 2: Ethische vereiste 2 - technische robuustheid en veiligheid

2. Ethische vereiste 2: technische robuustheid en veiligheid

2.1. Wat betekent de ethische vereiste?

De ethische vereiste van technische robuustheid houdt in dat AI-systemen met een **preventieve benadering** moeten worden ontwikkeld. AI-systemen moeten zich gedragen zoals voorzien en alle vormen van onaanvaardbare schade moeten worden vermeden. De fysieke en mentale integriteit van mensen moet altijd worden gewaarborgd.

Het vereiste van technische robuustheid bestaat uit **vier sub-componenten**: (1) weerbaarheid tegen aanvallen en bedreigingen, (2) algemene veiligheidsmaatregelen, (3) nauwkeurigheid en (4) betrouwbaarheid.

AI-systemen moeten **weerbaar zijn tegen aanvallen en bedreigingen**. Kwetsbaarheden waardoor AI-systemen kunnen worden aangevallen (bv. door hacking) zijn uit den boze. Dit geldt zowel voor de software als de hardware waarin het AI-systeem is ingebed. Deze kwetsbaarheden kunnen immers aanleiding geven tot allerhande vormen van schade.

Daarnaast moet voor elk AI-systeem een **uitwijkplan en algemene veiligheidsmaatregelen voorzien** zijn. AI-systemen moeten hun functie vervullen zonder daarbij schade toe te brengen aan mensen of het milieu. Ook onbedoelde schade moet worden vermeden. Bij AI-systemen hoort ook altijd een vorm van risicobeoordeling. Het nodige niveau hangt af van de feitelijke context: sommige AI-systemen vertonen een hoog risico en vereisen proactieve testen. Andere AI-systemen hebben een laag risico en vereisen minder zware testen.

Verder moeten AI-systemen **nauwkeurig** zijn. AI-systemen moet correcte afwegingen kunnen maken, bv. door informatie in de juiste categorieën in te delen of correcte aanbevelingen te doen. Zo kunnen onbedoelde risico's van foute voorspellingen worden verminderd. AI-systemen moeten duidelijk maken indien fouten niet kunnen worden voorkomen. Nauwkeurigheid wordt des te belangrijker naarmate de gevolgen van de beslissingen van het AI-systeem een impact hebben op (het leven, de integriteit) van mensen.

Ten slotte moeten AI-systemen **betrouwbaar en reproduceerbaar** zijn. Betrouwbare AI-systemen werken goed met allerlei input en in verschillende situaties. Reproduceerbaarheid omvat dat AI-systemen bij gelijke omstandigheden altijd op dezelfde manier werken. Zo kan het gedrag van AI-systemen voorspeld worden. Replicatiebestanden kunnen dit werk vereenvoudigen.

2.2. Welke regels zijn een uitdrukking van de ethische vereiste of kunnen dienen als inspiratiebron?

De ALTAI lijst voorziet per aangehaald sub-component verschillende vragen. We geven hieronder een overzicht van de vragen per sub-component en de wetgeving die reeds een uitdrukking vormt van deze vragen of kan worden gebruikt als inspiratie.

2.2.A. Weerbaarheid tegen aanvallen en beveiliging

Werden er waarschuwings- en reactiemethodologieën opgesteld voor het geval dat Kan het AI-systeem vijandige, kritieke of schadelijke effecten hebben (bv. voor de veiligheid van mensen of maatschappij) in geval van risico's of bedreigingen zoals technische fouten in het ontwerp, uitval, aanvallen, misbruik, ongepast of kwaadwillig gebruik?

TECHNISCHE NORMEN EN STANDAARDEN

De meeste normen die voor regelgevers belangrijk zijn, worden in eerste instantie aangenomen door internationale (bv. International Standards Organisation-ISO), Europese (bv. CEN, CENELEC of ETSI) of nationale **normeringsinstanties**. Dit zijn private entiteiten die als hoofdactiviteit de normen voor allerhande soorten producten opstellen (bv. Nationaal Bureau voor Normalisatie).

Deze normeringsprocessen zijn soms nog altijd te traag om de technologische ontwikkelingen bij te benen. Om die reden zijn er ook verschillende nieuwe normen uitgevaardigd door industrieconsortia (bv. World Wide Web Consortium (W3C) en Internet Engineering Task Force). Ook de normen van het Instituut voor Elektrische en Elektrotechnische Ingenieurs (IEEE) zijn belangrijk.

De naleving van deze normen is in principe volledig vrijwillig tenzij anders wordt bepaald. In de productveiligheidswetgeving leidt de naleving van de normen tot een vermoeden van veiligheid en naleving van de veiligheidsverplichtingen. Soms wordt een **conformiteitsbeoordeling** ook verplicht. Deze en andere wetgevingen worden hieronder besproken.

Is het AI-systeem gecertificeerd voor cyberveiligheid of is het in overeenstemming met specifieke veiligheidsstandaarden?

TECHNISCHE NORMEN EN STANDAARDEN ZOALS DE ISO NORMEN OVER INFORMATIETECHNOLOGIE EN BEVEILIGINGSTECHNIEKEN

De meest gekende cyberbeveiligingsstandaarden zijn de standaarden van de **ISO 27000-familie** die testen voorschrijven met betrekking tot het veiligheidsbeheer van informaticasystemen. Denk aan ISO/IEC 27001:2017 of ISO/IEC 27002. Er zijn op heden nog geen geharmoniseerde EU-normen voor AI. Op het niveau van de ISO en op sommige nationale niveaus zijn er wel al standaarden aangenomen omtrent AI (bv. ISO/IEC JTC 1/SC 42).

CYBERVEILIGHEID

In navolging van de NIS-Richtlijn voorziet de NIS-Wet in een **vermoeden van veiligheid** voor netwerk- en informatiesystemen die werden gecertificeerd conform ISO 27001. De naleving van veiligheidseisen wordt

aangetoond aan de hand van een certificaat dat wordt uitgereikt door een bevoegde geaccrediteerde instelling voor de conformiteitsbeoordeling.

Verder voorziet de Cyberbeveiligingsverordening voor een vrijwillige certificering van ICT-producten, diensten en processen (art. 52, 54 en 55). Dit certificeringskader wordt door de European Union Agency for Cybersecurity (ENISA) voorbereid in opdracht van de Europese Commissie. Op volgende link kan een ontwerp van een kandidaat-certificeringskader worden gevonden.

GEGEVENSBESCHERMING

Een uitvoerige bespreking over de AVG is beschikbaar bij de toelichting van de ethische vereiste 3 over privacy en databeheer. Het volstaat hier te benadrukken de verwerking van persoonsgegevens voor **beveiligingsdoeleinden** mag gebeuren op grond van de rechtsgrond van het gerechtvaardigd belang (art. 6, lid 1, sub f)).

De AVG voorziet verder ook dat organisaties **gedragscodes** kunnen opstellen. Deze kunnen afspraken bevatten over hoe de verwerking moet gebeuren, hoe de rechten van betrokkenen moeten worden uitgeoefend, welke informatie moet worden verstrekt en welke beveiligingsmaatregelen worden aanvaard (art. 40). Art. 42 AVG verduidelijkt dat **certificeringsmechanismen** evenzeer worden aangemoedigd. De aansluiting bij dergelijke gedragscodes geldt als een bewijs van de naleving van verschillende verplichtingen (zie bv. relevante bepalingen in art. 24 en 25).

PRODUCTVEILIGHEID

In navolging van de Richtlijn Productveiligheid, bepaalt art. IX.2. WER dat de fabrikant uitsluitend **veilige producten en diensten** op de markt mag brengen.

Volgens artikel IX.3 WER wordt een product of dienst **vermoed veilig** te zijn indien het voldoet aan geharmoniseerde normen of (bij afwezigheid daarvan) aan de toepasselijke Belgische normen, aanbevelingen van de Europese Commissie, gedragscodes omtrent productveiligheid, de stand van vakkennis en techniek, de veiligheid die een gebruiker redelijkerwijze mag verwachten en internationale normen.

ALGEMENE VEILIGHEIDSVERPLICHTING EN SPECIFIEKE VEILIGHEIDSREGELS

Terugkerende elementen in relevante regelgeving zijn onder andere het **veiligheidsvermoeden** en de **veiligheidsverplichting**. Daarbovenop leggen deze regels ook bijzondere veiligheidsregels vast voor de **conformiteitsbeoordeling** van bepaalde producten (bv. medische hulpmiddelen).

De vormen van conformiteitsbeoordeling worden beschreven in Bijlage II van het EU-Kaderbesluit betreffende een gemeenschappelijk kader voor het verhandelen van producten. Daarnaast verplichten deze regels vaak ook tot het voorzien van de **CE-markering** die moet bewijzen dat producten in overeenstemming zijn met de productveiligheidswetgeving. Voor sommige producten moet een onafhankelijke aangemelde instantie worden betrokken die nagaat of een product conform is en dus een CE-label kan krijgen. Dit is terug te vinden in regels per productcategorie. De fabrikant moet ook een EG-verklaring van overeenstemming opmaken en de technische documentatie opmaken. Voorbeelden zijn de speelgoedwetgeving of de wetgeving voor machines. Een ander voorbeeld is de wetgeving inzake elektrische apparatuur.

Een samenvatting van de verschillende categorieën producten en de toepasselijke regelgeving en normen kan op volgende link worden gevonden.

GEMEEN KOOPRECHT, AANNEMINGSRECHT EN VERBINTENISSENRECHT

De naleving van het gemeen verbintenissenrecht zorgt ook voor de naleving van (veiligheids)normen. Dit geldt zowel voor de koop van zaken (naar Belgisch recht is dit alleen voor hardware of software die op een drager is geïnstalleerd) en een dienstverlening (dit is ook de levering van software zonder enige drager).

Art. 1604 en 1614 van het BW bepalen dat de verkoper aan de koper een zaak moet leveren die in overeenstemming is met de overeenkomst (**'conforme levering'**). Deze conformiteit betreft ook de overeengekomen kwaliteit. Ook voor dienstenovereenkomsten geldt dat de dienstverlener de afgesproken of de gebruikelijke kwaliteit moet leveren. Het is dan ook aangewezen hieromtrent duidelijke afspraken te maken in een **service level agreement**.

In navolging van Richtlijn 1999/44 voorzien art. 1649bis e.v. van het BW in bijkomende conformiteits-garanties voor de verkopen van goederen aan **consumenten**. Tussen ondernemingen die in verschillende landen gevestigd zijn kan ook het Weens Koopverdrag gelden.

De nieuwe Richtlijn 2019/770 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en diensten (Richtlijn Digitale Inhoud) en Richtlijn 2019/771 betreffende bepaalde aspecten van overeenkomsten voor de verkoop van goederen (Richtlijn Consumentenkoop) voorzien beide in een **conformiteitsplicht** voor de levering van digitale inhoud (software, data, etc. die online wordt geleverd) en consumentengoederen. Deze conformiteit wordt zowel subjectief (op grond van de overeenkomst) als objectief (op grond van de thans geldende normen en geschiktheid voor de doeleinden van het product of de inhoud) beoordeeld. Deze richtlijnen moeten uiterlijk op 1 juli 2021 in Belgische wetgeving worden omgezet en van kracht gaan met ingang van 1 juli 2022.

ALGORITMISCHE HANDEL

In navolging van de MiFiD II-richtlijn voorziet de Wet van 21 november 2017 over de Infrastructuren voor de markten voor financiële instrumenten in de verplichting van marktexploitanten om erop toe te zien dat er in doeltreffende systemen, procedures en regelingen wordt voorzien om te waarborgen dat de handelssystemen weerbaar zijn, voldoende capaciteit hebben om volumepieken in orders en orderberichten op te gangen, in staat zijn een ordelijke handel onder zeer gespannen marktomstandigheden te waarborgen, volledig zijn getest om te garanderen dat aan deze voorwaarden is voldaan en onderworpen zijn aan doeltreffende regelingen ter verzekering van de continuïteit van de bedrijfsuitoefening om de continuïteit van de dienstverlener te verzekeren in geval van storingen in de handelssystemen. (artikel 22 §1 Wet 21 november 2017)

Deze bepaling wordt hernomen in het KB van 19 december 2017 tot bepaling van nadere regels tot omzetting van de richtlijn betreffende markten voor financiële instrumenten, waarnaar wordt verwezen in m.n. de Bankwet en de Wet Beleggingsondernemingen.

Bijkomende technische vereisten voor deze verplichting onder MiFiD 2 worden vastgelegd in de Gedelegeerde Verordening 2017/589 van de Commissie van 19 juli 2016 met betrekking tot technische reguleringsnormen tot specificering van de organisatorische vereisten voor beleggingsondernemingen die zich met algoritmische handel bezig houden.

Hoezeer is het AI-systeem blootgesteld aan cyber-aanvallen?

- Werd rekening gehouden met de mogelijke soorten aanvallen waarvoor het AI-systeem kwetsbaar kan zijn?
- Werden verschillende vormen van kwetsbaarheden en mogelijke ingangspunten gevonden voor aanvallen zoals datavergiftiging, modelontwijking en modelinversie?

AANVALLEN

Zoals alle andere ICT-systemen zijn ook AI-systemen vatbaar voor aanvallen.

Datavergiftiging houdt bv. in dat een aanvaller nieuwe incorrect gelabelde trainingsdata invoert in het systeem om het gedrag van het zelflerend systeem te verstoren. AI-systemen kunnen ook worden aangevallen via **modelontwijkingstechnieken**. Dit is het gebruik maken van kwetsbaarheden (uitbuiting) in het model zodat het zaken niet of verkeerd herkent. Een laatste gekende tactiek is **modelinversie** waarbij de aanvaller aan de hand van een beschrijving van het AI-model of van de output de onderliggende training-gegevens probeert te achterhalen.

GEGEVENSBESCHERMING

De verwerkingsverantwoordelijke is verplicht om gegevens op een dusdanige manier te verwerken dat een **'passende' beveiliging** ervan gewaarborgd is. De gegevens moeten onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (art 5, lid 1, f) AVG).

Evenzeer verplicht art. 32 AVG de verwerkingsverantwoordelijke en de verwerker tot het nemen van passende **technische en organisatorische maatregelen** om een op het risico afgestemd beveiligingsniveau te waarborgen. In bepaalde gevallen moet ook een **GEB** worden uitgevoerd.

Zie voor meer informatie "Hoofdstuk 3: Ethische vereiste 3 - privacy en databeheer". Uit zijn aard omvat een GEB een modellering van mogelijke bedreigingen.

PRAKTISCHE METHODEN EN NORMEN

In de informatieveiligheid wordt voor de risicoanalyse gebruik gemaakt van **bedreigingsmodellering**. Dit houdt in dat binnen een onderneming iemand alle bedreigingen voor de veiligheid van alle informatie (waaronder persoonsgegevens) in kaart brengt en de nodige maatregelen neemt. Bekende bedreigingsmodelleringen zijn STRIDE (ontwikkeld door ingenieurs bij Microsoft) en LINDDUN Privacy-bedreigingsmodellering (ontwikkeld door de KU Leuven). Ook ISO 27001 verwijst naar een risicoanalyse en voorziet een lijst van risico's die aanwezig kunnen zijn voor de informatieveiligheid.

CYBERVEILIGHEID

De NIS-wet bepaalt dat de aanbieders van essentiële diensten en digitaledienstverleners **passende en evenredige technische en organisatorische maatregelen** moeten nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen waarvan zijn essentiële diensten afhankelijk te zijn te beheersen. De aanbieder neemt ook passende maatregelen om incidenten die de beveiliging van de voor de verlening van die essentiële diensten gebruikte netwerk- en informatiesystemen aantasten te voorkomen of de gevolgen ervan te minimaliseren. Voor de beheersing en de minimalisering van incidenten moet men deze kunnen identificeren, wat neerkomt op **bedreigingsmodellering**.

De Cyberbeveiligingsverordening bepaalt dat het opzet van het Europese cyberbeveiligings-certificeringskader er onder meer in bestaat **afhankelijkheden en kwetsbaarheden op te sporen** en te documenteren (art. 51). Er wordt geverifieerd dat ICT-producten, -diensten en -processen geen bekende kwetsbaarheden bevatten en door standaardinstellingen/ontwerp veilig zijn. Ook hier wordt verwezen naar risicobeoordeling, en dus ook naar bedreigingsmodellering.

ALGORITMISCHE HANDEL

De verplichting om weerbaarheid te voorzien in de systemen, waaronder in weerstand tegen storingen in de systemen, hierboven reeds besproken, kan worden gezien als een verplichting om weerbaar te zijn tegen aanvallen van buitenuit. De systemen moeten ook op passende wijze zijn getest. Verder voorziet de Gedelegeerde Verordening 2017/589 ook in de verplichting in een realtimemonitoring en een geautomatiseerd toezichtssysteem om markmanipulatie op te sporen.

MOGELIJKS SANCTIES

Er zijn reeds **verschillende informaticamisdrijven** terug te vinden zoals valsheid in informatica (art. 210bis Strafwetboek), informaticabedrog (art. 504quater Strafwetboek), hacking (art. 550bis Strafwetboek), informaticasabotage/ongeoorloofde datamanipulatie (Art. 550ter Strafwetboek).

Werden maatregelen genomen om de integriteit, robuustheid en de algemene veiligheid van het AI-systeem te garanderen tegen potentiële aanvallen over de gehele levenscyclus?

CYBERVEILIGHEID

De **algemene verplichtingen** van essentiële dienstverleners en digitaledienstverleners onder de NIS-wet werden hierboven reeds besproken. Deze maatregelen gelden gedurende de levenscyclus van het systeem. Ook bepalingen in de Cyberbeveiligingsverordening zijn relevant (bv. art. 51, j)).

ALGEMENE VERORDENING GEGEVENSBESCHERMING

De verwerkingsverantwoordelijke is verplicht om de **passende maatregelen te nemen** om de naleving van de AVG te waarborgen. Passende beveiligingsmaatregelen omvatten onder meer het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaar en veerkracht van de verwerkingssystemen en diensten te garanderen. Dit impliceert een constante beveiliging.

VERPLICHTINGEN VAN AANBIEDERS VAN ELEKTRONISCHE COMMUNICATIEDIENSTEN

In navolging van art. 4 van de e-Privacyrichtlijn verplicht artikel 114 van de Wet van 13 juni 2005 betreffende de elektronische communicatie de aanbieders van openbare elektronische-communicatiediensten om passende technische en organisatorische maatregelen te voorzien om de veiligheid van hun diensten te garanderen. Deze moeten in verhouding staan met het betrokken risico, rekening houdend met de stand van de techniek en de kosten van uitvoering.

CONSUMENTENRECHT

De handelaar zorgt ervoor dat (beveiligings)updates die nodig zijn om de conformiteit van de digitale inhoud of de dienst te handhaven aan de consument worden gemeld en geleverd gedurende de voorziene periode (art. 8 Richtlijn Digitale Inhoud). De Richtlijn Consumentenkoop bevat gelijkaardige

bepalingen voor goederen met digitale elementen (art. 7).

PRODUCTVEILIGHEID

In navolging van de Richtlijn Productveiligheid bepaalt art. IX.8 §2 WER dat de producenten van producten en diensten maatregelen moeten nemen die zijn afgestemd op de kenmerken dan de door hen geleverde producten en diensten om 1) op de hoogte te blijven van de risico's van deze producten en diensten en 2) de passende acties te ondernemen om de risico's van deze producten te voorkomen. Distributeurs dragen ook bij tot de naleving van de veiligheidseisen. Ze nemen binnen het bestek van hun activiteiten deel aan de bewaking van de veiligheid van de op de markt gebrachte producten (art. IX.8 §3 WER).

Ze moeten ook het **Centraal Meldpunt voor Producten** onmiddellijk in kennis wanneer zij weten dat het product of dienst voor de gebruiker risico's met zich meebrengt die onverenigbaar zijn met de algemene veiligheidsverplichting (art. IX.8 §4 WER). Deze verplichting geldt ook voor de producenten en distributeurs van producten die aan specifieke veiligheidswetgeving onderworpen zijn. Soms worden verplichtingen ook opgelegd in andere regelgeving (bv. art. 11 Bouwproductenverordening).

ALGORITMISCHE HANDEL

De verplichting om in weerbare systemen voor algoritmische handel te voorzien werd hierboven reeds besproken. De Gedelegeerde Verordening 2017/589 voorziet o.a. in een jaarlijkse zelfbeoordeling en realitimemonitoring als waarborg voor een continue naleving van deze voorschriften.

?	Werd het AI-systeem geredteamed/pentest?

STRAFRECHT

De strafbaarstelling van hacking werd reeds aangehaald. Voor red teams of penetratietesten van een netwerk is het aangewezen dat er **duidelijke afspraken** zijn gemaakt over welke informaticasystemen mogen worden geïnfiltreerd en op welke wijzen dit mag gebeuren.

STANDAARDEN

Voor penetratietests zijn onder andere de volgende **methodes** beschikbaar: het Open Source Security Testing Methodology Manual, de OWASP Web Application Penetration Checklist en de Penetration Testing Execution Standard.

REGELGEVING BELEGGINGSONDERNEMINGEN DIE ZICH MET ALGORITMISCHE HANDEL BEZIG HOUDEN

De verplichting om in weerbare systemen te voorzien werd reeds besproken voor alle ondernemingen die algoritmen gebruiken voor de uitvoering van bijvoorbeeld het kopen en verkopen van effecten.

De Gedelegeerde Verordening 2017/589 voorziet in bijkomende verplichtingen. Een beleggingsonderneming moet een **IT-strategie** implementeren met gedefinieerde doelstellingen en maatregelen die in overeenstemming is met effectief en veilig IT-beheer. Een beleggingsonderneming onderneemt **jaarlijks penetratietests** en kwetsbaarheidsscans om cyberaanvallen te simuleren (art. 18).

Werden eindgebruikers geïnformeerd over de duur van de beveiliging en eventuele updates?

CYBERBEVEILIGING

Conform de Cyberbeveiligingsverordening moet de fabrikant en de aanbieder van ICT-producten, -diensten en -processen o.a. de periode voorzien gedurende **dewelke beveiligingsondersteuning zal worden aangeboden** aan eindgebruikers, met name wat betreft de beschikbaarheid van actualiseringen in verband met cyberbeveiliging (art. 55).

GEGEVENSBESCHERMING

De verwerkingsverantwoordelijke moet de betrokkene onder andere informeren over de **bewaartermijnen** van de gegevens, dan wel de criteria die worden gehanteerd om de bewaartermijn te bepalen (art. 13, lid 2 en art. 14, lid 2 AVG).

CONSUMENTENRECHT

Binnen het consumentenrecht zijn er tal van **informatieplichten** ten aanzien van de eindgebruiker. Deze worden besproken onder "Hoofdstuk 4: Ethische vereiste 4 - transparantie".

VERBINTENISSENRECHT

De verkoper van software heeft een informatieplicht omtrent de voornaamste kenmerken van de zaak bij een verkoop. Ook de aannemer moet zijn diensten uitvoeren volgens de regels van de kunst en heeft een informatieplicht. Hieromtrent is echter geen wettelijke regelgeving. Om die reden is het in alle geval aangewezen om de duur van updates duidelijk op te laten nemen in een **service level agreement** om discussies te vermijden.

Hoe lang moeten beveiligingsupdates voor het AI-systeem worden voorzien?

CONSUMENTENBESCHERMING

De Richtlijn Digitale Inhoud (art. 8) en Richtlijn Consumentenkoop (art. 7) bevatten ook bepalingen over **(beveiligings)updates**. De verkoper zal verplicht zijn om gedurende de contractueel voorziene periode alle nodige beveiligingsupdates aan te bieden die "de consument redelijkerwijze kan verwachten" om aansprakelijkheid te vermijden. Dit omvat ook updates betreffende de beveiliging.

PRODUCTVEILIGHEIDSWETGEVING

De **bewakingsplicht** voor producenten betreffende alle risico's die betrekking hebben op hun producten werd reeds besproken (art. IX.8 §2 WER). Deze maatregelen omvatten eveneens dat producenten van producten die software bevatten ervoor zorgen dat zij een inschatting maken van hoe lang updates moeten worden voorzien, en dat zij gedurende de looptijd van de software updates voorzien. Een regeling voor producenten van software ontbreekt.

2.2.B. Algemene veiligheid

Werden de risico's, risicometriek en het risiconiveau van het AI-systeem in elk specifiek geval gedefinieerd?
Werd een proces voorzien om voortdurend de risico's te meten en te beoordelen?

ALGEMEEN

Hierboven werd de verplichting aangehaald om een **risicoanalyse uit te voeren** van alle bedreigingen en de nodige testen te doen op grond van regelgeving inzake cyberveiligheid, gegevensbescherming, het consumenten/contractenrecht en productveiligheid.

PRODUCTVEILIGHEID

Hierboven werd reeds toegelicht dat producenten op grond van de **productveiligheidswetgeving** een bewakingsplicht hebben betreffende alle risico's die betrekking hebben op hun producten.

GEGEVENSBESCHERMING

Er staat geen strikte tijdslimiet op de verplichting om passende technische en organisatorische beveiligingsmaatregelen te nemen (art. 32 AVG). Deze verplichting **blijft van toepassing** tijdens elke verwerking. Ook de beginselen van verwerking in art. 5 AVG (met name doelbeperking en integriteit) verplichten dat er een proces is om de **veiligheid te beoordelen**. Ook kan worden gesteld dat men de risico's waarvoor een GEB is uitgevoerd voortdurend moet blijven beoordelen (art. 35, lid 11).

ALGORITMISCHE HANDEL

De verplichting om in weerbare en adequaat geteste systemen te voorzien en de verplichting om de continuïteit van de bedrijfsuitoefening te garanderen werden reeds besproken.

Krachtens artikel 14 Gedelegeerde Verordening 2017/589 voorzien de regelingen ter verzekering van de continuïteit van de bedrijfsuitoefening in de effectieve behandeling van verstorende incidenten en waarborgen een tijdige hervatting van de algoritmische handel. Deze regelingen omvatten o.a. een reeds mogelijke ongunstige scenario's in verband met de exploitatie van algoritmische handelssystemen. De IT-strategie waarover eerder werd gesproken, dient ook aangepast te zijn aan de operationele activiteiten en de risico's waaraan de onderneming is blootgesteld.

Werden de eindgebruikers en de betrokken personen geïnformeerd van de bestaande of potentiële risico's?

ALGEMEEN

Deze vereisten moet samen worden gelezen met verplichtingen onder "Hoofdstuk 4: Ethische vereiste 4 - transparantie".

VERBINTENISSENRECHT

Een verkoper is gehouden tot **vrijwaring voor de verborgen gebreken** van de verkochte zaak (art. 1641 BW). Naar Belgisch recht is er geen strikte informatieplicht voor de verkoper. De verkoper moet weliswaar op grond van de goede trouw de koper volledig informeren van wat hij aanbiedt. Hierbij moet rekening worden gehouden met de behoeften, verwachtingen en mogelijkheden van de klant. Duidelijke contractuele afspraken zijn dus aanbevolen.

ARBEIDSVEILIGHEID

De Welzijnswet en de Codex Welzijn op het Werk voorzien ook in verplichtingen voor de werkgever om te zorgen voor de veiligheid van het personeel. Dit impliceert dat hij alle informatie moet geven die betrekking heeft op de risico's en de preventiemaatregelen ter beperking van die risico's. (zie o.a. artikel I.2-16 Codex Welzijn op het Werk)

ALGORITMISCHE HANDEL

De wetgeving inzake algoritmische handel verplicht beleggingsondernemingen om het personeel op te leiden inzake het beheer van de regelingen ter verzekering van de bedrijfscontinuïteit. Zie o.a. artikel 14 Gedelegeerde Verordening 2017/589.

Werden mogelijke bedreigingen voor het AI-systeem geïdentificeerd (gebreken in ontwerp, technische gebreken, bedreigingen voor het milieu) en de mogelijke gevolgen hiervan?

Werd het risico beoordeeld van een mogelijk schadelijk gebruik, misbruik of ongepast gebruik van/voor het AI-systeem?

CYBERBEVEILIGING

Verschillende bepalingen over het nemen van **technische en organisatorische maatregelen** onder de NIS-wet werden reeds aangehaald. De betrokken actoren moeten dus alle mogelijke bedreigingen te identificeren.

De Cyberbeveiligingsverordening voorziet in bijkomende regels wat betreft de **certificatie**. Teneinde een cyberbeveiligingscertificaat te bekomen, heeft de entiteit die de software ontwikkelt de verplichting om de **voorgeschreven conformiteitsbeoordelingsprocedure** uit te voeren. Art. 51 voorziet in verschillende

beveiligingsdoelstellingen van de cyberbeveiligingscertificeringsregelingen waaronder afhankelijkheden en kwetsbaarheden opsporen en documenteren en nagaan of ICT-producten, -diensten en -processen geen bekende kwetsbaarheden vertonen.

PRODUCTVEILIGHEID

De **algemene veiligheidsverplichting**, de **bewakingsplicht** en andere verplichtingen in specifieke regelgeving werden reeds besproken.

PRODUCTAANSPRAKELIJKHEID

Volgens de Wet Productaansprakelijkheid is een producent aansprakelijk voor de schade die veroorzaakt wordt door **gebrekkige producten** tenzij hij o.a. bewijst dat het op grond van de stand van de wetenschappelijke en technische kennis op het tijdstip waarop hij het product in het verkeer bracht onmogelijk was om het bestaan van het gebrek te ontdekken. Een product is gebrekkig als het **niet de veiligheid biedt die men gerechtigd is te verwachten**. Een producent van producten heeft er dus alle baat bij om de risico's en bedreigingen op voorhand te identificeren.

CONSUMENTENRECHT

Het werd reeds aangehaald dat de verkoper de consument op voorhand moet inlichten over de **functionaliteiten van het product of de dienst**, zowel bij offline als bij online overeenkomsten. Dit impliceert dat zij de mogelijke bedreigingen hebben geïdentificeerd.

VERBINTENISSENRECHT

De verplichting tot **conforme levering** van goederen en diensten, alsook de informatieplichten van de verkoper en de dienstverlener, werden reeds besproken.

ALGORITMISCHE HANDEL

De verplichting om in voldoende weerbare en adequaat geteste systemen te voorzien werd reeds besproken. Deze omvatten o.a. een IT-strategie die aangepast is aan de risico's die de onderneming loopt, wat inhoudt dat de onderneming deze risico's moet hebben gedefinieerd. Ook moet de onderneming als regeling voor het behoud van haar bedrijfscontinuïteit o.a. de ongunstige scenario's beschrijven die met haar activiteiten verbonden zijn.

ARBEIDSVEILIGHEID

De Welzijnswet verplicht werkgevers om de nodige maatregelen te nemen ter bevordering van het welzijn van de werknemers bij de uitvoering van hun werk. Daarbij moeten als preventiebeginselen o.a. worden toegepast dat de werkgever risico's moet voorkomen, risico's die niet kunnen worden voorkomen moet

evalueren en zo veel als mogelijk de risico's moet inperken, rekening houdend met de ontwikkelingen van de techniek. De Codex Welzijn op het Werk voorziet ook in verplichtingen met betrekking tot de risicoanalyse (zie o.a. artikelen I.2.-5-I.2-7).

MILIEUVEILIGHEID

Dit moet worden samengelezen met "Hoofdstuk 6: Ethische vereiste 6 - maatschappelijk en milieuwelzijn".

Werden de niveaus van ernst gedefinieerd (bijvoorbeeld voor menselijke integriteit) van de mogelijke gevolgen van gebreken of misbruiken van het AI-systeem?

CYBERBEVEILIGING

In het kader van haar algemene verplichtingen om de veiligheid van hun netwerken te voorzien, zijn zowel de verleners van essentiële diensten als digitaledienstverleners onder de NIS-wet verplicht om **niveaus van ernst** te definiëren. De Cyberbeveiligingsverordening maakt een onderscheid tussen drie zekerheidsniveaus: 'basis', 'substantieel' of 'hoog'.

PRODUCTVEILIGHEID

De risico-gebaseerde aanpak van de **veiligheidsverplichting** impliceert dat voor bepaalde producten strengere regels gelden dan voor andere. Voor bepaalde categorieën (bv. voor medische hulpmiddelen of bepaalde machines) kunnen strengere conformiteitsbeoordelingsprocedures worden opgelegd. Dit houdt op zich reeds in dat er een onderscheid wordt gemaakt in de risico's van verschillende producten. Een **risico-inschatting** moet ook altijd worden gemaakt bij het nemen van corrigerende maatregelen door producenten, zoals bijvoorbeeld een terugroeping.

GEGEVENSBESCHERMING

De verwerkingsverantwoordelijke en de verwerker moeten **passende technische en organisatorische maatregelen** treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's (art. 32 AVG). Een verwerkingsverantwoordelijke moet ook een **inbreuk** in verband met persoonsgegevens **melden** aan de toezichthoudende autoriteit (art. 33) en aan de betrokkene wanneer deze waarschijnlijk een hoog risico inhoudt voor diens rechten en vrijheden (art. 34).

MILIEURISICO'S

Een uitvoerige uitleg over de **milieueffectbeoordeling, milieueffectrapportering en productnormen** kan worden teruggevonden in de toelichting van "Hoofdstuk 6: Ethische vereiste 6 - maatschappelijk en milieuwelzijn".

Werd de afhankelijkheid van de beslissingen van een kritiek AI-systeem beoordeeld op zijn stabiel en betrouwbaar gedrag?

Werden de betrouwbaarheids-/testvereisten aangepast aan de gepaste niveaus van stabiliteit en betrouwbaarheid?

ALGEMEEN

AI-systemen zijn in de regel softwaretoepassingen die leren. Hun **betrouwbaarheid** is daarom in alle omstandigheden **essentieel**. Betrouwbaarheid betekent dat het AI-systeem doet waarvoor het is ontworpen. De betrouwbaarheid van software is voor gebruikers in de praktijk moeilijker te voorspellen. Software is immers niet zichtbaar: de gebruiker ervaart slechts de grafische interface, maar ziet geen fouten in het ontwerp van de software. Voor AI-systemen is dit nog moeilijker, net omdat deze systemen zichzelf bijsturen.

CYBERBEVEILIGINGSWETGEVING

Het opzet van een **cyberbeveiligingscertificeringsregeling** is onder meer dat de afhankelijkheid en kwetsbaarheden worden opgespoord. Indien deze gekend zijn moeten ze worden gedocumenteerd. Verder is er op dit punt een 'Trustworthiness' standaard in ontwikkeling bij de ISO.

PRODUCTVEILIGHEID EN PRODUCTAANSPRAKELIJKHEID

De veiligheid van producten en diensten houdt in dat het product of de dienst bij normale of redelijkerwijze te verwachten gebruiksomstandigheden **geen enkel risico oplevert, dan wel slechts beperkte risico's die verdedigbaar zijn met het gebruik** en vanuit het oogpunt van een hoog beschermingsniveau voor de gezondheid en de veiligheid van personen, aanvaardbaar wordt geacht.

In de Wet Productaansprakelijkheid wordt een gebrekkig product gedefinieerd als een product dat niet de **veiligheid biedt die men normalerwijze gerechtvaardigd** is te verwachten. Om dit correct in te schatten, moet ook de **betrouwbaarheid van het systeem** voldoende worden ingeschat. Men moet de foutenmarge ook correct inschatten. Verder voorzien de specifieke productregelgevingen ook vereisten inzake de betrouwbaarheid van de producten (wanneer die bv. gebruik maken van AI). Een voorbeeld kan worden gevonden in Bijlage 1 van het KB van 12 augustus 2008 betreffende het op de markt brengen van machines. Dit voorziet als één van de essentiële vereisten ook 'betrouwbaarheid'.

ALGORITMISCHE HANDEL

De verplichting om de weerbaarheid van handelssystemen te garanderen in artikel 22 van de Wet van 21 november 2017 en het KB van 19 oktober 2017 werden reeds besproken.. Verder kan worden verwezen naar de operationele vereisten in de Gedelegeerde Verordening 2017/589, o.a. omtrent de regelingen ter

verzekering van de bedrijfscontinuïteit, realtimemonitoring en beveiliging.

Werd een foutentolerantie gedefinieerd door bijvoorbeeld een gedupliceerd systeem of een ander parallel systeem (op AI gebaseerd of conventioneel)?

Werd een mechanisme gebouwd om te evalueren of een AI-systeem is veranderd om een nieuwe beoordeling van technische robuustheid en veiligheid te waarborgen?

ALGEMEEN

In de beoordeling van de informatieveiligheid kan gebruik worden gemaakt van **gedupliceerd systemen of parallelle systemen**, waarop vervolgens de nodige testing kan gebeuren. Onder andere de LINDDUN-bedreigingsmodelleringsmethode werkt op deze manier.

PRODUCTVEILIGHEID

Art. IX.8 §2 van het WER voorziet in de verplichting van producenten om de **passende maatregelen** te nemen om op de hoogte te blijven van de risico's van deze producten en diensten, alsook de passende acties te nemen om deze risico's te voorkomen. De distributeurs moeten ook op de hoogte blijven van de risico's van de producten en informatie melden aan de producenten.

CYBERVEILIGHEID

Ook de **verplichtingen in de NIS-wet** zijn niet beperkt in de tijd en gelden dus in principe gedurende de hele activiteit van de verlener van essentiële diensten of de digitaledienstverlener. Deze regels gelden echter niet voor micro- of kleine ondernemingen zoals bepaald in art. 32.

De Cyberbeveiligingsverordening stelt dat een cyberbeveiligingscertificeringsregelingen zorgt dat een aantal beveiligingsdoelstellingen worden verwezenlijkt. Eén daarvan is dat ICT-producten, -diensten en -processen worden geleverd **met actuele software en hardware die geen algemeen bekende kwetsbaarheden bevatten, en met mechanismen voor beveiligde updates** (art. 51).

CONSUMENTENRECHT

De relevante bepalingen rond **beveiligingsupdates** onder consumentenregelgeving werden reeds besproken.

BESCHERMING VAN PERSOONSGEGEVENS

Verschillende bepalingen over de **beveiliging van de verwerking** in art. 32, lid 1 van de AVG maken duidelijk dat de veiligheidsverplichting permanent is. Dit impliceert dat ook voor AI-systemen telkens

de maatregelen op gezette tijdstippen moeten worden geëvalueerd. Een **GEB** wordt ook niet alleen uitgevoerd bij aanvang van een verwerking van persoonsgegevens, maar ook wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden. Dit omvat geen essentiële verplichting om regelmatig te controleren, maar gelet op de risico's en onvoorspelbaarheid van AI-systemen is het aangeraden om minstens een systeem te hebben om nieuwe risico's te melden (art. 35).

ALGORITMISCHE HANDEL

De algemene verplichting voor aanbieders van diensten m.b.t. algoritmische handel om weerbare systemen te ontwikkelen werd reeds besproken. Inzake de technische vereisten kan o.a. worden verwezen naar de verplichtingen inzake jaarlijkse zelfbeoordeling in afdeling 2 Gedelegeerde Verordening 2017/589.

MILIEUVEILIGHEID

Dit wordt uitvoeriger besproken bij de "Hoofdstuk 6: Ethische vereiste 6 - maatschappelijk en milieuwelzijn".

2.2.C. Nauwkeurigheid

Kan een laag niveau van nauwkeurigheid van het AI-systeem resulteren in een kritieke, vijandige of schadelijke gevolgen?
Werden maatregelen genomen om ervoor te zorgen dat de (trainings)data die gebruikt wordt om het AI-systeem te ontwikkelen: (1) up-to-date zijn, (2) van hoge kwaliteit zijn, (3) volledig zijn en (4) representatief zijn van de omgeving waarin het systeem zal worden gebruikt?

GEGEVENSBESCHERMING

Volgens de AVG moeten persoonsgegevens **juist zijn en zo nodig worden geactualiseerd** (art. 5). De persoonsgegevens die in het AI-systeem worden ingevoerd, dienen op zijn minst **correct en accuraat** te zijn. De verwerkingsverantwoordelijke is dus in principe verplicht om de persoonsgegevens die hij verwerkt periodiek te updaten. Dit is echter niet altijd mogelijk aangezien de informatie over de juistheid in de praktijk vaak zal komen van de betrokkene zelf, die bijvoorbeeld nieuwe gegevens meedeelt of een verzoek tot correctie formuleert (art. 16). Iedere **rectificatie** dient wel aan elke ontvanger van de persoonsgegevens te worden meegedeeld (art. 19). Verder dient het proces ook op die manier te worden georganiseerd dat voormelde **principes worden nageleefd** op grond van de verplichting om gegevensbescherming door ontwerp te realiseren (art. 25).

PRODUCTVEILIGHEID

De veiligheidsverplichting van producenten (art. IX.2 WER) houdt in dat er moet worden gezorgd dat

het AI-systeem **geen onnauwkeurigheden** bevat die kunnen leiden tot een schadegeval. Deze risico's moeten permanent worden **gemonitord** (art. IX.8 WER). ISO voorziet ook in relevante internationale normen voor AI-systemen.

CONSUMENTENBESCHERMING

De vereiste van **nauwkeurigheid** kan ook een deel vormen van de objectieve conformiteitsvereisten binnen de Richtlijn Digitale Inhoud (art. 8) en de Richtlijn Consumentenkoop (art. 7).

DISCRIMINATIERECHT

Zie voor meer uitleg de bespreking "Hoofdstuk 5: Ethische vereiste 5 - diversiteit, non-discriminatie en rechtvaardigheid".

Werd een systeem in werking gesteld om de nauwkeurigheid van het AI-systeem te monitoren en documenteren?

GEGEVENSBESCHERMING

De **veiligheidsverplichting** in de AVG werd reeds besproken. Die omvatten onder andere een procedure voor het op gezette tijdstippen **testen, beoordelen en evalueren** van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking (art. 32 AVG).

PRODUCTVEILIGHEID

De **bewakingsplicht** onder art. IX.8 §2 WER werd al besproken. De producenten moeten de nauwkeurigheid van het AI-systeem **monitoren en documenteren**. Het uitvoeren van steekproeven en de bewakingsplicht zorgen voor documentatie die dit mogelijk maakt. Ook de distributeurs hebben een verplichting om de veiligheid te bewaken door verschillende maatregelen (art. IX.8, §3).

Verder hebben zowel producenten als distributeurs een **meldingsplicht** aan het Centraal Meldpunt voor Producten (art. IX.8, §4).

Ook op grond van de specifieke productreglementeringen dienen de kenmerken van elk product minstens in kaart te worden gebracht. Veel voorkomende verplichtingen zijn immers dat de fabrikant minstens een **conformiteitsbeoordelingsprocedure** moet (laten) uitvoeren. Ook moet de fabrikant **technische documentatie** opstellen. Deze technische documentatie moet toelaten te beoordelen of het product aan de relevante eisen voldoet (bv. medische hulmiddelen of machines).

CYBERBEVEILIGING

De verplichtingen van de actoren om risico's te identificeren en passende maatregelen te nemen onder de NIS-wet werden reeds aangehaald. Digitaledienstverleners zijn dus verplicht om alle risico's bij te houden en te documenteren (art. 30). Ze zijn ook verplicht om incidenten te melden (art. 35 e.v.). Ook onder de Cyberbeveiligingsverordening moeten actoren afhankelijkheden nagaan en kwetsbaarheden documenteren (art. 51). De gecertificeerde fabrikant of de aanbieder van ICT-producten, -diensten en -processen moet ook bepaalde informatie openbaar maken (art. 55).

ALGORITMISCHE HANDEL

Ook de MiFID II-wetgeving (hierboven reeds besproken) en de Gedelegeerde Verordening voorzien in een permanente zelfbeoordeling, in functie waarvan aanbieders van systemen voor algoritmische handel systematisch moeten beoordelen of hun systemen voldoende weerbaar zijn. Zij zijn verplicht in functie hiervan zichzelf permanent aan te passen.

	Werden processen in werking gesteld om te verzekeren dat het nauwkeurigheidsniveau van het AI-systeem dat eindgebruikers en/of betrokkenen mogen verwachten op degelijke wijze werd gecommuniceerd?

De **communicatieverplichtingen** werden reeds besproken en komen ook aan bod bij de bespreking van "Hoofdstuk 4: Ethische vereiste 4 - transparantie".

BETROUWBAARHEID, FAILSAFE-PLANNEN EN REPRODUCEERBAARHEID

	Kan het AI-systeem kritieke, vijandige, of schadelijke gevolgen (bijvoorbeeld voor de menselijke veiligheid) hebben in geval van een lage betrouwbaarheid en/of reproduceerbaarheid?

De verplichting om de betrouwbaarheid op te volgen houdt dezelfde regelgeving in als de algemene **verplichtingen tot beveiliging en bewaking** van de veiligheid. Deze werden reeds besproken.

	Werd een goede gedefinieerd proces voorzien om op te volgen of het AI-systeem de beoogde doelen bereikt?

GEGEVENSBESCHERMINGSRECHT

Persoonsgegevens moeten **toereikend zijn, ter zake dienend en beperkt** tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (art. 5, lid 1, c) AVG). Verder is de verwerking van persoonsgegevens maar toegestaan indien de verwerking noodzakelijk is voor één van de rechtsgronden

die in art. 6 AVG worden opgesomd. Al deze doeleinden moeten worden vermeld in het **register** van gegevensverwerkingen (art. 32 AVG).

PRODUCTVEILIGHEID

In dit verband is de reeds besproken **bewakingsplicht** relevant. Vooral het bijhouden van de technische documentatie en het bijhouden van o.a. een klachtenregister, alsook de algemene verplichting om steekproeven te nemen teneinde op de hoogte te blijven van alle risico's die aan producten verbonden zijn springen in het oog (art. XI.8 WER)

ALGORITMISCHE HANDEL

De verplichtingen zoals opgenomen in de MiFiD II-wetgeving werden hierboven reeds besproken. Als technische vereisten kan worden verwezen naar de verplichtingen inzake jaarlijkse zelfbeoordeling en validatie, stresstests en het beheer van materiële wijzigingen.

Werd getest of specifieke contexten of voorwaarden in acht moeten worden genomen om de reproduceerbaarheid te verzekeren?

Hiervoor gelden de **algemene vereisten** inzake productveiligheid. De cyberveiligheidsstandaarden zijn vooral gericht op het weerstaan van aanvallen, niet zozeer op gebreken inzake het AI-model. Er lijken op het eerste zicht geen specifieke standaarden beschikbaar voor de reproduceerbaarheid van AI-systemen.

Werden verificatie- en validatiemethoden en documentatie (bijvoorbeeld logging) voorzien om verschillende aspecten van de betrouwbaarheid en de reproduceerbaarheid van het AI-systeem te evalueren en te verzekeren?
Werden processen om de betrouwbaarheid en de reproduceerbaarheid van het AI-systeem te testen op een duidelijke wijze gedocumenteerd en geoperationaliseerd?

GEGEVENSBESCHERMINGSRECHT

Volgens de AVG is een **register van verwerkingsactiviteiten** vereist (art. 30), een **lijst van gevenslekken** (art. 33), alsook de **voorgeschreven maatregelen** die daarbij moeten worden genomen en worden gedocumenteerd. Ook de **GEB** kan als een vorm van logging beschouwd worden (art. 35). Zie hierover ook "Hoofdstuk 3: Ethische vereiste 3 - privacy en databeheer".

CYBERVEILIGHEID

De relevante bepalingen rond de **identificatie van risico's** en het nemen van **passende technische en organisatorische maatregelen** onder de NIS-wet kwam al aan bod (art. 33). Daarnaast is er ook

een **meldingsplicht** van incidenten (art. 35-37). De Uitvoeringsverordening 2018/151 bepaalt dat de digitaledienstverlener een aantal maatregelen kan nemen met betrekking tot de behandeling van incidenten (art. 2). De **certificeringsregeling** onder de Cyberbeveiligingsverordening test ook op de vraag of er logging is voorzien die ervoor zorgt dat de veiligheid van de verschillende systemen gewaarborgd blijft (art. 51).

MILIEUVEILIGHEID

Hier kan meer informatie over worden gevonden bij de bespreking van "Hoofdstuk 6: Ethische vereiste 6 - maatschappelijk en milieuwelzijn".

ALGORITMISCHE HANDEL

In het kader van de technische en organisatorische vereisten ter naleving van de beveiligingsplicht uit de MiFiD II-wetgeving kan o.a. worden verwezen naar de conformiteitstests, alsook de jaarlijkse zelfbeoordeling.

Werd voorzien in een geteste failsafe-methodes om systeemfouten van eender welke oorsprong aan te pakken en zijn er bestuursprocessen om deze methodes te activeren?

ALGEMEEN

Een failsafe is methode die ervoor zorgt dat het AI-systeem bij een fout **stopt** of terugkeert naar een veilige stand.

STANDAARDEN

Op het niveau van de IEEE is thans een standaard in opmaak voor het failsafe ontwerp van autonome systemen: P7009 Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems. Meer informatie vindt u hier.

ALGORITMISCHE HANDEL

Afdeling 3 van Gedelegeerde Verordening 2017/589 met betrekking tot technische reguleringsnormen tot specificering van de organisatorische vereisten voor beleggingsondernemingen die zich met algoritmische handel bezighouden voorziet in verschillende beveiligingsverplichtingen. Er moet bijvoorbeeld een **kill-functionaliteit** worden ingebouwd (art. 12).

ALGEMENE VEILIGHEIDSWETGEVING

Producenten zijn verplicht om uitsluitend **veilige** producten op de markt te brengen en veilige diensten aan te bieden (art. IX.2 WER). Om aan dit veiligheidsvermoeden te voldoen, kan beroep worden gedaan op geharmoniseerde normen die van toepassing zouden zijn op AI-systemen (art. IX.3 WER).

SPECIFIEKE SECTORALE REGELGEVING

Verder kan het zijn dat in bepaalde sectorale regelgeving een failsafe-methode moet worden voorzien als onderdeel van één van de **essentiële vereisten**. Denk bijvoorbeeld aan machines (punt 1.2.1. van Bijlage 1) of medische hulpmiddelen.

CYBERVEILIGHEID

De NIS-wet verplicht de aanbieder van essentiële diensten en de digitaledienstverleners om **passende maatregelen** te nemen om incidenten te voorkomen of de gevolgen ervan te minimaliseren, teneinde de continuïteit van deze diensten te waarborgen (art. 20 en 33). Ook de Uitvoeringsverordening 2018/151 bevat bepalingen over **rampenplannen en uitwijkcapaciteiten** (art. 2, lid 3). Deze rampenplannen maken duidelijk dat er voor de netwerk- en informatiesystemen een failsafe moet zijn. In dit verband is ook ISO 27001:2017 relevant.

De Cyberbeveiligingsverordening stelt ook uitdrukkelijk als beveiligingsdoelstellingen voorop dat bij een fysiek of technisch incident **de toegang wordt hersteld** en ICT-producten, -diensten en -processen door standaardinstellingen door ontwerp veilig zijn (art. 51).

GEGEVENSBESCHERMING

De AVG voorziet in een eerste failsafe als er fouten zijn bij geautomatiseerde individuele besluitvorming waaronder profilering (art. 22). Een andere failsafe is de uitoefening van het recht op **rectificatie** (art. 16) en op de **beperking van de verwerking** (art. 18).

Werd een degelijke procedure aangenomen wanneer het AI-systeem resultaten voorziet met lage betrouwbaarheidsscore?

PRODUCTVEILIGHEID

Deze verplichting valt onder de **algemene verplichting** conform art. IX.8 WER om de nodige maatregelen te nemen om ten allen tijde op de hoogte te blijven van de risico's die gelden aangaande de producten en/of diensten die men op de markt brengt.

GEGEVENSBESCHERMINGSRECHT

Er kan verwezen worden naar het **recht op bezwaar tegen uitsluitend op geautomatiseerde verwerking waaronder profilering** (art. 22 AVG) en het **recht op rectificatie** (art. 16). Ook regels in verband met de GEB zijn relevant (art. 35 AVG). Deze maatregelen dienen om lage betrouwbaarheid – of althans de gevolgen daarvan – te voorkomen.

CONSUMENTENRECHT

Zowel de Richtlijn Digitale Inhoud als de Richtlijn Consumentenkoop voorzien uitdrukkelijk in de verplichting om de **updates** te bieden die de consument zou mogen verwachten.

CYBERVEILIGHEID

De definitie van 'beveiliging van netwerk- en informatiesystemen' in Richtlijn 2016/1148 wijst op de **resiliëntie**, maar niet noodzakelijk op de betrouwbaarheid van het AI-systeem als dusdanig. Andere normen zijn dus nodig om dit kader aan te vullen.

ALGORITMISCHE HANDEL

De MiFiD II-wetgeving voorziet uitdrukkelijk in de verplichting om doeltreffende regelingen te treffen om o.a. de continuïteit van de dienstverlening te verzekeren in geval van stortingen. Indien een AI-systeem beperkte betrouwbaarheid toont, is dit voorzien. In Gedelegeerde Verordening 2017/589 kan o.A. worden verwezen naar de in afdeling II vooropgestelde controlemethoden.

Vereist het AI-systeempermanent (online) leren?
Werd rekening gehouden met mogelijke negatieve gevolgen doordat het AI-systeem nieuwe of ongebruikelijke methoden heeft geleerd om goed te scoren op zijn objectieve functie?

PRODUCTVEILIGHEID

Ook hier moet naar de **algemene veiligheidsverplichtingen** worden verwezen (art. IX.8 WER). Gedurende de levenscyclus van het AI-systeem moet er worden gewaakt over de vraag of het AI-systeem doet wat het moet doen op de correcte manier. De vraag rijst naar hoe dit in de praktijk dient te worden omgezet. Een belangrijk element hiervan zal zijn dat de code van AI-systemen te allen tijde transparant is. Zie hierover ook de bespreking onder "Hoofdstuk 4: Ethische vereiste 4 - transparantie". Transparantie, zgn. 'uitlegbare' AI, kan echter ook een belemmering voor innovatie zijn. Een gepast evenwicht tussen transparantie en functionaliteit is dan ook nodig.

2.3. Waar zitten mogelijke punten van verbetering of aandachtspunten?

Convergentie en coherentie tussen de verschillende veiligheidsregimes

Eén van de voornaamste kenmerken van (goed) technologiebeleid is **technologieneutraliteit**. De regels moeten kunnen worden toegepast in om het even welke technologische context en moeten bestand zijn tegen wijzigingen in de technologie.

In de diverse rechtsdomeinen die deze ethische vereiste ten uitvoer brengen, wordt dit op een redelijk adequate manier gerealiseerd. De veiligheidsstandaarden worden altijd gekoppeld aan begrippen als 'passend' en 'veilig', die op hun beurt worden gekoppeld aan de op het moment van de ingebruikname gekende risico's. Deze aanpak – de Nieuwe Aanpak van de Europese Commissie – laat flexibiliteit toe: de algemene regels verwijzen naar standaarden die vanuit de markt worden opgesteld. Dit laat toe dat entiteiten met expertise de verdere standaarden waar nodig uitbouwen om veiligheidsrisico's op te vangen. Dit is niet noodzakelijk gebonden aan het product zelf.

Door doorgedreven digitalisering en het gebruik van AI-systemen is een **verdergaande convergentie** tussen regimes noodzakelijk. Meerdere (veiligheids)regimes zijn van toepassing op fysieke (lichamelijke) producten en dus op AI-systemen die in hardware zijn ingebed. Het cyberveiligheidsregime is vooral gericht op het verhinderen van externe aanvallen. Het onderscheid op grond van het type product, en niet het risico, lijkt echter arbitrair. Verder staan de normering en certificatie voor ICT-systemen in het algemeen en voor AI-systemen in het bijzonder nog in hun kinderschoenen (hoewel er binnen ISO al heel wat werk wordt verricht). Slechts enkele specifieke regimes zoals de regels inzake medische hulpmiddelen en algoritmische handel voorzien in regels die deze convergentie volgen.

Het **regelgevend regime voor veiligheid moet de huidige digitale en AI-gedreven realiteit volgen**. Voorlopig is dit enkel van toepassing voor sommige toepassingen, zoals algoritmische handel. Sommige initiatieven zijn reeds onderweg, zoals de Richtlijn Digitale Inhoud en de Richtlijn Consumentenkoop. Verdere ontwikkeling van de andere regimes is vereist, waarbij de basis van de Nieuwe Aanpak behouden moet blijven om flexibiliteit en rechtszekerheid te garanderen. **Interdisciplinaire samenwerking** tussen industrie en academische instellingen rond certificering van AI-systemen is ook nuttig.

Er zijn weinig tot geen failsafe-methodes als vereiste of manieren om als consument een rechtzetting te vereisen. Het is prioritair dat er, net zoals bij algoritmische handel, **criteria** worden ontwikkeld die bepalen wanneer een failsafe- of kill-knop nodig zijn. Indien de AVG van toepassing is, kan een betrokkene zijn recht op bezwaar uitoefenen tegen uitsluitend op geautomatiseerde verwerking waaronder profilering. Aangezien het beperkt is tot natuurlijke personen betekent dit dat bedrijven geen bezwaar kunnen

uitoefenen indien een beslissing automatisch werd gemaakt die juridische gevolgen heeft. Deze gevolgen zijn vandaag al aanwezig in de automatische censuur van bedrijven zoals Facebook in hun strijd tegen fake news.

Toegang tot technische normen

Een ander verbeterpunt betreft de **toegang tot normen en standaarden**. Normen en standaarden zijn voor ontwikkelaars essentieel om te weten aan welke eisen hun producten of diensten moeten voldoen. Deze standaarden zijn beschikbaar tegen betaling via kanalen zoals de NBN-webshop. Deze kosten kunnen voor sommige ontwikkelaars prohibitief worden. Het lijkt dus aangewezen om meer toegang te voorzien tot technische normen en regelgeving, naar analogie met de mogelijkheid om het Belgisch recht te raadplegen. Dit kan zowel via private initiatieven (databanken) als via regulering.

Grote verantwoordelijkheid bij de gebruiker

Er zijn verschillende informatie-, waarschuwings- en veiligheidsplichten ten aanzien van gebruikers. Daarbij bestaat het risico dat de gebruikers overweldigd worden door de (hoeveelheid) informatie, waardoor ze hun rechten niet altijd zullen/kunnen uitoefenen. Bovendien is de eindgebruiker vaak een leek en moet dus worden nagedacht over manieren waarop de bescherming van de gebruiker efficiënt(er) kan worden georganiseerd.

Verduidelijking juridische concepten

Er is nood aan een **aanvulling, aanpassingen of verduidelijking van het toepasselijke wetgevende kader**. Het begrip 'product' verwijst in de toepasselijke wetgeving niet expliciet naar software. Los van de vraag naar de uiteindelijke kwalificatie van software is het alvast aangewezen dat hier binnen korte termijn duidelijkheid over komt. Een gelijkaardig probleem stelt zich met betrekking tot het begrip 'gebrek' en de legitieme veiligheidsverwachtingen van het grote publiek met betrekking tot AI-systemen.

2.4. Welke tools kunnen worden gebruikt om aan de ethische vereiste te voldoen?

CYBERVEILIGHEID

- Cyberveiligheidstool van het Centrum voor Cybersecurity België om te testen hoe men de cyberveiligheid naleeft.
- De verschillende bedreigingsmodelleringen o.a.
    - Open Web Application Security Project voorziet in een lijst van de 10 meest frequente veiligheidsrisico's voor webapplicaties;
- LINDDUN.
- De kaders in verband met penetratietesten
    - OSSTMM;
    - OWASP Web Application Penetration Checklist;
    - Penetration Testing Execution Standard.

NORMEN

- Toegang via databank myNBN tot verschillende normen die in België van toepassing zijn.
- Toegang via het WTCB tot normen in verband met bouwproducten.

PRODUCTVEILIGHEID

- De autoriteiten van de EU voorzien een tool voor de melding van gevaarlijke producten.

GEGEVENSBESCHERMING

- De CNIL voorziet in een tool voor het uitvoeren van een GEB.
- De Gegevensbeschermingsautoriteit voorziet in een standaardtool voor het melden van gegevenslekken.

Hoofdstuk 3: Ethische vereiste 3 - privacy en databeheer

3. Ethische vereiste 3: privacy en databeheer

3.1. Wat betekent de ethische vereiste?

Deze ethische vereiste heeft betrekking op de grondrechten van eenieder op bescherming van het privéleven en het nauw daaraan verwante recht op gegevensbescherming. Deze rechten dragen bij aan het beschermen van de mentale en fysieke integriteit van natuurlijke personen. Het beginsel 'preventie van schade' speelt dan ook een belangrijke rol bij deze ethische vereiste. Om deze schade in de praktijk te beperken, is een doorgedreven **risico-gebaseerde benadering** nodig die op zich een performante data-governance (databeheer) vereist.

Deze ethische vereiste dekt de volgende **drie sub-componenten** (1) privacy en gegevensbescherming, (2) kwaliteit en integriteit van gegevens en (3) toegang tot gegevens.

Ten eerste heeft deze betrekking op **privacy en gegevensbescherming**.

AI-systemen hebben doorgaans een grote honger naar informatie en data. Daarbij moet tijdens de gehele levenscyclus van het AI-systeem vermeden worden dat onwettige/ongegronde informatie verzameld, verwerkt of gegenereerd wordt die tot de privésfeer van de betrokkenen hoort of die daar een ongewenste inkijk in verschaft. Bij het verwerken en het genereren van persoonsgegevens moet rekening gehouden worden met het recht van de betrokkenen om deze gegevens niet te laten verwerken. Daarbij moet bijzonder gewaakt worden over het feit dat uit rechtmatig verwerkte informatie geen conclusies getrokken worden die aspecten van iemand leven blootleggen die deze persoon niet wenst te delen of schade kunnen berokkenen. Persoonsgegevensverwerking kan immers een grote impact hebben op iemands rechten en vrijheden en resulteren in ernstige lichamelijke, materiële of immateriële schade (bv. discriminatie, reputatieschade, identiteitsdiefstal of -fraude, financiële verliezen of verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegeven). De naleving van de relevante regels is daarom vereist om aan burgers het nodige vertrouwen in AI-systemen te geven, zodat zij in volle vertrouwen hun gegevens met deze systemen kunnen delen, wetende dat zij hier niet onterecht door benadeeld zullen worden.

Ten tweede heeft deze ethische vereiste betrekking op de **kwaliteit en integriteit van gegevens**.

De kwaliteit van de gegevens die gebruikt worden om AI-systemen te trainen is essentieel om een kwalitatieve uitkomst te verzekeren. Daarbij is van groot belang dat de gegevens accuraat, voldoende breed en representatief zijn, maar ook dat ze geen sociaal geconstrueerde vertekeningen of onnauwkeurigheden (bias) bevatten. Ook in de ontwikkelingsfases en de gebruiksfase moet gewaakt worden over de kwaliteit van de gegevens door systematische tests en controles uit te voeren op zowel

de gegevenssets als de processen en deze controles te documenteren.

Tot slot heeft deze ethische vereiste betrekking op **toegang tot gegevens**.

De bescherming van persoonsgegevens begint bij een degelijk toegangsbeleid tot persoonsgegevens. Door de toegang tot de eigenlijke persoonsgegevens te beperken tot die personen en die situaties waarin die toegang werkelijk nodig is, wordt de blootstelling hiervan beperkt en de risico's op zowel een goedwillige als kwaadwillige datalekken aanzienlijk verminderd.

3.2. Welke regels zijn een uitdrukking van de ethische vereiste of kunnen dienen als inspiratiebron?

De ALTAI lijst voorziet vragen op basis van de indeling privacy – databeheer. Hierna geven we op basis van dezelfde indeling per vraag weer hoe deze (al dan niet) opgevangen worden door bestaande regelgeving.

3.2.A. Privacy

Werd nagedacht over de gevolgen van het AI-systeem voor het recht op privacy, het recht op fysieke, mentale en/of morele integriteit en het recht op gegevensbescherming?

Gelet op het onderdeel waaronder deze vraag valt, wordt het recht op fysieke, morele en mentale integriteit geïnterpreteerd als samenhangend of voortkomend uit (een schending van) de rechten op privacy en gegevensbescherming. Gegevensbescherming is **verregaand gereguleerd** en de verplichting om persoonsgegevens doordacht te verwerken volgt dan ook reeds uit een groot aantal nationale en internationale bepalingen.

GRONDRECHTEN

Art. 8 van het Handvest van de grondrechten van de Europese Unie (Handvest) en art. 16 van het Verdrag betreffende de werking van de Europese Unie (VWEU) bevestigen dat eenieder recht heeft op bescherming van zijn persoonsgegevens.

Art. 7 van het Handvest, art. 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (BUPO) en art. 22 van de Belgische Grondwet bevestigen het recht op de bescherming van het privéleven. De erkenning van de bescherming van het privéleven en persoonsgegevens als fundamentele rechten impliceert reeds dat het verwerken van informatie die daar afbreuk aan kan doen, een doordachte en door de wet ondersteunde aanpak vereist.

EUROPESE REGELGEVING

Het gegevensbeschermingsrecht is op Europees niveau in grote mate geharmoniseerd door de **AVG**. De AVG regelt de verwerking van persoonsgegevens op uitgebreide en gedetailleerde wijze en geldt als de 'basiswetgeving' voor elke verwerking van persoonsgegevens. De AVG heeft een **risico-gebaseerde benadering**. Dit uit zich onder meer in verplichtingen om vooraf aan een verwerking de risico's te evalueren, maar heeft ook algemeen als gevolg dat bij elke verwerking geëvalueerd moet worden of die verwerking een mogelijke impact heeft op de rechten en vrijheden van de betrokkenen. Het voornaamste doel van deze bepalingen is om de betrokkenen, wiens gegevens verwerkt worden, te beschermen tegen inbreuk op hun rechten en tegen schade.

De AVG moet samen gelezen worden met de richtlijnen en standpunten van het Europees Comité voor gegevensbescherming (European Data Protection Board of EDPB) en deze van de toezichthoudende autoriteiten die als soft law beschouwd kunnen worden. Ook de beslissingen van de toezichthoudende autoriteiten en de nationale en Europese rechtspraak dienen in aanmerking genomen te worden bij de interpretatie en toepassing.

Verschillende bepalingen uit de AVG verplichten naar gelang het geval ontwikkelaars, gebruikers en aanbieders van AI-systemen om **vooraf na te denken** over de impact van hun verwerking op de rechten van een betrokkene. We verwijzen in dit verband naar de eerder gepubliceerde gids over gegevensbescherming en AI waar reeds veel informatie kan worden gevonden. Daarin worden een aantal zaken uitvoerig behandeld. We bespreken hier kort een aantal belangrijke aspecten.

Persoonsgegevens mogen enkel worden verwerkt wanneer de **verwerkingsbeginselen** zoals bv. 'rechtmatigheid', 'transparantie', 'doelbinding' en 'minimale gegevensbescherming' worden nageleefd (art. 5). Deze beginselen verplichten om vooraf te zorgen dat zowel het verzamelen als het (verder) verwerken van persoonsgegevens conform deze beginselen (zullen) gebeuren. De verwerkings-verantwoordelijke en de verwerker moeten steeds in staat zijn om aan te tonen dat zij hun **verplichtingen** onder de AVG nakomen ('verantwoordelijkheidsplicht').

De AVG legt als kernbeginsel dus o.a. een **algemene transparantieverplichting** op bij elke verwerking van persoonsgegevens (art. 5.1 (a), (b) en 12 en overweging 58). Hieruit volgen onder meer een brede voorafgaandelijke informatieverplichting ten aanzien van personen bij wie persoonsgegevens verzameld worden en een gelijkaardige informatieverplichting op zeer korte termijn ten aanzien van betrokkenen wiens gegevens via derden verzameld werden (art. 12, 13 en 14 AVG). Voor meer informatie verwijzen we ook naar "Hoofdstuk 4: Ethische vereiste 4 - transparantie".

Betrokkenen wiens gegevens verwerkt worden, beschikken onder bepaalde voorwaarden over een aantal **specifieke rechten** ten aanzien van degene die hun gegevens verzamelen en verwerken, ook

als die verwerking kadert binnen de ontwikkeling, het gebruik of het aanbieden van een AI-systeem. Denk aan het recht van inzage, rectificatie, bezwaar of om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit (art. 15-22). Deze rechten verplichten de verwerkingsverantwoordelijke tot het op voorhand te zorgen dat de persoonsgegevens verwerkt worden op een manier die toelaat om aan deze rechten te voldoen. Ook zullen op voorhand de nodige processen opgezet moeten worden om adequaat op dergelijke uitoefening te kunnen reageren.

De verwerkingsverantwoordelijke moet **passende technische en organisatorische maatregelen** treffen teneinde een rechtsgeldige verwerking te waarborgen én te tonen (art. 24.1 AVG). Daarbij moet hij een passend gegevensbeschermingsbeleid opmaken, indien de omvang van de activiteiten dat vereist (art. 24.2 AVG). Dit lijkt ons in ieder geval van toepassing voor ontwikkelaars, aanbieders en gebruikers die handelen als verwerkingsverantwoordelijke. Een verwerkingsverantwoordelijke moet ook bij zowel de bepaling van de verwerkingsmiddelen als bij de verwerking zelf passende technische en organisatorische maatregelen treffen (art. 25). Ook hieruit volgt dat verwerkings-verantwoordelijken in een AI-context op voorhand moeten nadenken hoe AI-systemen impact kunnen hebben op de verschillende rechten van de betrokkenen en hoe ze deze adequaat kunnen vrijwaren.

De **GEB** omvat de meest concrete verplichting om vooraf na te denken over de risico's die het verwerken van persoonsgegevens kan hebben voor de rechten en vrijheden van natuurlijke personen. Een GEB moet op voorhand uitgevoerd worden bij elke verwerking waarbij vermoedelijk een hoog risico bestaat voor de betrokkenen (art. 35.1 AVG). Dit zal in regel steeds het geval zijn wanneer persoonsgegevens gebruikt worden in AI-systemen, in welke fase dan ook. Indien twijfel bestaat over de nood om een GEB uit te voeren, kan voorafgaand een pre-GEB (pre-DPIA) uitgevoerd worden. Daarvoor kan bijv. de 'handleiding GEB' van de Belgische Gegevensbeschermingsautoriteit gebruikt worden.

Een GEB beschrijft de verwerking van persoonsgegevens, beoordeelt de noodzaak en evenredigheid ervan en helpt om de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te beheren door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken. Hierdoor kunnen organisaties in het beginstadium van de ontwikkeling van een AI-systeem nagaan of er discriminerende elementen zijn of dat bepaalde personen uitgesloten zouden kunnen worden. Hoewel een GEB enkel verplicht is bij verwerkingen met een waarschijnlijk hoog risico, wordt het toch aangeraden deze ook in andere situaties uit te voeren. Het is immers een nuttig instrument dat organisaties helpt om de wetgeving inzake gegevensbescherming na te leven.

Daarbij kan bovendien vereist zijn dat de verwerkingsverantwoordelijke de toezichthoudende autoriteit raadpleegt voorafgaand aan de verwerking indien deze verwerking een hoog risico met zich meebrengt.

Binnen elke lidstaat is verplicht een **toezichthoudende autoriteit** actief, voor België is dat de Gegevensbeschermingsautoriteit of GBA (art. 51 AVG, zie ook de Belgische Wet tot oprichting van de

Gegevensbeschermingsautoriteit). De toezichthoudende autoriteit kan de niet-naleving van de AVG sanctioneren, onder andere door een stakingsbevel en administratieve geldboeten op te leggen. Deze laatste kunnen oplopen tot 20 miljoen euro of, indien hoger, een bedrag tot 4% van de totale wereldwijze omzet in het vorig boekjaar van de overtreder (art. 84 AVG).

Deze controle- en sanctiemogelijkheid, waarbij onder meer aangetoond moet kunnen worden dat vooraf over de risico's voor de betrokkenen nagedacht werd, verplicht degenen die persoonsgegevens verwerken bij gebruik, aanbieding of ontwikkeling van een AI-systeem om dat ook effectief te doen en dit onderbouwd te documenteren, zodat deze documentatie aan de toezichthoudende autoriteit kan voorgelegd worden.

Verder bevat de AVG nog een aantal andere relevante bepalingen die ex ante in overweging moeten worden genomen om mogelijke risico's op rechten van betrokkenen (bv. door de verwerking van persoonsgegevens door AI-systemen) in kaart te brengen. Denk bv. aan de verplichting om een **register van werkingsactiviteiten** bij te houden (art. 30), de **verwerking te beveiligen** door passende technische en organisatorische veiligheidsmaatregelen (art. 32), **gegevenslekken te melden** aan de toezichthoudende autoriteit en mogelijk ook aan de getroffen betrokkenen (art. 32 en 33), een functionaris voor gegevensbescherming of DPO aan te stellen (art. 35) en waarborgen te voorzien bij doorgeven van **persoonsgegevens aan derde landen** (art. 44-47).

BELGISCHE REGELGEVING

Aanvullend op en naast de AVG zijn er heel wat **nationale bepalingen** die minstens onrechtstreeks verplichten om na te denken over de gevolgen die een AI-systeem kan hebben op de betreffende rechten en vrijheden van de betrokkenen. De belangrijkste ervan worden hierna kort toegelicht.

De **Belgische Gegevensbeschermingswet** 'implementeert' (onder meer) de AVG en legt onder meer een aantal regels vast die conform de AVG bij nationale wet aangepast of ingevuld konden worden. De Gegevensbeschermingswet voorziet in het bijzonder in een afwijkende regeling voor overheden evenals voor verwerkingen buiten het toepassingsgebied van de EU.

Daarnaast bestaan er nog een aantal **specifieke wetten**, die telkens bepaalde aspecten reguleren die betrekking hebben op bepaalde verwerkingen van persoonsgegevens. Deze hebben steeds mede tot doel om de rechten van betrokkenen wiens gegevens verwerkt worden te beschermen. Afhankelijk van onder meer de context waarbinnen een AI-systeem gebruikt zal worden of van de herkomst van de gebruikte persoonsgegevens (bijv. voor training), zullen deze wetten als gevolg hebben dat nagedacht moet worden over de rechten die ze beschermen, minstens dat hiertoe bepaalde maatregelen moeten worden genomen.

Het betreft onder meer de volgende wetten:

- de Belgische Camerawet op het gebruik van bewakingscamera's;
- CAO nr. 68 betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats;
- de Wet Patiëntenrechten, die onder meer specifieke verplichtingen omvat voor elektronische communicatiedienstverleners, maar ook algemene verplichtingen van toepassing indien gebruik gemaakt wordt van cookies (bijv. in combinatie een AI-systeem gericht op direct marketing;
- de Wet Elektronische Communicatie;
- de Belgische NIS-wet, die een kader vaststelt voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;
- bepalingen uit het Wetboek Economisch Recht zoals deze van toepassing op het consumentenrecht (Boek VI) of het recht van de elektronische economie (Boek XII);
- de wet op het rijksregister, die op straffe van strafrechtelijke vervolging verbiedt om het rijksregisternummer te verwerken zonder machtiging. Dit kan dus ook niet in het kader van AI-systemen;
- CAO nr. 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens.

ANDERE NORMEN

Naast de internationale en nationale regels, kunnen ook **andere normen** aanzetten of nopen tot het op voorhand nadenken over de risico's die een verwerking kan betekenen voor de rechten van betrokkenen. De **(niet-bindende) ISO-normen** onder de ISO 27000-serie omvatten informatieveiligheidsnormen. Aanvullend daaraan kan ook gekeken worden naar de norm ISO 27701 die een uitbreiding vormt op ISO27001 en ISO 27002. De toepassing ervan vereist eveneens dat op voorhand nagedacht wordt over hoe bepaalde verwerkingen de rechten van betrokkenen kunnen schaden en de toepassing beschermt tot op zekere hoogte tegen de schending van deze rechten.

De **PCI-DSS-normen** of voluit de Payment Card Industry Data Security Standard zijn zelfregulerende informatieveiligheidsnormen opgelegd door de krediet- en betaalkaartenindustrie, waaraan voldaan moet zijn door betaaldienstaanbieders (payment service providers) om betalingen te kunnen uitvoeren, bijv. in een online omgeving of in een toepassing op een smartphone. Ze vereisen eveneens een vergaande voorafgaande risicoanalyse. Elk AI-systeem dat gebruik zou maken van dergelijk betaalsysteem, bv. in een gebruikersinterface, of dat de daarbij gebruikte data zou willen gebruiken, moet er rekening mee houden.

?	Werden afhankelijk van het toepassingsgeval mechanismen ingesteld die het mogelijk maken om bij het AI-systeem privacy-kwesties te identificeren?

De vereiste om privacy-kwesties tijdens de verwerking te identificeren hangt vanuit regelgevend oogpunt nauw samen met de hierboven besproken vereiste om op **voorhand na te denken over de risico's** die een AI-systeem kan betekenen voor de rechten van de betrokkenen. Dit niettegenstaande de vaststelling dat het in de praktijk wel nuttig is om beide vragen te stellen. Voor de hierop toepasselijke regels wordt dan ook verwezen naar degene die hierboven werden besproken. Deze vereisen eveneens dat **privacy-kwesties tijdens de verwerking geïdentificeerd** en **adequaat opgevolgd** kunnen worden.

3.2.B. DATABEHEER

Wordt het AI-systeem getraind of is het ontwikkeld door het gebruik of de verwerking van persoonsgegevens (inclusief speciale categorieën van persoonsgegevens)?

Deze vraag wordt gedekt door de verplichtingen volgend uit onder meer de **AVG**, de Belgische **Gegevensbeschermingswet** en **verschillende andere wetten** om voorafgaand aan iedere verwerking van persoonsgegevens en tijdens die verwerking aan de daarin opgenomen verplichtingen te voldoen. Voor een meer uitgebreid overzicht van de toepasselijke normen wordt verwezen naar hetgeen hierboven besproken werd.

Werd een van de volgende maatregelen genomen, waarvan sommige verplicht zijn op grond van de AVG of een niet-Europees equivalent?

- Gegevensbeschermingseffectbeoordeling;
- Aanwijzing van een functionaris voor gegevensbescherming en het betrekken hiervan in een vroeg stadium in de ontwikkelings-, inkoop- of gebruiksfase van het AI-systeem;
- Toezichtmechanismen voor gegevensverwerking (met inbegrip van het beperken van de toegang tot gekwalificeerd personeel, mechanismen voor het registreren van de toegang tot gegevens en het aanbrengen van wijzigingen);
- Maatregelen om gegevensbescherming door ontwerp en door standaardinstellingen te bekomen (bv. versleuteling, pseudonimisering, aggregatie, anonimisering);
- Minimalisering van gegevens, met name persoonsgegevens (met inbegrip van bijzondere gegevenscategorieën).

Zowel de vraag of deze maatregelen genomen moeten worden als de eventuele uitvoering ervan volgen uit de toepasselijke gegevensbeschermingswetgeving zoals de **AVG**, de Belgische **Gegevensbeschermingswet** en **verschillende andere wetten** om een risico-evaluatie te doen bij het verwerken van persoonsgegevens en desgevallende verplicht de met dat risiconiveau overeenstemmende maatregelen te nemen. Voor een meer uitgebreid overzicht van de toepasselijke normen wordt verwezen naar hetgeen reeds besproken werd.

	Werden het recht om toestemming in te trekken, het recht om bezwaar te maken en het recht om te worden vergeten in de ontwikkeling van het AI-systeem geïmplementeerd?

De verplichting om deze rechten te implementeren volgt rechtstreeks uit de **AVG** en wordt voor specifieke aspecten hernomen in specifieke wetgeving, zoals bv. in het **WER** en de **Camerawet**. Voor een meer uitgebreid overzicht van de toepasselijke normen wordt verwezen naar hetgeen hierboven reeds werd besproken.

	Werd rekening gehouden met de gevolgen voor de privacy en de gegevensbescherming van gegevens die in de loop van de levenscyclus van het AI-systeem worden verzameld, gegenereerd of verwerkt?

Deze vraag wordt gedekt door de verplichtingen volgend uit onder meer de AVG, de Belgische Gegevensbeschermingswet en verschillende andere wetten om voorafgaand aan iedere verwerking van persoonsgegevens en tijdens die verwerking aan de daarin opgenomen verplichtingen te voldoen, die oefening geldt eveneens voor de persoonsgegevens verzameld tijdens de levenscyclus van het AI-systeem. Voor een meer uitgebreid overzicht van de toepasselijke normen wordt verwezen naar wat reeds werd besproken.

	Werd rekening gehouden met de implicaties voor de privacy en gegevensbescherming van de trainingsgegevens die geen persoonsgegevens zijn of van andere verwerkte niet-persoonsgegevens?

Deze vraag wordt gedekt door de verplichtingen volgend uit onder meer de **AVG**, de Belgische **Gegevensbeschermingswet** en **verschillende andere wetten** om voorafgaand aan iedere verwerking van persoonsgegevens en tijdens die verwerking aan de daarin opgenomen verplichtingen te voldoen, die verplichting geldt eveneens voor de persoonsgegevens die gecreëerd kunnen worden tijdens de levenscyclus van het AI-systeem, alhoewel dit een vraag is die in de praktijk gemakkelijk over het hoofd gezien zal worden. Voor een meer uitgebreid overzicht van de toepasselijke normen wordt verwezen naar wat reeds werd besproken.

	Werd het AI-systeem afgestemd op relevante normen (bijv. ISO, IEEE) of algemeen aanvaarde protocollen voor (dagelijks) gegevensbeheer en -governance?

De vraag heeft betrekking op de vrijwillige toepassing van **normen of protocollen**.

Er zijn geen algemeen verplichte normen of protocollen van toepassing bij ontwikkeling, aanbieding of

gebruik van AI-systemen.

Voor nuttige normen kan gekeken worden naar de (niet-bindende) ISO-normen onder de **ISO 27000-serie**, die betrekking hebben op informatieveiligheid. Aanvullend daaraan kan ook gekeken worden naar de norm **ISO 27701** die een uitbreiding vormt op ISO27001 en ISO 27002. Ook de **PCI-DSS-normen** zijn relevant.

3.3. Waar zitten mogelijke punten van verbetering/ aandachtspunten?

Check-the-box attitude

Een algemeen probleem bij de toepassing van het gegevensbeschermingsrecht is de zgn. check-the-box attitude. Verplichtingen worden dan op een **formalistisch-administratieve** wijze ingevoerd, zonder dat ze effectief leiden tot een afdoende gegevensbescherming, noch tot een privacy-vriendelijke (bedrijfs-)cultuur. Het breder gegevensbeschermingsbeleid wordt dan (deels) gereduceerd tot een papieren tijger, waarbij op papier alle(rlei) maatregelen en processen aanwezig zijn, die in de praktijk niet worden toegepast.

Vanuit het beleid moet worden nagedacht hoe organisaties kunnen worden aangezet tot het **effectief bevorderen van een privacy-vriendelijke cultuur**. Dit kan bijvoorbeeld worden gedaan door het organiseren van workshops en verdere informatieverspreiding.

Gebrek aan duidelijkheid

Ondanks de vergaande harmonisering van het gegevensbeschermingsrecht via de AVG bestaan tot op heden nog heel wat **vragen bij hoe bepaalde principes toegepast moeten worden**. Mede ingevolge de jonge leeftijd van de AVG en de continue technologische evolutie is het gegevensbeschermingsrecht nog in volle ontwikkeling. In de maand september 2020 werd bv. nog een ontwerp-richtlijn bekend gemaakt, open voor consultatie, over de concepten verwerkingsverantwoordelijke en verwerker en een andere over gerichte reclame via sociale media.

Tegelijkertijd krijgt de invulling van de AVG ook vorm door de **verschillende nationale bepalingen** dienaangaande, door de sancties, beslissingen en adviezen van de nationale toezichthoudende autoriteiten en door de zich daarover ontwikkelende rechtspraak en rechtsleer.

Dit alles terwijl organisaties de AVG in de praktijk moeten toepassen en nieuwe standpunten en richtlijnen soms ingaan tegen of voorwaarden toevoegen aan bestaande goede praktijken. Dit wordt des te complexer in een AI-context, aangezien veel van deze regels moeilijk toepasbaar zijn in verschillende AI-contexten. Er blijft dus ook **nood aan verduidelijking** van hoe de AVG toe te passen en dit in het bijzonder in een AI-context. Als stap bij het lenigen van deze nood verwijzen wij graag naar onze verkennende gids 'Artificiële intelligentie en gegevensbescherming'.

Onvoldoende kennis in startup omgeving

In de praktijk blijkt vaak dat startups zich **vaak onvoldoende bewust** zijn of onvoldoende bezighouden met gegevensbescherming. Ook hier kunnen workshops en gerichte informatiecampagnes worden georganiseerd.

Gebrek aan voorlichting en handhaving

De Gegevensbeschermingsautoriteit voert sinds meer dan een jaar actief inspecties uit. Er werden bijna 100 beslissingen uitgesproken in geschillendossiers (oktober 2020) en er wordt ook actief aan voorlichting gedaan. Er moet echter vastgesteld worden dat de **kans op effectieve sanctionering** bij overtreding van het gegevensbeschermingsrecht erg laag blijft. Ook het privacy-bewustzijn in de markt ligt laag, alhoewel dit klaarblijkelijk stijgend is. De lage kans op sanctionering en het lage privacy-bewustzijn dragen ongetwijfeld bij aan de hierboven besproken problemen, waardoor gegevensbescherming al te vaak niet, laag of niet effectief op de agenda staat.

Geen verplichting voor ontwikkelaars of verkopers om privacy-by-design toe te passen op AI-systemen

Een essentieel probleem bij de toepassing van gegevensbeschermingsrecht in de technologiesector en dus ook in een AI-context, is dat dit in principe niet van toepassing is op de ontwikkelaars en verkopers van systemen, tenzij en in die mate waarin ze zelf als verwerkingsverantwoordelijke of verwerker optreden. Het zijn immers enkel deze laatsten die de gegevensbeschermingsregels moeten naleven en bv. zorgen dat gegevensbescherming door ontwerp en standaardinstellingen toegepast worden.

Ongetwijfeld zal het vanuit commercieel oogpunt nuttig zijn als ontwikkelaar of aanbieder om systemen aan te bieden die wel voldoen aan de gegevensbeschermingsvereisten, maar feit blijft dat de eindverantwoordelijkheid bij de gebruiker ligt, terwijl deze daar niet altijd vat op heeft. Idealiter zou op Europees niveau de **verplichting om gegevensbescherming door ontwerp en standaardinstellingen opgelegd worden aan alle ontwikkelaars** van AI-systemen ontwikkeld voor of gebruikt binnen de

Europese Unie.

Remmend effect op de ontwikkeling en het gebruik van AI-systemen?

De vergaande verplichtingen die vanuit gegevensbeschermingsrecht van toepassing zijn bij het verwerken van persoonsgegevens in een AI-context, remmen volgens sommige marktspelers de ontwikkeling en de efficiëntie van AI-systemen, waardoor de maatschappij het potentieel daarvan niet ten volle kan benutten.

Het is daarom belangrijk om specifiek voor AI-systemen **voldoende duidelijkheid** te krijgen over hoe zij moeten voldoen aan de gegevensbeschermingsverplichtingen, hoe deze verplichtingen een (ongewenste) remming met zich kunnen meebrengen en hoe zij bv. te verenigen zijn met het 'black box' principe dat van toepassing is bij sommige AI-systemen. Als stap bij het lenigen van deze nood verwijzen wij graag naar onze verkennende gids 'Artificiële intelligentie en gegevensbescherming'.

'Ken je data'

Een vraag die zeker nog ontbreekt in voormelde vragenlijst maar die wel gedekt wordt door het gegevensbeschermingsrecht, is een vraag die ertoe strekt om de verwerker of verwerkingsverantwoordelijke het **belang te doen inzien van de gebruikte (persoons-)gegevens** en de erop van toepassing zijnde eigenschappen en attributen door en door te kennen. Deze kennis is vereist om een goede en aangepaste kwaliteit van de persoonsgegevens te garanderen. Dit vormt op zich de basisvereiste om persoonsgegevens gegevensbeschermingsconform te verwerken.

3.4. Welke tools kunnen worden gebruikt om aan de ethische vereiste te voldoen?

Er zijn een groot aantal tools beschikbaar om te evalueren of AI-projecten en -systemen voldoen aan de gegevensbeschermingsvereisten. Hieronder worden er een aantal opgesomd die publiek beschikbaar zijn en afkomstig zijn van openbare overheden, onderzoeksinstellingen en instellingen met een openbare doelstelling.

- AI Blindspots aan de hand waarvan mogelijke 'AI Blindspots' kunnen worden geïdentificeerd door te reflecteren over de beslissingen en acties die voorafgaand aan de ontwikkeling van een AI-systeem worden genomen.
- LINDDUN en LINDDUN GO zijn privacy-bedreigingsmodellering.
- Online beschikbare gegevensbeschermingseffectbeoordelingen, zoals deze van:

    - CNIL, de Franse toezichthoudende autoriteit: open source PIA software;
    - ICO, de toezichthoudende autoriteit van het Verenigd Koninkrijk: DPIA
- AI System Ethics Self-Assessment Tool laat toe om na te gaan hoe ethisch een AI-toepassing is aan de hand van vier ethische principes: eerlijkheid, verantwoordelijkheid, transparantie, uitlegbaarheid.
- Data Ethics Framework is bedoeld voor overheidsinstellingen te informeren over het correct en verantwoord gebruik van data bij het plannen, evalueren en implementeren van beleid of een dienst.
- Ethical OS tool kit moet helpen om moeilijk te voorspellen en onwelkome consequenties bij het ontwikkelen van producten en projecten, gebaseerd op AI, te voorkomen.
- Data Ethics Canvas geeft handvaten om ethische vragen te behandelen tijdens het ontwerp en de ontwikkeling van een project of product gebaseerd op data, zoals een AI-toepassing.
- De Artificiële Intelligentie Impact Assessment
- De aanpak begeleidingsethiek
- Data Ethics Decision Aid (DEDA)

Hoofdstuk 4: Ethische vereiste 4 - transparantie

4. Ethisch Vereiste 4: Transparantie

4.1. Wat betekent de ethische vereiste?

Een cruciaal onderdeel van het bereiken van een betrouwbare AI is transparantie. Transparantie heeft betrekking op verschillende elementen die relevant zijn voor een AI-systeem waaronder de **gegevens**, het **systeem** en de **bedrijfsmodellen**.

Deze vereiste van transparantie bestaat uit **drie sub-componenten**, namelijk (1) traceerbaarheid, (2) verklaarbaarheid en (3) open communicatie over de beperkingen van het AI-systeem.

Traceerbaarheid impliceert dat de gegevenssets en de processen waaruit de beslissing van het AI-systeem voortkomt, met inbegrip van die van de verzameling en indeling van gegevens alsook de gebruikte algoritmen, zo goed mogelijk moeten worden gedocumenteerd om ze traceerbaar te maken.

Verklaarbaarheid heeft te maken met het vermogen om zowel de technische processen van een AI-systeem als de daaraan gerelateerde menselijke beslissingen (bv. de toepassingsgebieden van een AI-systeem) te verklaren. Voor de technische verklaarbaarheid is het nodig dat de door een AI-systeem genomen beslissingen door mensen kunnen worden begrepen en traceerbaar zijn. Wanneer een beslissing door een AI-systeem significante gevolgen heeft voor het leven van mensen moet het steeds mogelijk zijn om te vragen naar een geschikte verklaring van het besluitvormingsproces van het systeem.

Open communicatie betekent dat AI-systemen zich tegenover gebruikers niet als mensen mogen voordoen. Mensen hebben het recht om te weten dat ze met een AI-systeem te maken hebben. Dat houdt in dat AI-systemen als zodanig herkenbaar moeten zijn. Daarnaast moet de optie worden geboden om menselijke interactie aan te gaan in plaats van interactie met een AI-systeem wanneer dit nodig is om naleving van de grondrechten te waarborgen. Bovendien moeten de capaciteiten en beperkingen van het AI-systeem worden aangegeven, zowel ten aanzien van beroepsbeoefenaars als eindgebruikers. Daarbij wordt dus rekening gehouden met de specifieke situatie.

4.2. Welke regels zijn een uitdrukking van de ethische vereiste of kunnen dienen als inspiratiebron?

De ALTAI lijst voorziet per aangehaald sub-component verschillende vragen. We geven hieronder een overzicht van de vragen per sub-componenten telkens met de relevante wetgeving. De transparantievereisten en informatieverplichtingen spelen een belangrijke rol in **verschillende takken van het recht** zoals gegevensbeschermingsrecht, consumentenrecht, verbintenissenrecht en

productveiligheidsregels.

4.2.A. Traceerbaarheid

Mechanismen moeten worden aangenomen met betrekking tot de traceerbaarheid van het AI-systeem doorheen de hele levensduur.

Werden maatregelen aangenomen die de kwaliteit van de invoergegevens voor het AI-systeem en de output van dergelijke systemen voortdurend te beoordelen?

ALGEMEEN

Er zijn **verschillende mogelijkheden** die er inderdaad voor zorgen dat de kwaliteit van invoergegevens en de output voor AI-systemen voortdurend kunnen worden beoordeeld.

Contractuele afspraken tussen betrokken actoren lijken alvast aangewezen conform de toepasselijke beginselen van het verbintenissenrecht of bijzondere wetgeving. Ook de Wet van 4 april 2019 met betrekking tot misbruiken van economische afhankelijkheid, onrechtmatige bedingen en oneerlijke marktpraktijken tussen ondernemingen is van belang. Deze wet beoogt een betere bescherming van (kleinere) ondernemingen ten aanzien van grotere spelers.

Ook andere maatregelen worden door AI HLEG voorgesteld die op termijn kunnen worden geïmplementeerd zoals bijvoorbeeld **standaard geautomatiseerde kwaliteitsbeoordeling van de gegevensinvoer**. Dit kan door middel van het kwantificeren van ontbrekende waarden of hiaten in de gegevens; het opsporen van wanneer gegevens onvoldoende zijn voor een bepaalde taak; of het nagaan van wanneer de ingevoerde gegevens foutief, onjuist, onnauwkeurig of niet in het juiste formaat zijn.

Wat betreft de **kwaliteit van de outputgegevens** worden eveneens een aantal maatregelen/opties voorgesteld. Deze maatregelen kunnen bv. de vorm aannemen van een **standaard geautomatiseerde kwaliteitsbeoordeling van de AI-output**: de voorspellingsscores zijn bv. binnen het verwachte bereik; anomaliedetectie in de uitvoer en het opnieuw toewijzen van invoergegevens die leiden tot de gedetecteerde anomalie.

GEGEVENSBESCHERMING

De **AVG** bevat een aantal relevante bepalingen. Persoonsgegevens moeten worden verwerkt op een **rechtmatige, behoorlijke en transparante** wijze. Ze moeten ook juist zijn en worden **geactualiseerd** indien nodig (art. 5.1.). De betrokkenen heeft een **recht van inzage** (art. 15) en het recht om van de verwerkingsverantwoordelijke onverwijld **rectificatie** van betreffende onjuiste persoonsgegevens te verkrijgen (art. 16). Er is ook een recht op **beperking van de verwerking** indien bijvoorbeeld de juistheid

van de persoonsgegevens wordt betwist (art. 18). De betrokkene heeft onder de bepaalde voorwaarden ook het recht om vanwege met zijn specifieke situatie verband houdende redenen **bezwaar** te maken tegen de verwerking van hem betreffende persoonsgegevens (art. 21) en **niet te worden onderworpen** aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering (art. 22).

CONSUMENTENBESCHERMING

Richtlijn 1999/44 (omgezet in België door de wet van 1 september 2004 en opgenomen in art. 1649bis-1649octies BW), Richtlijn Digitale Inhoud en de Richtlijn over overeenkomsten voor de verkoop van goederen kunnen mogelijks ook interessant zijn omdat een gebrekkige kwaliteit van invoergegevens eventueel ook kan zorgen voor een gebrek aan **objectieve of subjectieve conformiteit van goederen**, diensten of digital inhoud, waarvoor de verkoper aansprakelijk kan worden gesteld.

Producenten zijn gehouden uitsluitend **veilige producten** op de markt te brengen en **veilige diensten** aan te bieden (art. IX.2. WER). Indien de veiligheid van een product dat AI incorporeert samenhangt met de input of output van gegevens, kan deze bepaling relevant zijn. Sectorale wetgeving legt aan producenten soms ook op dat product/dienst veilig moet zijn wanneer het op de markt komt. Dit kan eventueel samenhangen met de kwaliteit van de invoergegevens ervan. Denk aan **medische hulpmiddelen** en **machines**.

NORMEN

Informatie kan in de toekomst mogelijks ook worden gevonden in **ISO normen** rond AI. Zie ook de bespreking in "Hoofdstuk 2: Ethische vereiste 2 - technische robuustheid en veiligheid".

Kan worden nagaan welke gegevens door het AI-systeem werden gebruikt om een bepaalde beslissing(en) of aanbeveling(en) te nemen?
Kan worden nagaan welk AI-model of welke regels hebben geleid tot de beslissing(en) of aanbeveling(en) van het AI-systeem?

ALGEMEEN

De eerder besproken contractuele afspraken en de Wet van 4 april 2019 zijn relevant.

GEGEVENSBESCHERMING

De AVG speelt ook hier een rol. De verwerkingsverantwoordelijke moet passende maatregelen nemen opdat de betrokkene de **informatie en communicatie** in verband met de verwerking van persoonsgegevens in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt. Deze informatie heeft onder andere betrekking op het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en betreft ten minste in die gevallen,

nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene (art. 12-14). De betrokkene ook **recht van inzage** onder andere met betrekking tot de betrokken categorieën van persoonsgegevens die worden verwerkt (art. 15).

CONSUMENTENBESCHERMING

Binnen het consumentenrecht zijn er ook een aantal bepalingen betreffende informatieplichten ten aanzien van de consument.

Op grond van Richtlijn 2011/83 over consumentenrechten geeft art. VI.45 WER aan **welke informatie op duidelijke en begrijpelijke wijze** aan de consument moet worden verstrekt. Het gaat daarbij onder andere over de **voornaamste kenmerken** van de goederen of diensten, de functionaliteit van digitale inhoud met inbegrip van toepasselijke technische beveiligingsvoorzieningen en de relevante interoperabiliteit ervan met hardware en software waarvan de handelaar op de hoogte is of redelijkerwijs kan worden verondersteld op de hoogte te zijn.

In dit verband kan ook worden verwezen naar bepalingen in de WER (art. VI.93-100) over oneerlijke en misleidende handelspraktijken volgens dewelke informatie die (bijvoorbeeld over de werking van het AI-systeem) verstrekt wordt **correct** moet zijn en **niet misleidend**. Deze regeling is gebaseerd op Richtlijn 2005/29 over oneerlijke handelspraktijken.

Richtlijn 2019/2161 tot modernisering EU consumentenrecht volgens dewelke consumenten duidelijk moeten worden geïnformeerd wanneer de **prijs die zij te zien krijgen gepersonaliseerd** is aan de hand van **geautomatiseerde besluitvorming**. Er is ook een bijkomende transparantieverplichtingen voor onlineplatformen met betrekking tot de weergave van zoekresultaten. De consument moet worden ingelicht over de parameters die gebruikt worden voor de rangschikking van resultaten.

Werden adequate logging procedures ingevoerd om de beslissing(en) of aanbeveling(en) van het AI-systeem vast te leggen?

ALGEMEEN

De eerder besproken contractuele afspraken en de Wet van 4 april 2019 zijn relevant.

GEGEVENSBESCHERMING

Volgens de AVG heeft de betrokkene het **recht om uitsluitsel te verkrijgen** over het al dan niet verwerken van hem betreffende persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens en van de opgesomde informatie (art. 15). De verwerkingsverantwoordelijke moet ook passend **passende technische en organisatorische maatregelen** treffen om te waarborgen en te

kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd (art. 24). Ook moet de verwerkingsverantwoordelijke de passende technische en organisatorische maatregelen nemen om aan de beginselen van gegevensbescherming door ontwerp en door standaardinstellingen te voldoen (art. 25). Elke (vertegenwoordiger van) de verwerkingsverantwoordelijke houdt bovendien ook een **register van de verwerkingsactiviteiten** die onder hun verantwoordelijkheid plaatsvinden (art. 30).

SECTORALE WETGEVING

Ook in **sectorale wetgeving** zijn bepalingen te vinden rond het opstellen, bijhouden en actualiseren van technische documentatie (bv. Verordening Medische Hulpmiddelen of Machinerichtlijn).

AANSPRAKELIJKHEID

Het invoeren van adequate logging procedures zal in de toekomst ook aan belang winnen binnen het aangepast wetgevende kader rond aansprakelijkheid. Een **'log-verplichting'** zou in beginsel op producenten van AI-systemen (kunnen) rusten. Ze zou inhouden dat producenten hun AI-systemen uitrusten met de capaciteit om alle informatie op te slaan die gewoonlijk essentieel is om naderhand uit te maken of een aan de technologie verbonden risico zich heeft gemanifesteerd (logging by design).

4.2.B. Verklaarbaarheid

Het werd reeds gesteld dat verklaarbaarheid betrekking heeft op het vermogen om zowel de technische processen van een AI-systeem als de daaraan gerelateerde menselijke beslissingen te verklaren.

Werden de beslissingen van het AI-systeem aan de gebruikers uitgelegd?

Werd onderzocht of de gebruikers de beslissing(en) van het AI-systeem voortdurend begrijpen?

ALGEMEEN

Dit is afhankelijk van de **manier waarop de uitleg** kan worden gedaan.

Als de ontwikkelaars direct in interactie kunnen gaan met de gebruikers van het AI-systeem, bijvoorbeeld door middel van het organiseren van workshops, kan de deze vraag/vereiste daar worden toegelicht. Als de ontwikkelaars echter niet rechtstreeks betrokken zijn met gebruikers moet de organisatie die bijvoorbeeld AI-systemen verspreid zorgen dat gebruikers het AI-systeem begrijpen en eventuele misverstanden/onduidelijkheden aan ontwikkelaars duidelijk maken.

GEGEVENSBESCHERMING

Onder de AVG moet de verwerkingsverantwoordelijke passende maatregelen nemen opdat de betrokkene de **informatie en communicatie** in verband met de verwerking van persoonsgegevens in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt (art. 12). Daarnaast zijn verwerkingsverantwoordelijken ook verplicht om te informeren omtrent het bestaan en gebruik van geautomatiseerde (individuele) besluitvorming en profilering, om nuttige informatie omtrent de onderliggende logica te geven en om te informeren omtrent het belang en de verwachte gevolgen van deze verwerking voor de betrokkene (artikel 13.2.(f), 14.2.(g), 15.1.(h)).

PRODUCTVEILIGHEID

Producenten moeten binnen het bestek van hun activiteiten de gebruiker de **informatie geven** die hem in staat stelt zich een oordeel te vormen over de aan een product **inherente risico's** gedurende de normale of redelijkerwijs te verwachten gebruiksduur, indien deze risico's zonder passende waarschuwing niet onmiddellijk herkenbaar zijn, en zich tegen deze risico's te beschermen (art. IX.8 WER). Deze bepaling is nuttig voor producten die gebruik maken van AI, zoals autonome motorvoertuigen.

Ook **sectorale wetgeving** kan relevant zijn. Conform art. 5 van de Machinerichtlijn bijvoorbeeld moet de fabrikant alvorens een machine in de handel te brengen en/of in bedrijf te stellen de noodzakelijke informatie verstrekken, zoals de gebruiksaanwijzing.

4.2.C. Communicatie

De mogelijkheden en beperkingen van het AI-systeem moeten aan de gebruikers zijn gecommuniceerd op een wijze die past bij het gebruik. Dit omvat o.a. informatie over de nauwkeurigheid en beperkingen van het AI-systeem.

In het geval van interactieve AI-systemen (bijv. chatbots), werden gebruikers ingelicht dat ze met een AI-systeem werken in plaats van met een mens?

ELEKTRONISCHE HANDEL

Richtlijn 2000/31 stelt standaardregels in de EU vast voor verschillende zaken die verband houden met elektronische handel. Ze bevat ook een aantal **informatieplichten**. Deze moeten op een **duidelijke, begrijpelijke en ondubbelzinnige wijze** worden verstrekt voor het plaatsen van een order. Een onderneming moet voorafgaand aan het aanbieden van deze dienst onder andere de verschillende technische stappen vermelden die nodig zijn om het contact te sluiten (art. XII.7 WER). Het feit dat een AI-systeem wordt ingezet bij de totstandkoming van een contract moet dus worden aangegeven door een onderneming, zodat de consument de eventuele risico's van dergelijke systemen kan inschatten.

Zie voor meer informatie ook "Hoofdstuk 1: Ethische vereiste 1 - menselijke controle en menselijk toezicht".

MODERNISERING CONSUMENTENRECHT

Ook in Richtlijn 2019/2161 tot modernisering EU consumentenrecht zijn een aantal bepalingen openomen die relevant zijn. Consumenten moeten bijvoorbeeld duidelijk worden geïnformeerd wanneer de **prijs** die zij te zien krijgen aan de hand van **geautomatiseerde besluitvorming** is **gepersonaliseerd**, zodat zij in hun aankoopbesluit rekening kunnen houden met de potentiële risico's.

Werden mechanismen ingesteld om gebruikers te informeren over het doel, de criteria en de beperkingen van de door het AI-systeem gegenereerde beslissing(en)?
Werden de voordelen van het AI-systeem aan de gebruikers gecommuniceerd?
Werden de technische beperkingen en potentiële risico's van het AI-systeem gecommuniceerd aan gebruikers, zoals het niveau van de nauwkeurigheid en/of de foutenpercentages?
Werden aan de gebruikers passend trainingsmateriaal en disclaimers ter beschikking gesteld over hoe het AI-systeem adequaat en correct te gebruiken?

CONSUMENTENBESCHERMING

Richtlijn 2011/83 betreffende consumentenrechten voorziet in een verhoging van consumentenbescherming door harmonisatie van belangrijke aspecten van nationale wetgeving betreffende contracten tussen klanten en verkopers. De Richtlijn bevat o.a. informatieplichten. De Richtlijn geeft aan welke **informatie op duidelijke en begrijpelijke wijze** aan de consument moet worden verstrekt. Het gaat daarbij onder andere over de voornaamste kenmerken van de goederen of diensten, de functionaliteit van digitale inhoud met inbegrip van toepasselijke technische beveiligingsvoorzieningen en de relevante interoperabiliteit ervan met hardware en software waarvan de handelaar op de hoogte is of redelijkerwijs kan worden verondersteld op de hoogte te zijn (art. VI. 2, 1° en 8°, art. VI. 45, 1° en 18° en art. VI. 64, 1° en 17° WER). De informatieverplichtingen omtrent de functionaliteit van de digitale inhoud moeten consumenten bovendien ook in staat stellen om de risico's van het gebruik van AI-systemen in aanmerking te nemen.

Ook de **Richtlijn Digitale Inhoud** en **Richtlijn Consumentenkoop** zijn relevant. Informatieplichten kunnen immers in overweging worden genomen bij het bepalen of een digitale dienst of inhoud of een goed met digitale elementen voldoet aan de contractueel toepasselijke subjectieve of objectieve conformiteitsvereisten (bv. functionaliteit, compatibiliteit en interoperabiliteit). Daarnaast moeten goederen en diensten met digitale inhoud ook geleverd worden met (installatie-)instructies. Ten slotte zijn er updateverplichtingen die als doel hebben om de blijvende conformiteit van digitale inhoud of diensten of van goederen met digitale elementen te waarborgen.

Zie voor meer informatie ook "Hoofdstuk 1: Ethische vereiste 1 - menselijke controle en menselijk toezicht".

GEGEVENSBESCHERMING

Volgens de AVG moet elke communicatie met een betrokkene in een **beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm** zijn, en in duidelijke en eenvoudige taal worden opgesteld (art. 12). De doeleinden van de verwerking evenals de wettelijke grondslag en de gerechtvaardigde belangen voor de verwerking moeten duidelijk zijn. Om een behoorlijke en transparante verwerking te waarborgen, kan daarbij ook het bestaan van geautomatiseerde besluitvorming met inbegrip van profilering worden verstrekt. Ook de nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene kunnen door de verwerkingsverantwoordelijke worden verstrekt (art. 13-14).

PRODUCTVEILIGHEID

Producenten moeten binnen het bestek van hun activiteiten de gebruiker de informatie geven die hem in staat stelt om zich een **oordeel te vormen over de aan een product inherente risico's** gedurende de normale of redelijkerwijs te verwachten gebruiksduur, indien deze risico's zonder passende waarschuwing niet onmiddellijk herkenbaar zijn, en zich tegen deze risico's te beschermen (art. IX.8 WER).

SECTORALE WETGEVING

Conform de **Machinerichtlijn** moet de fabrikant alvorens een machine in de handel te brengen en/of in bedrijf te stellen de noodzakelijke informatie verstrekken, zoals gebruiksaanwijzing (art. 5). Conform de **Verordening Medische Hulpmiddelen** zien de fabrikanten erop toe dat zij bij het in de handel brengen of gebruik van hulpmiddelen dat deze overeenkomstig de toepasselijk vereisten zijn ontworpen en vervaardigd. Dit impliceert o.a. het verstrekken van de nodige **informatieplichten** zoals etikettering en gebruiksaanwijzingen (art. 10).

4.3. Waar zitten mogelijke punten van verbetering/ aandachtspunten?

Informatieplichten specifiek voor AI-systemen

Er is al heel wat wetgeving van toepassing op producten die gebruik maken van AI. Toch kan er een **duidelijker kader** worden gecreëerd via soft law of/en aanbevelingen specifiek gericht op informatieplichten voor AI-systemen zelf. Het wetgevende kader moet dus niet worden veranderd, maar kan als basis worden gebruikt om specifieke informatieplichten aan te nemen voor AI-systemen over o.a. (1) oorsprong en verwerking invoerdata, (2) de werking van het AI-systeem, (3) hoe het systeem tot stand is gekomen (4) wat de voordelen en risico's zijn. Daarbij moet worden nagegaan wie de uiteindelijke gebruiker is en de nodige informatie- en transparantieplichten daarop afstemmen. De idee

kan bijvoorbeeld zijn om een soort '**AI bijsluiter**' te ontwerpen die afhankelijk van de eindgebruiker of -afnemer al dat niet uitgebreider kan of moet zijn. Er moet worden nagedacht over hoe een dergelijke bijsluiter eruit moet zien, wat erin moet staan, etc. In het algemeen kan ook worden nagedacht over **legal design** zodat de informatie ook verstaanbaar is voor leken ('de gewone man').

Documentatie voorzien voor (transparante) AI-systemen

Er moet steeds worden gezorgd dat de nodige **documentatie** over de werking, het besluitvormingsproces, … van AI-systemen wordt bewaard. Los van de bestaande regelgeving zou alle informatie gaande van het ontwerp, de ontwikkelingen en het gebruik van AI-systemen op één of andere manier moeten worden bewaard. Een mogelijkheid zou zijn om organisaties verder aan te moedigen om de effecten van AI-systemen op de samenleving in kaart te brengen en te evalueren, net zoals dit het geval is bij een GEB. In een dergelijke **Artificial Intelligence Impact Assessment** kunnen de risico's bij het gebruik van AI-technieken voor de gebruikers en organisaties worden geanalyseerd. Er kan ook worden nagedacht over het invoeren van een **checklist** voor de betrokken organisaties, bedrijven en actoren werkzaam in AI-sector om de transparantie van AI-systemen te verhogen (bv. identificatie van actoren en bepalen hoe zij verantwoordelijk zijn voor transparantie of het verschaffen van uitleg).

Kennisdeling en (multidisciplinaire) samenwerking

Het is van belang om het algemene publiek te **blijven informeren over de realiteit en werking van AI**. Loutere **bewustmaking** over het feit dat AI-systemen niet steeds transparant zijn (cf. black box) kan al helpen. Er moet dus worden gezorgd dat gebruikers (blijven) weten hoe het AI-systeem werkt, welke gegevens worden verwerkt,enz. Door samenwerking binnen het Vlaams AI-plan, samenwerking met Mediawijs en participatie in andere projecten (bv. Iedereen Datawijs) speelt het KDM hier al een rol en het moet dit blijven doen.

Ook bijkomende bewustwording rond transparantie van actoren die betrokken zijn bij het ontwerp en de ontwikkeling van AI-systemen is relevant o.a. door de publicatie van best practices met betrekking tot de gekende vulnerabiliteiten van AI-modellen en technische oplossingen om deze aan te pakken. Er moet ook blijvend worden gezorgd voor een formele **interdisciplinaire samenwerking** zoals reeds wordt gedaan binnen het Vlaamse AI-programma. **Informatie-uitwisseling** is cruciaal. De transparantie bij het ontwerpen van modellen voor machinaal leren kan ook worden bevorderd door de nadruk te blijven leggen op de noodzaak van een explainability-by-design benadering voor AI-systemen met een potentieel negatieve impact op fundamentele rechten van gebruikers.

4.4. Welke tools kunnen worden gebruikt om aan de ethische vereiste te voldoen?

Er zijn een aantal tools die reeds werden ontwikkeld en worden gebruikt door AI-ontwikkelaars om de transparantie van AI-systemen te verhogen:

- Google Explainable AI: is een pakket tools en omkaderingen waarmee begrijpelijke en inclusieve machine learning-modellen kunt worden ontwikkeld.
- Microsoft Interpret ML: is een toolkit om modellen te helpen begrijpen en verantwoord machinaal leren mogelijk te maken
- LIME (Local Interpretable Model-agnostic Explanations): gaat over het uitleggen van wat machine learning classifiers (of modellen) doen.
- ALIBI: is een open source Python-bibliotheek gericht op het machinaal leren van modelinspectie en -interpretatie.
- DeepLIFT: Deep Learning Important FeaTures: is een methode voor het ontbinden van de output voorspelling van een neuraal netwerk op een specifieke input door het back-propageren van de bijdragen van alle neuronen in het netwerk aan elke kenmerk van de ingang.
- What If Tool: is een tool waarmee de prestaties in hypothetische situaties kunnen worden getest, het belang van verschillende gegevensfuncties kunnen worden geanalyseerd en het modelgedrag over meerdere modellen en subsets van invoergegevens kunnen worden gevisualiseerd.
- SHapley Additive exPlanations: is een spel-theoretische benadering om de output van eender welke machinale leermodus te verklaren.
- AI Explainability 360: biedt verschillende algoritmes aan die kunnen worden gebruikt om explainability en fairness onderdeel te laten worden van AI-systemen.
- Artificiële Intelligentie Impact Assessment.
- De aanpak begeleidingsethiek.
- SDoC for AI / AI service FactSheets: stelt dat leveranciers van AI-toepassingen voor elk product een fact sheet moeten creëren, waarmee ze aantonen dat de toepassing 'conform' is. Ze leveren geen template, maar wel een aantal vragen in de appendix als basis.
- People + AI guidebook: omvat principes die zijn bedoeld om user experience (UX) professionals en product managers te helpen met een human-centered aanpak van AI. Deze gids helpt hen om de gebruiker centraal te stellen bij het ontwikkelen van een AI-toepassing.
- AI systems Ethics Self-Assessment Tool: is een vragenlijst die helpt bij het zelf inschatten van vier ethische principes: eerlijkheid, verantwoordelijkheid, transparantie, uitlegbaarheid.
- De Principles for Accountable Algorithms en Social Impact Statement for Algorithms: bestaat uit een aantal vragen die helpen om verschillende ethische principes te waarborgen. De tool bevat ook stappen die kunnen worden gevolgd om deze principes verder te onderzoeken in de verschillende ontwikkelingsfasen van je AI-project.

- TreeInterpreterRandom-Forest-Explainability-Pipeline
- Activation Atlases
- Rulex Explainable AI

Hoofdstuk 5: Ethische vereiste 5 - diversiteit, non-discriminatie en rechtvaardigheid

5. Ethisch Vereiste 5: Diversiteit, non-discriminatie en rechtvaardigheid

5.1. Wat betekent de ethische vereiste?

Om betrouwbare AI te verwezenlijken moeten inclusie en diversiteit mogelijk worden gemaakt gedurende de hele levenscyclus van het AI-systeem. Er moet daarbij gedurende het hele proces met alle betrokken belanghebbenden rekening worden gehouden. Er moet ook worden gezorgd voor gelijke toegang via inclusieve ontwerpprocessen, alsook voor gelijke behandeling. Deze vereiste is nauw verbonden met het beginsel van rechtvaardigheid.

Deze vereiste houdt rekening met **drie sub-componenten**: (1) voorkomen van onrechtvaardige vertekeningen, (2) verzekeren van toegankelijkheid en universeel ontwerp en (3) zorgen voor participatie van belanghebbenden.

Ten eerste wil deze vereiste **onrechtvaardige vertekening (bias) voorkomen**.

De gegevenssets die in AI-systemen gebruikt worden kunnen onvolledig zijn, onbedoelde historische vertekeningen of slechte governance-modellen bevatten. Hierdoor kunnen er onbedoelde (in)directe vooroordelen en discriminatie tegen bepaalde groepen of mensen ontstaan. Dit kan vooroordelen en marginalisering mogelijks versterken. Aanwijsbare en discriminerende vertekening moet in de verzamelingsfase waar mogelijk worden verwijderd. Er kan ook sprake zijn van vertekening in de manier waarop AI-systemen worden ontwikkeld (bijv. het programmeren van algoritmen). Deze vertekening kan worden tegengegaan door toezichtsprocessen in te stellen om het doel, de beperkingen, de vereisten en de beslissingen van het systeem op een heldere en transparante manier te analyseren en te behandelen.

Ten tweede houdt het verband met **toegankelijkheid en universeel ontwerp**.

Met name in B2C-domeinen (Business to Consumer) moeten systemen gericht zijn op de gebruiker en op zo'n manier ontworpen zijn dat alle mensen gebruik kunnen maken van AI-systemen of diensten, ongeacht hun leeftijd, geslacht, mogelijkheden of karakteristieken. In het bijzonder is het belangrijk dat deze technologie toegankelijk is voor mensen met een beperking. AI-systemen zouden geen gebruik mogen maken van een one size fits all benadering, maar moeten principes van universeel ontwerp in overweging nemen, gericht op het breedst mogelijke scala aan gebruikers, hierbij rekening houdend met de relevante toegankelijkheidsstandaarden.

Ten derde staat **participatie van belanghebbenden** centraal.

Om betrouwbare AI-systemen te ontwikkelen is het aangeraden om de belanghebbenden te raadplegen die gedurende de levenscyclus van het project, er direct of indirect mee te maken zullen hebben. Het is nuttig om, ook na de implementatie, regelmatig feedback te vragen en initiatieven op lange termijn op te stellen voor de participatie van belanghebbenden, bijvoorbeeld door te verzekeren dat werknemers geïnformeerd en geconsulteerd worden en ook kunnen participeren gedurende het volledige toepassingsproces van AI in een organisatie.

5.2. Welke regels zijn een uitdrukking van de ethische vereiste of kunnen dienen als inspiratiebron?

De ALTAI lijst voorziet per aangehaald sub-component verschillende vragen. We geven hieronder een overzicht van de (gebundelde) vragen per sub-component en de mogelijk relevante wetgeving die reeds een uitdrukking vormen van deze vragen of kunnen worden gebruikt als inspiratie.

5.2.A. Voorkomen van onrechtvaardige vertekening (bias)

Is er een strategie of procedure opgesteld om de creatie of versterking van oneerlijke bias te vermijden, zowel betreffende het gebruik van inputdata als voor het ontwerp van het algoritme?

Werd rekening gehouden met diversiteit en representativiteit van eindgebruikers en/of onderwerpen in de data?

ALGEMEEN

Er zijn reeds verschillende voorbeelden van AI-systemen die discrimineren. Denk aan robot TAY die binnen de kortste keren racistisch werd, Google Photos dat zwarte vrienden per ongeluk kwalificeerde als apen of het algoritme van Amazon dat vrouwen discrimineerde tijdens een sollicitatie. Er zijn (vooralsnog) geen specifieke bepalingen rond discriminatie door AI-systemen. Toch is er al heel wat relevante anti-discriminatie wetgeving die mogelijks relevant is in een AI-context, zeker omdat het vaak mensen zijn of vooroordelen die aan de basis liggen van bias in AI-systemen.

De toepasselijke en relevante wetgeving rond **anti-discriminatie is vrij uitgebreid** en terug te vinden op Europees, nationaal en regionaal niveau. Deze wetgeving kan zowel algemeen als specifiek zijn en dient als inspiratiebron voor specifieke wetgeving om **algoritmische discriminatie** tegen te gaan.

ALGEMENE BEPALINGEN ROND ANTI-DISCRIMINATIE: EUROPEES VERDRAG RECHTEN VAN DE MENS

Er is heel wat Europese regelgeving rond discriminatie in het algemeen. Het **Europees Verdrag voor de Rechten van de Mens** (EVRM) is een verdrag dat afdwingbaar is en waarin de mensen- en burgerrechten voor alle inwoners van de lidstaten van de Raad van Europa zijn geregeld.

Art. 14 voorziet in een verbod van discriminatie. Het genot van de rechten en vrijheden in het EVRM moet worden verzekerd zonder enig onderscheid op welke grond ook, zoals geslacht, ras, kleur, taal, godsdienst, politieke of andere mening, nationale of maatschappelijke afkomst, het behoren tot een nationale minderheid, vermogen, geboorte of andere status.

Rechtspraak van het Europese Hof voor de Rechten van de mensen toont dat zowel directe als indirecte discriminatie verboden is.

Bij directe discriminatie wordt iemand expliciet ongelijk behandeld op basis van een beschermde grond, bijvoorbeeld nationaliteit of geslacht. In het geval van indirecte discriminatie gaat het om een praktijk die op het eerste zicht neutraal lijkt, maar die in realiteit leidt tot discriminatie van personen op basis van een beschermde grond zoals etniciteit. In dit laatste geval is het niet relevant of er de intentie was om te discrimineren, het zijn de gevolgen van de praktijk die gelden.

ALGEMENE BEPALINGEN ROND ANTI-DISCRIMINATIE: EUROPESE UNIE

De verwijzing naar non-discriminatie is terug te vinden in de basisverdragen van de EU:

- Art. 20-26 Handvest van de grondrechten van de Europese Unie: gelijkheid voor de wet, non-discriminatie, verscheidenheid van cultuur, godsdienst en taal, de gelijkheid van mannen en vrouwen, de rechten van het kind, de rechten van ouderen en de integratie van personen met een handicap;
- Art. 10 Verdrag betreffende de werking van de Europese Unie: bestrijding van iedere discriminatie op grond van geslacht, ras of etnische afkomst, godsdienst of overtuiging, handicap, leeftijd of seksuele gerichtheid;
- Art. 2, 3(3) en 9 van het Verdrag betreffende de Europese Unie: nadruk op gelijkheid, non-discriminatie, rechtvaardigheid, pluralisme, de rechtsstaat en eerbiediging van mensenrechten waaronder de rechten van personen die tot minderheden behoren.

De EU heeft 4 algemene richtlijnen rond discriminatie uitgevaardigd:

- Richtlijn 2000/43 van 29 juni 2000 voorziet in een gelijke behandeling van personen ongeacht ras of etnische afstamming;
- Richtlijn 2000/78 van 27 november 2000 voorziet in een algemeen kader voor gelijke behandeling in arbeid en beroep. De criteria zijn godsdienst of overtuiging, handicap, leeftijd, seksuele geaardheid;
- Richtlijn 2004/113 van 13 december 2004 en Richtlijn 2006/54 van 5 juli 2006 (herschikking) voorziet in gelijke kansen en gelijke behandeling van mannen en vrouwen in arbeid en beroep. De criteria zijn geslacht inclusief zwangerschap en moederschap.

Ook op het niveau van de EU is zowel directe als indirecte discriminatie verboden. Daarnaast heeft de EU een aantal **specifieke richtlijnen** uitgevaardigd:

- Richtlijn 79/7 van 19 december 1978 betreffende de geleidelijke tenuitvoerlegging van het beginsel van gelijke behandeling van mannen en vrouwen op het gebied van de sociale zekerheid. De richtlijn

is van toepassing op de beroepsbevolking;

- Richtlijn 2010/41 van 7 juli 2010 betreffende de toepassing van het beginsel van gelijke behandeling van zelfstandig werkzame mannen en vrouwen;
- Richtlijn 2010/18 van 8 maart 2010 inzake een raamovereenkomst over ouderschapsverlof.

Bovendien moet er rekening gehouden met de **regelgeving rond de verwerking van persoonsgegevens**, waarin gewaarschuwd wordt voor mogelijke discriminerende gevolgen zoals:

- De AVG;
- Richtlijn 2016/680 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
- Richtlijn (2016/681 van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit.

ALGEMENE BEPALINGEN ROND ANTI-DISCRIMINATIE: BELGISCHE WETGEVING

Die 4 Europese Richtlijnen werden op federaal niveau omgezet in de onderstaande **3 wetten van 10 mei 2007**. Zij vormen de juridische basis voor de bestrijding van discriminatie.

- Wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden gewijzigd door de wet van 10 mei 2007. Deze wet verbiedt discriminatie op basis van nationaliteit, zogenaamd 'ras', huidskleur, afkomst of nationale of etnische afstamming;
- Wet van 10 mei 2007 ter bestrijding van bepaalde vormen van discriminatie. Deze wet verbiedt discriminatie op grond van geloof of levensbeschouwing, handicap, leeftijd, seksuele geaardheid, burgerlijke staat, vermogen, politieke overtuiging, syndicale overtuiging, taal, huidige of toekomstige gezondheidstoestand, fysieke of genetische eigenschap, sociale afkomst;
- Wet van 10 mei 2007 ter bestrijding van discriminatie tussen vrouwen en mannen. Deze wet verbiedt elke vorm van discriminatie op basis van geslacht. Discriminatie op basis van geslachtsverandering, genderidentiteit en genderexpressie wordt hieraan gelijkgesteld.

ALGEMENE BEPALINGEN ROND ANTI-DISCRIMINATIE: VLAAMSE WETGEVING

In Vlaanderen is het antidiscriminatiebeleid vastgelegd in een aantal decreten:

- Decreet van 8 mei 2002 houdende evenredige participatie op de arbeidsmarkt. Dit decreet beschrijft dat alle groepen uit de bevolking evenveel recht hebben om aan de arbeidsmarkt deel te nemen, ongeacht de specifieke eigenschappen van bepaalde bevolkingsgroepen;
- Decreet van 10 juli 2008 houdende een kader voor het Vlaamse gelijkekansen- en gelijkebehandelingsbeleid. Dit decreet is de omzetting van de 4 eerder aangehaald Europese Richtlijnen;
- Decreet private arbeidsbemiddeling van 10 december 2010. Dit decreet bevat een beperkt aantal

bepalingen over discriminatie (o.a. de wetgeving voor uitzendkantoren).

SPECIFIEKE BEPALINGEN ROND ANTI-DISCRIMINATIE

Naast de algemene bepalingen zijn er ook een aantal **specifieke bepalingen** rond discriminatie. Deze zijn onder andere opgenomen in art. III.2 WER over de **vrijheid van vestiging**. Het vergunningstelsel mag geen discriminerende werking hebben ten aanzien van de betrokken dienstverrichter. Voorbeelden zijn een betere behandeling van de Belgische dienstverlener, het opleggen van bijkomende voorwaarden aan de buitenlandse dienstenverlener. Ook ten aanzien van afnemers van diensten wordt bepaald dat ze niet onderworpen mogen worden aan discriminerende vereisten op grond van nationaliteit of woonplaats (art. III.80-81 WER). Voorbeelden zijn de ontvangst van televisiediensten afkomstig van een andere lidstaat, overeenkomsten inzake mobiele telefonie, aanbod van goederen en diensten op het internet.

Een andere bepaling houdt verband met de **toegang tot betaalrekeningen en basisbankdienst**. De consument mag op geen enkele manier worden gediscrimineerd op grond van zijn nationaliteit of verblijfplaats, of op grond van een zogenaamd ras, huidskleur, afkomst of nationale of etnische afstamming (art. VII.56/1 WER). Deze verplichting van non-discriminatie geldt wanneer de consument de opening van een betaalrekening aanvraagt, er toegang toe krijgt of een dergelijke rekening aanhoudt, of wanneer hij wenst gebruik te maken van de basisbankdienst. Voor wat betreft de basisbankdiensten mag er "in generlei opzicht" andere discriminatie zijn, zoals bijvoorbeeld de financiële situatie van de consument (art. VII.57 §2 WER).

Er zijn ook anti-discriminatie bepalingen in voege over het **sluiten van een kredietovereenkomst**. Een kredietgever is gehouden tot het raadplegen van de Centrale om de kredietwaardigheid van de persoonlijke zekerheidsstellers of consumenten te beoordelen. De voorwaarden inzake toegang tot de Centrale of elke ander bestand dat aangewend wordt om de kredietwaardigheid van de consument of een persoonlijke zekerheidssteller te beoordelen, of om na te gaan of deze kredietwaardigheid wordt gehandhaafd, mogen niet discriminerend zijn (art. VII.77.1 § 1 WER).
Op het gebied van **verzekeringen** gelden de algemene wetten. Verzekeringsmaatschappijen maken gebruik van segementering. Dit is een techniek die de verzekeraar aanwendt om de premie en eventueel ook de dekking te differentiëren in functie van een aantal specifieke karakteristieken van het te verzekeren risico, met de bedoeling tot een betere overeenstemming te komen tussen de verwachtingswaarde van de schade en de kosten die een bepaalde persoon ten laste legt van de collectiviteit van de verzekeringnemers en de premie die hij voor de geboden dekking moet betalen. De wet betreffende de verzekeringen stelt wel dat elke segmentatie op het vlak van acceptatie, tarifering en/of de omvang van de dekking objectief moet worden gerechtvaardigd door een legitiem doel en de middelen voor het bereiken van dat doel moeten passend en noodzakelijk zijn (art. 44).

Werd gezorgd voor een mechanisme dat het mogelijk maakt om problemen met bias, discriminatie of de slechte prestaties van het AI-systeem aan te geven?

GEGEVENSBESCHERMING

Onder de AVG moet elke organisatie die persoonsgegevens verwerk nagaan of daar risico's aan verbonden zijn. Indien een organisatie vermoedt dat een AI-systeem naar alle waarschijnlijkheid een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet zij een GEB uitvoeren (art. 35).

Bovendien kunnen betrokkenen zelf actie ondernemen door een beroep te doen op hun recht op inzage en hun recht op rectificatie. Betrokkenen kunnen te weten komen welke informatie een organisatie over hun in bezit heeft (art. 15). Dit stelt hen in staat om te controleren of deze informatie juist en volledig is. Is dit niet het geval, dan kunnen ze om een rectificatie van hun persoonsgegevens verzoeken (art. 16).

PRODUCTVEILIGHEID

Ook voor producten of diensten die gebruik van maken van AI (embedded software) zijn er reeds een aantal relevante bepalingen voorhanden. Dit kwam bij vorige vereisten al uitvoerig aan bod.

In navolging van art. 5, lid 1 van de Richtlijn Productveiligheid bepaalt art. IX.8 §2 WER dat de producenten van producten en diensten binnen het bestek van hun activiteiten maatregelen moeten nemen die zijn afgestemd op de kenmerken dan de door hen geleverde producten en diensten om 1) op de **hoogte te blijven van de risico's** van deze producten en diensten en 2) de **passende acties te ondernemen** om de risico's van deze producten te voorkomen. Dit omvat het uit de handel nemen, het aangepast en doeltreffend waarschuwen van de gebruikers en het terugroepen. Art. IX.8 §3 WER voorziet voor de distributeurs dat zij bijdragen tot de naleving van de veiligheidseisen o.a. binnen het bestek van hun activiteiten deelnemen aan de bewaking van de veiligheid van de op de markt gebrachte producten.

Krachtens art. IX.8 §4 WER stellen de producenten en distributeurs het **Centraal Meldpunt voor Producten** onmiddellijk in kennis wanneer zij weten, of op grond van de hun ter beschikking staande gegevens beroepshalve behoren te weten, dat een product of dienst voor de gebruiker risico's met zich meebrengt die onverenigbaar zin met de algemene veiligheidsverplichting. Deze verplichting geldt ook voor de producenten en distributeurs van producten die aan specifieke veiligheidswetgeving onderworpen zijn. Soms worden ook specifieke verplichtingen opgelegd door Europese regelgeving (bv. art. 11 van de Bouwproductenverordening).

Zowel producenten als distributeurs hebben de verplichting om tijdens de levensduur van producten deel te nemen aan de **constante bewaking van de productveiligheid** en gebruikers de informatie ter beschikking stellen die hem in staat stelt zich een oordeel te vormen over de aan een product inherente

risico's gedurende (art. IX.8 van het WER).

Zowel voor als het op de markt brengen van een product of dienst is de producent verplicht om alle mogelijke **bedreigingen te testen die het product kunnen treffen** teneinde te kunnen voldoen aan de algemene veiligheidsverplichting, de bewakingsplicht en andere verplichtingen zoals vermeld in specifieke regelgeving. Deze verplichtingen werden hierboven reeds besproken.

Artikel 8 van de **Wet Productaansprakelijkheid** bepaalt dat de producent aansprakelijk is voor de schade die veroorzaakt wordt door veilige producten, tenzij hij o.a. bewijst dat het op grond van de stand van de wetenschappelijke en technische kennis op het tijdstip waarop hij het product in het verkeer bracht onmogelijk was het bestaan van het gebrek te ontdekken. Een producent van producten heeft er dus alle baat bij om de risico's en bedreigingen op voorhand te identificeren.

De risico-gebaseerde aanpak van de veiligheidsverplichting impliceert dat voor bepaalde producten strengere regels gelden dan voor andere. Voor bepaalde **categorieën van producten** (bv. voor medische hulpmiddelen of bepaalde machines) kunnen strengere conformiteitsbeoordelings-procedures worden opgelegd dan andere. Dit houdt op zich reeds in dat er een onderscheid wordt gemaakt in de risico's van verschillende producten.

Een risico-inschatting moet ook altijd worden gemaakt bij het nemen van **corrigerende maatregelen** door producenten. In de praktijk wordt bij het plannen van een corrigerende maatregel altijd een risicobeoordeling gemaakt. Dit wordt verduidelijkt doordat uitdrukkelijk wordt bepaald dat 'passende' acties moeten worden genomen om de risico's van de producten te voorkomen. In de praktijk zal men eerst een risicobeoordeling uitvoeren, zowel wanneer het product op de markt wordt gebracht als bij een corrigerende maatregel. Deze hangt af van de corrigerende actie. De basisprincipes van deze risicobeoordeling werden reeds uitgelegd in de Gids voor corrigerende acties van de Europese Commissie.

Werden mechanismen voorzien om de rechtvaardigheid van een AI-systeem te waarborgen?

ALGEMEEN

De ontwikkeling, de installatie en het gebruik van AI-systemen moeten rechtvaardig zijn. De AI HLEG erkent dat er veel verschillende interpretaties van rechtvaardigheid bestaan. De groep stelt evenwel dat rechtvaardigheid zowel een **inhoudelijke als een procedurele dimensie** heeft.

INHOUDELIJK

Dit impliceert een toezegging om de **gelijke en rechtvaardige verdeling** van zowel voordelen als kosten

te waarborgen en ervoor te zorgen dat personen en groepen vrij zijn van onrechtvaardige vertekening, discriminatie en stigmatisering. Indien onrechtvaardige vertekening kan worden voorkomen, zouden AI-systemen zelfs de maatschappelijke rechtvaardigheid kunnen vergroten. **Gelijke kansen** wat betreft toegang tot onderwijs, goederen, diensten en technologie moeten ook worden bevorderd. Daarnaast mag het gebruik van AI-systemen nooit tot gevolg hebben dat de (eind)gebruikers worden misleid of worden beperkt in hun keuzevrijheid. Verder impliceert rechtvaardigheid dat beroepsbeoefenaars op het gebied van AI het **beginsel van evenredigheid** tussen middelen en doelen moeten eerbiedigen en zorgvuldig moeten afwegen hoe ze tegengestelde belangen en doelstellingen in evenwicht kunnen brengen.

PROCEDUREEL

Dit omvat het vermogen om beslissingen die worden genomen door AI-systemen en door de mensen die deze systemen beheren, **aan te vechten** en er **effectief beroep** tegen in te stellen. Om dat te kunnen doen moet de entiteit die verantwoordelijk is voor de beslissing, identificeerbaar zijn en moet het besluitvormingsproces verklaarbaar zijn.

GEGEVENSBESCHERMING

Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene **rechtmatig, behoorlijk en transparant** is (art. 5 AVG).

Werden opleidings- en bewustwordingsinitiatieven opgezet om AI-ontwerpers en ontwikkelaars bewust te maken van de mogelijke bias die ze kunnen inbrengen in het ontwerp en de ontwikkeling van het AI-systeem?

Hoewel er in wetgeving niet meteen iets te vinden is, zijn er een aantal **voorbeelden en gebruiken** die ontwerpers en ontwikkelaars hierover willen bewust maken zoals de Machine Learning Crash Course, Google's Responsible AI Practices en enkele informatieve blogs. Ook in verschillende AI-opleidingen komen ethische aspecten reeds uitvoerig aan bod.

5.2.B. Toegankelijkheid en universeel ontwerp

Werd ervoor gezorgd dat het AI-systeem overeenkomt met de diversiteit aan voorkeuren en vaardigheden in de samenleving?

Het VN **Verdrag inzake de Rechten van Personen met een Handicap** bevat een bepaling over toegankelijkheid. Teneinde personen met een handicap in staat te stellen zelfstandig te leven en volledig deel te nemen aan alle facetten van het leven, moeten overheden passende maatregelen nemen om personen met een handicap op voet van gelijkheid met anderen de toegang te garanderen tot de fysieke omgeving, tot vervoer, informatie en communicatie, met inbegrip van informatie-en

communicatietechnologieën en -systemen, en tot andere voorzieningen en diensten die openstaan voor, of verleend worden aan het publiek, in zowel stedelijke als landelijke gebieden (art. 9). Verder verschenen een aantal interessante documenten rond datakwaliteit en/of representativiteit in een AI-context.

Werd nagegaan of de user interface van het AI-systeem gebruikt kan worden door personen met speciale noden of beperkingen of personen die het risico lopen te worden uitgesloten?

VERDRAGSRECHTELIJKE BEPALINGEN

Het VN **Verdrag inzake de Rechten van Personen met een Handicap** bevat opnieuw een relevante bepaling. Overheden nemen eveneens passende maatregelen om de toegang voor personen met een handicap tot nieuwe informatie en communicatietechnologieën en -systemen, met inbegrip van het internet, te bevorderen. Ook moeten maatregelen worden genomen om het ontwerp, de ontwikkeling, productie en distributie van toegankelijke informatie-en communicatietechnologieën, en communicatiesystemen in een vroeg stadium te bevorderen, opdat deze technologieën en systemen tegen minimale kosten toegankelijk worden (art. 9).

OVERHEIDSOPDRACHTEN

Richtlijn 2014/24 betreffende het **plaatsen van overheidsopdrachten** bepaalt dat voor alle aanbestedingen die zijn bedoeld voor gebruik door natuurlijke personen, hetzij door het grote publiek, hetzij door het personeel van de aanbestedende dienst, technische specificaties, uitgezonderd in behoorlijk gemotiveerde gevallen, zodanig moeten worden opgesteld dat rekening wordt gehouden met de criteria inzake toegankelijkheid voor personen met een handicap of de geschiktheid van het ontwerp voor alle gebruikers. In deze technische specificaties worden de voor een werk, dienst of levering gestelde kenmerken voorgeschreven (art. 42).

Ook in de Wet inzake overheidsopdrachten van 17 juni 2016 staan een aantal relevante **bepalingen rond technische specificaties**. In geval van overheidsopdrachten voor werken wordt een technische specificatie gedefinieerd als alle technische voorschriften opgenomen in de opdrachtdocumenten die een omschrijving geven van de vereiste kenmerken van een materiaal, een product of een levering, zodat dit of deze beantwoordt aan het gebruik waarvoor het materiaal, product of de levering door de aanbesteder is bestemd. Een ontwerp dat aan alle vereisten voldoet met inbegrip van de toegankelijkheid voor gehandicapten en gebruiksgeschiktheid behoren daartoe. Dit geldt ook voor overheidsopdrachten voor levering of voor diensten (art. 2, 44°).

TOEGANKELIJKHEID VAN DE WEBSITES EN MOBIELE APPLICATIES VAN OVERHEIDSINSTANTIES

Op federaal niveau werd Richtlijn 2016/2102 omgezet in de wet van 19 Juli 2018 inzake toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties. Overheidsinstanties nemen de

noodzakelijke maatregelen om hun websites en mobiele applicaties toegankelijker te maken, overeenkomstig de bepalingen van deze wet, door ze waarneembaar, bedienbaar, begrijpelijk en robuust te maken. Op Vlaams niveau werd deze richtlijn opgenomen in het Vlaams Bestuursdecreet (Afdeling 4. Toegankelijkheid van websites en mobiele applicaties).

Richtlijn 2019/882 betreffende de toegankelijkheidsvoorschriften voor producten en diensten zal in de toekomst ook relevant zijn. De Richtlijn bevat toegankelijkheidsvoorschriften voor belangrijke producten en diensten zoals: telefoons, computers; bankdiensten voor consumenten; elektronische communicatiediensten met inbegrip van bijvoorbeeld telefoon- en internetdiensten; toegang tot audiovisuele mediadiensten en elektronische handel.

De Richtlijn bevat eveneens gemeenschappelijke toegankelijkheidsvoorschriften inzake het ontwerp van de gebruikersinterface en van de functionaliteit van producten, en meer specifieke toegankelijkheids-voorschriften voor bepaalde elektronische apparatuur voor gebruik door consumenten. Voor consumentenproducten die onder de richtlijn vallen, moeten de verpakking, de montage-instructies en andere productinformatie toegankelijk zijn. De richtlijn moet uiterlijk omgezet zijn op 28 juni 2022.

Werd ervoor gezorgd dat er rekening gehouden werd met de beginselen van universeel ontwerp en toegang in elke stap van het proces?

ALGEMEEN

Het W3C Web Accessibility Initiative (WAI) ontwikkelt standaarden en ondersteuningsmateriaal om **organisaties te helpen de toegankelijkheid te begrijpen en te implementeren**. Er wordt daarbij een onderscheid gemaakt tussen de begrippen toegankelijkheid, bruikbaarheid en inclusie. Ook de Europese Richtlijn betreffende de toegankelijkheidsvoorschriften voor producten en diensten is van belang in dit opzicht.

STANDAARDEN

Er zijn een aantal **standaarden**.

- CEN/CLC/JTC 12 - Design for All
- European Committee for Standardization - Design for All bepaalt de eisen die een organisatie in staat moeten stellen om producten, goederen en diensten te ontwerpen, te ontwikkelen en te leveren, zodat ze toegankelijk zijn voor, begrepen worden door en gebruikt worden door een zo groot mogelijk aantal gebruikers, waaronder personen met een handicap.
- ISO/IEC 40500:2012 bevat een breed scala aan aanbevelingen voor het toegankelijker maken van web content. Het volgen van deze richtlijnen zal de inhoud toegankelijk maken voor een breder scala aan mensen met een handicap.
- ISO/IEC TR 29138-1:2018 definieert toegankelijkheidsoverwegingen voor mensen met een handicap,

onafhankelijk van een bepaalde technologie, hardware of software.

- ISO/IEC 30071-1:2019 stelt eisen aan het ontwikkelingsproces in plaats van aan de daaruit voortvloeiende producten en diensten.
- W3C Web Content Accessibility Guidelines (WCAG) 2.0 geeft aanbevelingen voor het toegankelijk maken van web-content in het algemeen, en specifiek voor personen met een beperking.
- Authoring Tool Accessibility Guidelines (ATAG) voorzien richtlijnen voor het ontwerp van web-inhoud authoring tools die toegankelijk zijn voor personen met een handicap en om actoren te helpen meer toegankelijke web-inhoud te creëren.
- User Agent Accessibility Guidelines (UAAG) leggen uit hoe gebruikersagenten toegankelijk kunnen worden gemaakt voor mensen met een handicap.
- ETSI EN 301 549 is geschikt voor overheidsopdrachten voor ICT-producten en -diensten in Europa.
- Principles of Universal Design behelzen het ontwerp van producten en omgevingen om door iedereen te kunnen worden gebruikt mensen, voor zover mogelijk, zonder aanpassing of gespecialiseerd ontwerp.

5.3. Waar zitten mogelijke punten van verbetering of aandachtspunten?

Participatie van belanghebbenden

Participatie van belanghebbenden wordt benadrukt, maar de AI HLEG geeft geen voorbeelden van dergelijke mogelijkheden en werkt het concept ook niet verder uit. **Participatie** is een waarde die vaak geïdentificeerd wordt, maar zelden verder wordt geoperationaliseerd. Het zou helpen indien er concrete aanbevelingen gedaan zouden worden omtrent hoe belanghebbenden te engageren. Er moet ook werk gemaakt worden van de ontwikkeling van digitale skills van de bevolking zodat iedereen AI kan begrijpen, al is het maar op een basisniveau.

Er kan alvast inspiratie gevonden worden in de traditie van het **participatory design** waar gebruikers en belanghebbenden doorheen het volledige ontwikkelingstraject van een bepaalde oplossing/ beleid/ product/dienst worden betrokken. Er kan worden onderzocht hoe die traditie zich kan vertalen naar AI-projecten. Digitale inclusie kan voor bepaalde toepassingen een extra aandachtspunt zijn.

Discriminatie

Indirecte discriminatie kan verborgen blijven voor zowel de organisatie als het slachtoffer. Zelflerende algoritmes zijn vaak 'zwarte dozen'. Zo hebben de meeste mensen een gebrek aan expertise om te

begrijpen hoe zulke systemen tot bepaalde beslissingen komen. Zelfs de experten die het systeem opgesteld hebben weten niet altijd hoe het systeem zich in de realiteit zal gedragen. Wegens het gebrek aan transparantie in beslissingen van zelflerende algoritmes, is het moeilijk voor personen om na te gaan of zij gediscrimineerd worden.

De wetgeving rond discriminatie beschermt personen tegen discriminatie op basis van bepaalde beschermde kenmerken zoals geslacht en etniciteit. Maar algoritmen kunnen nieuwe categorieën van personen genereren op basis van schijnbaar onschuldige kenmerken, bijvoorbeeld de keuze van webbrowser of postcode, en dus ook resulteren in discriminatie. **Algoritmische besluitvorming** kan sociale ongelijkheid versterken. Zo heeft algoritmische prijsbepaling er in een aantal gevallen toe geleid dat arme mensen hogere prijzen aangerekend kregen. Beleidsmatig kan/moet hier meer aandacht aan worden gegeven en kan hierover bijkomende informatie worden verzameld en verspreid. Er kan bijvoorbeeld worden nagegaan of het consumentenrecht in staat is een antwoord te bieden op algoritmische discriminatie en of er eventueel aanpassingen nodig zijn.

Opleidings- en bewustwordingsinitiatieven kunnen (blijvend) worden opgezet voor ontwikkelaars van AI-systemen. Hierbij moet niet alleen aandacht gaan naar de typische gronden voor discriminatie (bv. etniciteit, geslacht), maar ook naar mogelijk nieuwe vormen van discriminatie (bv. browsergedrag) en naar de mogelijkheid dat op het eerste zicht 'onschuldige' gegevens (bv. postcode, diploma) toch kunnen leiden tot een vorm van discriminatie. Instrumenten zoals een GEB of een AIIA zijn belangrijk om mogelijke risico's vanaf de beginfase van een AI-systeem in te schatten. De AIIA en de GEB maken beide gebruik van een risicobenadering en hanteren gedeeltelijk dezelfde logica. Beide instrumenten zijn complementair, maar niet onderling inwisselbaar. Een GEB is enkel gericht op de risico's die verwerking van persoonsgegevens met zich mee kan brengen voor de betrokkene. De AIIA is een breder instrument dat zich richt op alle mogelijke ethische en juridische vraagstukken die geassocieerd kunnen worden met de toepassing van AI. Bovendien kijkt de AIIA niet alleen naar risico's, maar biedt het ook een kader voor het maken van ethische keuzes voor de inzet van AI.

Beleidsmakers kunnen nagaan of en in welke mate een dergelijke beoordeling aangewezen zou zijn voor organisaties. Zij kunnen tevens nagaan of er **adequate mechanismen voorhanden zijn die problemen met bias, discriminatie of de slechte prestaties van het AI-systeem aangeven**. Indien dit niet het geval zou zijn kan er onderzocht worden of de ontwikkeling van een dergelijk mechanisme mogelijk is en op welke manier. Te denken valt bijvoorbeeld aan een meldpunt voor problemen in verband met AI-systemen.

Inclusie

De AI HLEG benadrukt de noden van personen met een speciale nood of handicap of degenen die het risico

lopen te worden uitgesloten. Bovendien stelt ze ook vragen rond de vertegenwoordiging van verschillende groepen uit de samenleving en de mogelijke gevolgen van een dergelijke vertegenwoordiging voor de toegankelijkheid en de inclusiviteit.

Er worden echter geen vragen gesteld over mogelijke problemen rond toegang die kunnen voortvloeien uit financiële criteria of technologische ongeletterdheid, die evenzeer tot uitsluiting kunnen leiden. **Digitale geletterdheid** wordt belangrijker voor het algemene publiek. Vaak wordt de nadruk gelegd op technische vaardigheden en inzichten. Kinderen komen impliciet aan bod, maar het is duidelijk dat voor wat betreft toegang en ontwerp hiervoor een specifieke aanpak is vereist. Van belang is ook dat mensen **bewust** worden van de grotere impact op de samenleving, maar ook op hun eigen persoon, bijvoorbeeld door het risico op discriminatie. Beleidsmakers kunnen hier opnieuw een rol spelen met betrekking tot bewustwording en informatieverstrekking.

5.4. Welke tools kunnen worden gebruikt om aan de ethische vereiste te voldoen?

- Ethical OS Toolkit: helpt om moeilijk te voorspellen en onwelkome consequenties bij het ontwikkelen van op AI-gebaseerde producten en projecten te voorkomen.
- Data Ethics Canvas
- Aanpak begeleidingsethiek
- Artificial Intelligence Impact Assessment
- Aequitas: is bedoeld om te analyseren of er vooroordelen aanwezig zijn in de gebruikte data en modellen. De audit kan via de desktop of een online tool worden uitgevoerd.
- Building an Algorithm Tool: voorziet ethische vragen die gesteld kunnen worden tijdens het gehele AI-proces (het ontwerp, de ontwikkeling, de testfase en de implementatie).
- AI System Ethics Self-Assessment Tool: laat toe om na te gaan hoe ethisch een bepaalde AI-toepassing is aan de hand van vier ethische principes: eerlijkheid, verantwoordelijkheid, transparantie, uitlegbaarheid.
- Unbias Toolkit: is bedoeld om de online ervaringen van jongeren te delen met beleidsmakers, regulators en de ICT-industrie.
- Data Ethics Framework
- SDoC for AI / AI service FactSheets
- Ethics framework van Machine Intelligence Garage: bestaat uit zeven principes met elk een set vragen die kunnen leiden tot een beter begrip van hoe om te gaan met ethiek in design.
- Data Collection Bias Assessment: voorziet dat vanaf het begin van de datacollectie enkele keuzes vast liggen zodat eventuele vooroordelen in een vroeg stadium kunnen worden ontdekt.
- AI Blindspots Kaartenset
- Tarot Cards of Tech

- AI Explainability 360: biedt verschillende algoritmes aan die kunnen worden gebruikt om explainability en fairness onderdeel te laten worden van AI-systemen.

Hoofdstuk 6: Ethische vereiste 6 - maatschappelijk en milieuwelzijn

6. Ethisch Vereiste 6: Maatschappelijk en milieuwelzijn

6.1. Wat betekent de ethische vereiste?

Deze ethische vereiste vormt de uitdrukking van de ethische beginselen van **schadepreventie en rechtvaardigheid**. Deze vereiste houdt in dat bij de ontwikkeling, het ontwerp en gebruik van AI-systemen ook met **andere belanghebbenden** – de brede maatschappij, het milieu en andere wezens met gevoel – rekening wordt gehouden. Duurzaamheid en economische verantwoordelijkheid van AI-systemen moet worden aangemoedigd en onderzoek in dit veld moet worden gestimuleerd.

Dit ethisch vereiste heeft **drie sub-componenten**, namelijk (1) duurzaamheid en milieuvriendelijkheid, (2) sociale aspecten en (3) vrijwaring van democratie en samenleving.

AI-systemen moeten vooreerst **duurzaam en milieuvriendelijk** zijn. AI-systemen zijn met betrekking tot milieu een tweesnijdend zwaard. Enerzijds verbruiken AI-systemen ontzettend veel energie, wat een extra belasting op het milieu met zich meebrengt. Anderzijds kunnen AI-systemen ook juist gebruikt worden om patronen in het energieverbruik te meten en te herkennen en zo een efficiëntere besteding van energie bekomen. Het proces van de ontwikkeling, de installatie en het gebruik, alsook de volledige toeleveringsketen moeten daarom met het oog op duurzaamheid worden gecontroleerd. Maatregelen die de milieuvriendelijkheid van de toeleveringsketen van AI-systemen stimuleren, moeten worden aangemoedigd.

AI-systemen moeten daarnaast rekening houden met de **sociale gevolgen**. Het gebruik van AI-systemen kan immers een impact hebben op onze sociale relaties en hechting. AI-systemen kunnen sociale vaardigheden vergroten, maar kunnen evengoed bijdragen tot de verslechtering ervan. Het fysieke en geestelijke welzijn kan hierdoor worden geraakt. De effecten van AI-systemen moeten daarom zorgvuldig worden afgewogen bij het ontwerp, de installatie en de ingebruikname. In de ALTAI lijst wordt vooral ingegaan op de impact op werk en vaardigheden.

AI-systemen moeten tot slot de **samenleving en democratie vrijwaren**. Ze moeten democratische processen onderhouden en bevorderen en de pluraliteit van de waarden en levenskeuzen van mensen respecteren. Ze mogen democratische processen, menselijk overleg of democratische kiesstelsels niet ondermijnen. Ook moeten AI-systemen zo worden geprogrammeerd dat ze niet op manieren werken waardoor de basisbeginselen van de rechtsstaat en de toepasselijke wet- en regelgeving worden ondermijnd. Een eerlijke procesgang en gelijkheid voor de wet moet worden gewaarborgd.

6.2. Welke regels zijn een uitdrukking van de ethische vereiste of kunnen dienen als inspiratiebron?

De ALTAI lijst voorziet per aangehaald sub-component verschillende vragen. We geven hieronder een overzicht van de (gebundelde) vragen per sub-component met een overzicht van relevante wetgeving of wetgeving die als inspiratie kan dienen bij de ontwikkeling en het gebruik van AI-systemen.

6.2.A. Duurzaamheid en milieuvriendelijkheid

Zijn er mogelijke negatieve gevolgen van het AI-systeem op het milieu en welke mogelijke impact kan worden geïdentificeerd?

MILIEUKWALITEITSNORMEN

Er is heel wat milieuregelgeving te vinden. De algemene bepalingen vindt men terug in het **Vlaams Decreet van 5 april 1995 houdende algemene bepalingen inzake milieubeleid** (DABM). Krachtens artikel 2.2.1. e.v. stelt de Vlaamse Regering ter bescherming van het milieu **milieukwaliteitsnormen** vast die bepalen aan welke kwaliteitseisen de onderdelen van het milieu moeten voldoen. Er zijn twee soorten milieukwaliteitsnormen: basismilieukwaliteitsnormen en bijzondere milieukwaliteitsnormen.

Deze milieukwaliteitsnormen worden gedefinieerd in het Besluit van de Vlaamse Regering van 1 juni 1995 houdende de **algemene en sectorale bepalingen inzake milieuhygiëne** (VLAREM II). VLAREM voorziet ook in verschillende risicoklassen voor activiteiten. Naargelang het risico hoger of lager is, deelt men de inrichtingen en activiteiten in klasse 1 (hoogste risico), 2 of 3 (laagste risico).

Voor de handhaving van de milieukwaliteitsnormen is **monitoring** essentieel om de toestand van alle onderdelen van het milieu te kunnen bepalen en deze doorheen de tijd te kunnen opvolgen, alsook om eventuele overschrijdingen en hun oorzaken te kunnen vaststellen.

MILIEUEFFECTRAPPORTERING EN VEILIGHEIDSRAPPORTERING

In navolging van o.a. het verdrag van Espoo inzake milieu-effectrapportage in grensoverschrijdend verband, alsook Richtlijn 2011/92 betreffende de milieueffectbeoordeling van bepaalde openbare en particuliere projecten of Richtlijn 2011/42 betreffende de beoordeling van de gevolgen van het milieu van bepaalde plannen en programma's, voorzien verschillende bepalingen in Vlaamse decreten in een algemene verplichting tot **milieueffectrapportering**. Ook de **veiligheidsrapportering** die gericht is op het voorkomen van ongevallen is relevant.

Titel IV van het DABM voorziet de decretale basis voor alle vormen van milieueffectrapportering. Dit is de procedure waarbij, voorafgaande aan een bouw- of milieuvergunningsaanvraag voor een bepaald

project of voorafgaand aan een bepaald plan, de **milieugevolgen worden bestudeerd en geëvalueerd**. Zo kunnen schadelijke effecten voor het milieu in een vroeg stadium worden ingeschat en opgevangen.

Milieueffectenrapportering is ook een belangrijk onderdeel voor vergunningsprocedures, zoals de omgevingsvergunning. Voor bepaalde projecten moet de overheid eerst vaststellen of voor het betrokken project een milieueffectenrapport moet worden ingediend.

Veiligheidsrapportage is de procedure die al dan niet leidt tot het opstellen en goedkeuren van een ruimtelijk veiligheidsrapport of een omgevings-veiligheidsrapport over een voorgenomen actie en in voorkomend geval tot het gebruik ervan als hulpmiddel bij de besluitvorming omtrent deze actie.

VEILIGHEIDSRAPPORTERING OVER DE EXPLOITATIE VAN INRICHTINGEN

In navolging van de Richtlijn betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken (SEVESO III), voorziet het Samenwerkingsakkoord van 16 februari 2016 betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken in verschillende verplichtingen die de exploitant van bepaalde inrichtingen moet naleven om ernstige ongevallen met gevaarlijke stoffen te voorkomen. De exploitant moet alle maatregelen nemen om zware ongevallen te voorkomen en om de gevolgen daarvan voor de menselijke gezondheid en het milieu te beperken. Hij moet ook de naleving van alle verplichtingen kunnen aantonen (art. 5).

BODEMSANERING

Ter uitvoering van Richtlijn 2010/75 inzake industriële emissies, voorziet het Bodemdecreet ook in bijkomende regels met betrekking tot de mogelijkheid van inrichtingen en installaties om bodemverontreiniging te veroorzaken. Dit wordt verder uitgevoerd in het Besluit van 14 december 2007 van de Vlaamse Regering houdende vaststelling van het Vlaams reglement betreffende de bodemsanering en de bodembescherming (VLAREBO). Het decreet voorziet o.a. in een regeling voor identificatie en inventarisatie van verontreinigde gronden, een regeling saneringsplicht en aansprakelijkheid en een regeling bij overdracht van gronden en sluiten van inrichtingen.

ENERGIE (EN ELEKTRICITEIT IN HET BIJZONDER)

AI-systemen hebben inzake energie vooral als nut dat zij kunnen worden gebruikt om de algemene energie-efficiëntie te verbeteren.

Verschillende voorschriften verplichten om voor bepaalde installaties de **energieprestaties** te melden. Evenzeer worden verschillende energieprestatievereisten opgelegd. Veel bepalingen in de Vlaamse energieprestatieregelgeving zijn het direct gevolg van deze eisen die door de EU (bv. Richtlijn 2010/31) zijn opgelegd (art. 11.1.1. e.v. van het Energiedecreet). Verder moet voor gebouwen ook een **energieprestatiecertificaat** (EPC) worden gehanteerd (art. 9.2.1. Energiebesluit). In de toekomst kan het gebruik van AI-systemen in de energievoorziening gebruikt worden om dit certificaat gunstig te

beïnvloeden.

Zowel om de impact van AI-systemen op het milieu in kaart te brengen als om het verbruik van energie te optimaliseren, is het belangrijk om het energieverbruik correct te meten. Hierbij kunnen AI-systemen worden gebruikt in de vorm van **slimme meters en smart grids**. Slimme meters zijn digitale meters die in real time het energieverbruik meten en doorgeven aan de netbeheerder. Smart grids (slimme netwerken) zijn netwerken waarbij deze informatie wordt gebruikt om elektriciteit in real time te brengen naar die plaatsen die haar het meest nodig hebben.

Het gebruik van smart grids en slimme meters wordt in Europese regelgeving en beleidsdocumenten uitgebreid aangemoedigd (bv. art. 3, lid 11 Elektriciteitsrichtlijn). Verder zijn ook de Energie-Efficiëntie-richtlijn en Richtlijn 2019/944 relevant. Vlaanderen heeft ervoor geopteerd om de slimme meter in te voeren voor de meting van elektriciteit en voor de meting van het aardgasverbruik. De desbetreffende bepalingen vindt men terug in het Energiedecreet en het Energiebesluit. Deze documenten bevatten eveneens bepalingen rond de verwerking van persoonsgegevens die samen met de AVG moeten worden gelezen.

Grote ondernemingen moeten zich laten onderwerpen aan een **verplichte energieaudit**. De relevante bepalingen zijn terug te vinden in Titel 1 van het VLAREM (artikel 5 §8), artikel 7.7.2. van het Energiedecreet en Hoofdstuk V van het Energiebesluit. De regels voorzien in een verplichting tot opmaak van een energieplan, een energiestudie en een energieaudit.

SPECIFIEKE EMISSIENORMEN VOOR VOERTUIGEN

Aangezien **autonome motorvoertuigen** een van de meest bekende AI-systemen zijn, past het om ook hier te verwijzen naar de milieuvereisten die gelden voor verschillende soorten voertuigen zoals Verordening 2019/361 van 17 april tot vaststelling van CO2-emissienormen voor nieuwe personenauto's en nieuwe lichte bedrijfsvoertuigen of Verordening 2019/1242 van 20 juni 2019 tot vaststelling van CO2-emissienormen voor nieuwe zware bedrijfsvoertuigen.

PRODUCTVEILIGHEID

De bepalingen rond **productveiligheid** in het WER overlappen op sommige vlakken ook met de bescherming van het milieu. De risico's voor de veiligheid en gezondheid van personen omvat immers ook de bescherming van het leefmilieu, dat op haar beurt de veiligheid en gezondheid van personen kan schaden. Een voorbeeld vindt men terug in de essentiële vereisten van machines zoals bepaald in Bijlage I van het KB van 12 augustus 2008 betreffende het op de markt brengen van machines. Risico's door het gebruik van brandstoffen, trillingen of straling moeten worden vermeden bij het ontwikkelen van een machine.

Zie voor meer informatie ook "Hoofdstuk 2: Ethische vereiste 2 - technische robuustheid en veiligheid".

PRODUCTNORMEN

De **Verklaring van Rio** bepaalt dat staten niet-duurzame productiewijzen en consumptiepatronen moeten beperken en elimineren en passende demografische beleidsmaatregelen moeten nemen om duurzame ontwikkeling en een betere levenskwaliteit te bereiken.

De Wet van 21 december 1998 betreffende de productnormen ter bevordering van duurzame productie- en consumptiepatronen en ter bescherming van het leefmilieu, de volksgezondheid en de werknemers voorziet in **specifieke normen betreffende de kwaliteitsnormen** voor producten. Alle producten die op de markt worden gebracht moeten zodanig ontworpen zijn dat hun fabricage, voorziene gebruik en verwijdering de volksgezondheid niet aantasten en niet of zo weinig mogelijk bijdragen tot een toename van de hoeveelheid en de mate van schadelijkheid van afvalstoffen en tot andere vormen van verontreiniging (art. 4.).

De Koning (de federale regering) kan in functie van deze bescherming **bijkomende maatregelen** nemen. Er zijn tal van bijkomende Koninklijke Besluiten (KB) aangenomen zoals het KB van 25 maart 1999 houdende bepaling van productnormen voor verpakkingen. Een KB van 19 maart 2004 bepaalt de productnormen voor voertuigen. Een KB van 17 maart 2013 voorziet normen ter beperking van het gebruik van bepaalde gevaarlijke stoffen in elektrische en elektronische apparatuur. In navolging van de EU-Verpakkingsrichtlijn, voorzien artikel 10 e.v. Wet Productnormen in een verbod om producten op de markt te brengen met verpakkingen die niet-herbruikbaar zijn of niet vatbaar zijn voor nuttige toepassing. In uitvoering van de EU-Richtlijn betreffende de totstandkoming van een kader voor het vaststellen van eisen inzake ecologisch ontwerp voor energie-gerelateerde producten voorzien artikel 14bis e.v. van de Wet Productnormen in bijkomende vereisten voor alle producten die energie verbruiken.

BEDRIJFSINTERNE MILIEUZORG – DE EMAS-VERORDENING EN DE DECRETAAL VERPLICHTE MILIEUAUDIT

Verordening 1221/2009 inzake de vrijwillige deelneming van organisaties aan een communautair **milieubeheer- en milieuauditsysteem** (EMAS) voorziet voor alle organisaties een vrijwillig milieubeheer- en milieuauditschema. Een organisatie die voor een EMAS-registratie in aanmerking wenst te komen, dient een initiële milieuanalyse te doen van al haar activiteiten, producten en diensten. Krachtens artikel 3.3.2. van het Decreet Algemene Bepalingen inzake Milieubeleid kan de Vlaamse Regering ook de instanties aanduiden die verplicht zijn tot een periodieke dan wel eenmalige verplichte milieuaudit.

ISO 14000-NORMENFAMILIE

De ISO-norm 14001-2015 voorziet een internationale norm voor een **milieu-impact analyse**. Het is de eerste norm in een 'familie' van standaarden die technische specificaties voorziet voor milieubeheersystemen.

EU-MILIEUKEUR

Verder voorziet Verordening 66/2010 betreffende de EU-milieukeur in een label voor producten: het **Ecolabel**. Dit systeem beoogt ook door een keurmerk bij te dragen tot een verhoogd niveau van

bescherming. Dit systeem kent tot op heden een beperkt succes in de praktijk.

Werden, waar mogelijk, mechanismen in werking gesteld om de milieu-impact van de ontwikkeling, de installatie en het gebruik van het AI-systeem in kaart te brengen (bijvoorbeeld, de hoeveelheid energie die gebruikt wordt en de CO2-uitstoot)?

VRIJE TOEGANG TOT MILIEU-INFORMATIE

De EU-Richtlijn inzake de toegang van het publiek tot milieu-informatie verplicht de lidstaten om ervoor te zorgen dat overheidsinstanties ertoe gehouden zijn de **milieu-informatie** waarover zij beschikken of die voor hen wordt beheerd aan elke aanvrager op verzoek ter beschikking te stellen, zonder dat deze hiervoor een belang hoeft aan te voeren. Hierop gelden wel enkele uitzonderingen.

Deze omzetting van deze Richtlijn vindt men voor Vlaanderen terug in de artikelen II.36 e.v. van het Bestuursdecreet die bijzondere bepalingen voorzien voor de toegang tot milieu-informatie. Deze informatie kan worden gebruikt in het kader van AI-projecten ter bescherming van het milieu. Let ook op dat het omgekeerde eveneens kan: de bescherming van handelsgeheimen – een economisch belang dat in alle softwareactiviteiten van essentieel belang is – kan ook worden gebruikt om verzoeken om milieu-informatie af te blokken.

MILIEUEFFECTRAPPORTERING EN OMGEVINGSVERGUNNING

De voornaamste bepalingen inzake de milieueffectrapportering werden in de voorgaande vraag al besproken.

BEDRIJFSINTERNE MILIEUZORG

Het Decreet Algemene Bepalingen inzake Milieubeleid voorziet in verschillende maatregelen die betrekking hebben tot **bedrijfsinterne milieuzorg** (art. 3.1.1. en verder). Deze houden in dat elk bedrijf intern duurzame productiepatronen nastreeft en de milieubelasting van een bedrijf in al zijn aspecten beheerst en beperkt.

Sommige maatregelen zijn gericht op beperking van de milieu-impact (bv. de milieucoördinator). Andere verplichtingen omvatten ook verschillende vormen van rapportering die alle ondernemingen – en dus ook ondernemingen die AI-systemen ontwikkelen, installeren of gebruiken – moeten naleven. De milieuaudit werd reeds besproken bij de behandeling van de voorgaande vraag.

BODEMSANERING

Ook dit werd reeds in voorgaande vragen besproken.

BEHEER VAN AFVALSTOFFEN

In navolging van o.a. de Kaderrichtlijn Afvalstoffen voorziet het **Materialendecreet** in verschillende verplichtingen bij het gebruik van afvalstoffen. Natuurlijke en rechtspersonen die afvalstoffen beheren zijn verplicht om een chronologisch **afvalstoffenregister** bij te houden dat o.a. volgende elementen omvat: de aangevoerde hoeveelheid, aard, oorsprong en indien van toepassing de bestemming, frequentie van de inzameling, wijze van vervoer en van behandeling van de afvalstoffen. Nadere regels zijn uitgewerkt in het VLAREMA.

SPECIFIEKE PRODUCTNORMEN VOOR VOERTUIGEN

Verordening 2019/361 voorziet in een jaarlijkse publicatie van de **milieuprestaties** van de fabrikanten van personenwagens. Verordening 2019/1242 voorziet ook in specifieke **monitoringverplichtingen** voor de producenten van zware bedrijfsvoertuigen.

ENERGIERECHT

De belangrijkste maatregelen voor individuele gebruikers – de digitale meter en de energieaudit – werden reeds besproken. Ook het energieprestatiecertificaat werden al besproken.

ENERGIERAPPORT

Krachtens art. 12.1.1.-12.1.2. van het Energiedecreet publiceert de Vlaamse Overheid jaarlijks een **energierapport**. Dit bevat voor het Vlaamse Gewest globale gegevens betreffende het energieverbruik.

PRODUCTNORMEN

Dit werd reeds besproken.

ISO 14000-NORMENFAMILIE

Dit werd reeds besproken.

EU-MILIEUKEUR

Dit werd reeds besproken.

?	Werden maatregelen gedefinieerd om de milieu-impact van het AI-systeem te verminderen gedurende zijn levenscyclus?

VERGUNNINGSPLICHT EN DE OMGEVINGSVERGUNNING

Sinds 1991 geldt voor verschillende projecten en plannen een v**ergunningsplicht**. Krachtens art. 5.2.1. Decreet Algemene Bepalingen Milieubeleid stelt de Vlaamse Regering een indelingslijst vast en bepaalt ze of de activiteit en inrichting aan een vergunningsplicht is onderworpen (op basis van risico's).

De milieuvergunningsprocedure werd in 2014 vervangen door het Decreet betreffende de omgevingsvergunning, met als uitvoeringsbesluit het Omgevingsvergunningsbesluit. De **omgevingsvergunning** vervangt de milieuvergunning, de stedenbouwkundige vergunning, de verkavelingsvergunning en de meldingsprocedure. De aanvragen worden ingediend bij één loket, het Omgevingsloket, waarna één openbaar onderzoek en één adviesronde worden georganiseerd. Niemand mag zonder voorafgaande omgevingsvergunning een project dat krachtens de Vlaamse Codex of het Decreet Algemene Bepalingen Milieubeleid onderworpen is aan een vergunningsplicht, uitvoeren, exploiteren, verkavelen of een vergunningsplichtige verandering doorvoeren.

BEDRIJFSINTERNE MILIEUZORG

Het Decreet Algemene Bepalingen inzake Milieubeleid voorziet ook in bijkomende verplichtingen inzake bedrijfsinterne milieuzorg (bv. aanstelling milieucoördinator). Er is ook een meldings- en waarschuwingsplicht bij accidentele emissies (art. artikel 3.7.1.).

BODEMSANERING

Zoals reeds besproken, voorziet het Bodemdecreet in een **algemene saneringsplicht** die van toepassing is op de exploitant, de gebruiker en de eigenaar van de grond of inrichting.

PRODUCTNORMEN

De wetgeving inzake productnormen werd reeds besproken. De verplichtingen ingevolge deze wet zorgen ervoor dat producenten ook de mogelijke risico's van hun producten moeten **verminderen.**

VOORKOMEN VAN ZWARE ONGEVALLEN MET GEVAARLIJKE STOFFEN

Zoals reeds besproken, verplicht het Samenwerkingsakkoord voor de voorkoming van zware ongevallen aan alle exploitanten om de nodige maatregelen te nemen om zware ongevallen te voorkomen en de gevolgen voor de menselijke gezondheid te beperken. Verder moet de exploitant ook een **preventiebeleid** hebben vastgesteld en gedocumenteerd dat borg staat voor een hoog beschermingsniveau voor de menselijke gezondheid. De exploitant moet ook een **intern noodplan** optellen.

BEHEER VAN AFVALSTOFFEN

Naast verplichtingen inzake de rapportering van afvalstoffen, voorziet het Materialendecreet ook in bijzondere bepalingen die de **verwerking van afvalstoffen efficiënter** moet doen verlopen.

ENERGIE

Er werd reeds gesproken over de energieprestatiecertificaten voor gebouwen, over de digitale meter en de energieaudit. Deze maatregelen strekken niet alleen tot het in kaart brengen van de impact van de inrichtingen op het energieverbruik, maar voorziet ook een incentive om het verbruik te verminderen.

6.2.B. Sociale gevolgen: werk en vaardigheden

Indien er sprake is van een rechtstreekse interactie tussen AI-systemen en de mensen:
- Werd onderzocht of het AI-systeem mensen stimuleert om verbondenheid en empathie ten aanzien van het systeem te ontwikkelen?
- Werd gezorgd dat het AI-systeem duidelijk aangeeft dat zijn sociale interactie gesimuleerd is en dat het niet tot 'begrip' en 'gevoelens' in staat is?

CONSUMENTENBESCHERMING EN PRODUCTVEILIGHEID

Er zijn nog geen specifieke vormen van communicatie van AI-systemen die dergelijk gedrag zouden aangeven. Dit soort specifieke regelgeving lijkt ook niet nodig aangezien er reeds een algemeen kader is met betrekking tot **transparantie en informatieverplichtingen** vanuit o.a. het consumentenrecht en het productveiligheidsrecht.

Aangezien AI-systemen verschillende vormen van empathie kunnen opwekken, is aandacht voor **risico's voor mentale gezondheid**, alsook verdere convergentie tussen het veiligheidsregime voor hardware en software noodzakelijk om in alle gevallen een evenwaardig niveau aan veiligheid te garanderen.

BESCHERMING VAN PERSOONSGEGEVENS

Onder de AVG zijn er ook een aantal bepalingen die relevant zijn in kader van de interactie tussen mens en AI-systeem. Vele van deze bepalingen kwamen elders al aan bod. De verwerkingsverantwoordelijke moet de gegevens bijvoorbeeld verwerken op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is (art. 5,lid 1, a)). Er zijn ook een aantal informatieverplichtingen bij het bestaan van **geautomatiseerde individuele besluitvorming** (art. 13-14 en 22), alsook voor het uitvoeren van een **GEB** (art. 35).

Heeft het AI-systeem een impact op menselijk werk en werkorganisatie?

ALGEMEEN

Er werden reeds meerdere mogelijke risico's gedefinieerd die AI-systemen veroorzaken. Dergelijke systemen zouden een aanzienlijke **disruptie** kunnen veroorzaken, ook op vlak van werk en arbeid. De inhoud van een job en het takkenpakket zal mogelijks veranderen door de toenemende automatisering. AI-systemen kunnen echter ook de veiligheid op andere vlakken verbeteren. Robots kunnen worden gebruikt om het leven van werknemers aangenamer te maken of om hen uit onveilige situaties te houden.

Toch zijn er een **aantal bepalingen** die steeds in rekening moeten worden gehouden bij de introductie van AI op het werk, waaruit blijk dat het welzijn van de mens steeds primeert.

MENSENRECHTEN

De internationale rechten op en in verband met arbeid vindt men terug in het **Internationaal Verdrag inzake Economische, Sociale en Culturele Rechten**, bv. het recht op arbeid en het recht van een ieder op billijke en gunstige arbeidsvoorwaarden (art. 6-9).

Op het niveau van de Raad Van Europa kan worden verwezen naar het **Europees Sociaal Handvest** dat voorziet in een recht op arbeid (art. 1), recht op billijke arbeidsvoorwaarden (art. 2), recht op veilige en hygiënische arbeidsomstandigheden (art. 3), recht op vakopleiding (art. 10) en recht op bescherming van de gezondheid (art. 11).

Op het niveau van de Europese Unie voorziet het **Handvest van de Grondrechten van de Europese Unie** in de vrijheid van beroep en het recht om te werken (art. 15), alsook de vrijheid van ondernemerschap (art. 16). Ook voorziet het in o.a. het recht op informatie en raadpleging van de werknemers binnen de onderneming (art. 27), het recht op collectieve onderhandelingen en collectieve actie (art. 28), het recht op arbeidsbemiddeling (art. 29), de bescherming bij een kennelijk en onredelijk ontslag (art. 30), alsook het recht op rechtvaardige en billijke arbeidsomstandigheden en -voorwaarden (art. 31).

De **Belgische Grondwet** voorziet het recht om een menswaardig leven te leiden. Dit recht omvat o.a. het recht op arbeid en de vrije keuze van beroepsarbeid en het recht op sociale zekerheid (art. 23).

WELZIJNSWET EN CODEX OVER HET WELZIJN OP HET WERK

Er is ook specifieke wetgeving rond welzijn en veiligheid op werk. De Welzijnswet is de basiswet op het vlak van veiligheid en gezondheid op het werk. Deze wet schept een kader waarin ook de uitvoeringsbesluiten worden genomen. Deze uitvoeringsbesluiten worden hoofdzakelijk gebundeld in de Codex over het welzijn op het werk. De codex is opgebouwd volgens een filosofie die vernieuwend is ten opzichte van deze waarvan uitgegaan werd in het Algemeen Reglement voor de Arbeidsbescherming (ARAB), de vroegere codificatie van voorschriften inzake arbeidsveiligheid en gezondheid.

Werd het pad geëffend voor de introductie van het AI-systeem in een organisatie door de getroffen werknemers en hun vertegenwoordigers (vakbonden, Europese arbeidsraden) op voorhand te informeren en te raadplegen?

CAO NR. 39

Cao nr. 39 van 13 december 1983 betreffende de voorlichting en het overleg inzake de sociale gevolgen van de invoering van nieuwe technologieën voorziet in een specifieke regeling die bepaalde ondernemingen verplicht om de werknemers te **informeren** indien hij/zij een nieuwe technologie wenst in te voeren. Dit is dus een zinvol instrument om werknemers in te lichten indien men een AI-systeem wenst uit te rollen op de werkplek. De te geven informatie heeft o.a. betrekking op de aard van de technologie,

de aard van de sociale gevolgen en de termijn van inwerkingstelling. Ook moet de werkgever met de werknemersvertegenwoordigers **overleg plegen** over de sociale gevolgen van de invoering van de nieuwe technologie (art. 2).

WELZIJNSWETGEVING EN CODEX WELZIJN OP HET WERK

Ook met bepalingen over veiligheid en welzijn in de reeds aangehaalde Welzijnswet en de Codex over het welzijn op het werk moet rekening worden gehouden.

Werden maatregelen genomen om te verzekeren dat de impact van het AI-systeem op menselijk werk goed begrepen is?
Werd ervoor gezorgd dat werknemers begrijpen hoe het AI-systeem werkt, welke capaciteiten het heeft en welke capaciteiten het niet heeft?

CAO NR. 39

De **informatieverplichtingen** en het voorziene overleg in Cao nr. 39 zijn mogelijks relevant in dit verband (o.a. over de aard van de nieuwe technologie, over de gezondheid en de veiligheid van de werknemers en de vakbekwaamheid en de eventuele maatregelen voor opleiding en omscholing van de werknemers). Deze maatregelen voorzien op summiere en vage wijze in een informatieplicht omtrent de functionaliteiten van het AI-systeem en welke capaciteiten het al dan niet heeft.

WELZIJN OP HET WERK

Richtlijn 89/391 betreffende de tenuitvoerlegging van maatregelen ter bevordering van de verbetering van de veiligheid en de gezondheid van de werknemers op het werk voorziet in **algemene verplichtingen** van de werkgever om de **veiligheid en de gezondheid** van de werknemers te garanderen (art. 5). De richtlijn voorziet ook in een **verplichte voorlichting** van de werknemers o.a. over de risico's voor de veiligheid en de gezondheid alsmede de beschermings- en preventiemaatregelen en activiteiten (art. 10).

De werkgever is volgens de Arbeidsovereenkomstenwet verplicht om als een goed huisvader te zorgen dat de arbeid wordt verricht in **behoorlijke omstandigheden** met betrekking tot de veiligheid en de gezondheid van de werknemer en dat bij een ongeval de eerste hulpmiddelen kunnen worden verstrekt (art. 20, 2°). Een werkgever moet er dus voor zorgen dat werknemers op een veilige manier kunnen samenwerken met AI-systemen.

De Welzijnswet voorziet ook in bijzondere verplichtingen van de werkgever om de **nodige maatregelen te nemen ter bevordering van het welzijn van werknemers bij de uitvoering van hun werk** (art. 5 §1). Een werkgever moet o.a. het werk aanpassen aan de mens met betrekking tot de inrichting van de werkposten en de keuze van de werkuitrusting en de werk- en productiemethoden om monotone arbeid en tempo-gebonden arbeid draaglijker te maken en de gevolgen voor de gezondheid te beperken.

Verder voorziet de Codex over het welzijn op het werk in bijkomende verplichtingen omtrent de **arbeidsmiddelen** (bv. gebruikte machines, apparaten, gereedschappen en installaties). De werkgever moet ervoor zorgen dat de arbeidsmiddelen geschikt zijn voor het uit te voeren werk zodat de veiligheid en de gezondheid van de werknemers gewaarborgd blijft tijdens het gebruik ervan (zie o.a. art. IV.2-1). De werkgever is ook verplicht om de nodige maatregelen te nemen om ervoor te zorgen dat de werknemers over voldoende informatie en, in voorkomend geval, over gebruiksaanwijzingen betreffende de op het werk gebruikte arbeidsmiddelen beschikken (zie o.a. art. IV.2-5). Op grond van de welzijnswetgeving is de werkgever dus reeds verplicht om ook over AI-systemen de nodige informatie te geven omtrent de manier waarop zij het AI-systeem dienen te gebruiken.

Kan het AI-systeem het risico creëren dat het personeel vaardigheden verliest?
Werden maatregelen genomen om het verlies van vaardigheden tegen te gaan?
Bevordert of vereist het AI-systeem nieuwe (digitale) vaardigheden?

Werd voorzien in opleidingen en materialen voor reskilling en up-skilling?

CAO NR. 39

De **informatieverplichting en het voorziene overleg** in Cao nr. 39 werden reeds besproken. Indien een AI-systeem het risico creëert dat personeelsleden niet meer de gepaste vaardigheden hebben om hun job uit te oefenen (deskilling) moet de werkgever de werknemers informeren. Het overleg betreft o.a. de vakbekwaamheid en de eventuele maatregelen voor opleiding en omscholing van de werknemers wanneer AI wordt ingezet.

Van een echte reskilling is op grond van deze CAO echter niet onmiddellijk sprake. De verplichting tot overleg is maar van toepassing bij 'belangrijke collectieve sociale gevolgen'. Daarnaast is de verplichting om overleg te plegen niet gelijk te stellen met een verplichting om effectief maatregelen te nemen. Cao nr. 39 verplicht de werkgever niet om effectief maatregelen te nemen om werknemers te beschermen tegen het verlies van vaardigheden of om beroepsopleidingen te voorzien.

VERPLICHTINGEN INZAKE WELZIJN OP HET WERK

Op grond van art. I.2-21 van de Codex over het welzijn op het werk is de werkgever verplicht om ervoor te zorgen dat iedere werknemer een **voldoende en aangepaste vorming** in verband met het welzijn van de werknemers bij de uitvoering van hun werk ontvangt die speciaal gericht is op zijn werkpost of functie. Deze vorming wordt o.a. gegeven bij de invoering van een nieuwe technologie.

BEROEPSOPLEIDING

Bij Decreet van 7 mei 2004 werd de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (VDAB) opgericht. De specifieke organisatie van de beroepsopleidingen wordt geregeld bij het Besluit van 5 juni 2009 houdende de organisatie van de arbeidsbemiddeling en de beroepsopleiding. De VDAB heeft

als bevoegdheid om bijvoorbeeld aan een niet-werkende werkzoekende en de verplicht ingeschreven werkzoekenden voor te stellen om een passende beroepsopleiding te volgen (art. 66).

Inzake AI is het aanbod van opleidingen op heden beperkt, maar wel bestaande: de VDAB organiseert enkele opleidingen omtrent artificiële intelligentie, zowel voor werkzoekenden als voor werknemers.

6.2.C. Vrijwaring samenleving en democratie

Kan het AI-systeem een negatieve impact hebben de brede maatschappij of op democratie?
Werd een inschatting gemaakt van de impact van het gebruik van het AI-systeem op andere actoren dan de (eind)gebruiker en de betrokkene, zoals mogelijke onrechtstreeks getroffen belanghebbenden of de brede maatschappij?

ALGEMENE SCHETS: MENSENRECHTEN

AI-systemen kunnen een aanzienlijke impact hebben op de **uitoefening van mensenrechten** die als doel hebben het vrijwaren van de menselijke waardigheid en ons democratisch bestel. De relevante mensenrechten vindt men o.a. terug in het Internationaal Verdrag inzake burgerrechten en politieke rechten; het Europees Verdrag voor de Rechten van de Mens, het Handvesten van Grondrechten van de Europese Unie en de Belgische Grondwet. Denk bv. aan het recht op privacy, het recht op vrijheid van gedachte, geweten en godsdienst, het recht op vrijheid van meningsuiting en de vrijheid van vereniging. Het gebruik van het social credit-systeem in China of het schandaal rond Cambridge Analytica tonen aan dat het vrijwaren van fundamentele rechten cruciaal is en dat mensen kunnen worden geraakt in hun autonomie. Hierover kan meer informatie worden gevonden onder "Hoofdstuk 1: Ethische vereiste 1 - menselijke controle en menselijk toezicht".

Anderzijds kunnen AI-systemen ook worden gebruikt om de **werking van democratische instellingen** te verstoren. AI-systemen lenen zich bijzonder goed tot het maken en verspreiden van valse of illegale informatie, die het moeilijker maakt om de juiste informatie te achterhalen. Enkele voorbeelden zijn deepfakes of de mogelijkheid voor derden om AI-systemen te manipuleren om valse of schadelijke meningen te spuien (cf. racistische chatbot Tay).

Mensenrechten zijn echter niet absoluut. Op het recht op bescherming van het privéleven, het recht op godsdienstvrijheid en het recht op vrijheid van meningsuiting in het EVRM zijn beperkingen toegestaan, voor zover bij wet voorzien en noodzakelijk in het kader van een legitiem doel.

PRODUCTVEILIGHEID

Er zijn bijzondere verplichtingen voor de fabrikanten om de **gezondheid en veiligheid** van alle gebruikers te waarborgen bij de ontwikkeling van producten. De 'gebruiker' is in dit geval niet alleen de consument,

maar iedereen die het goed kan gebruiken. Het vermijden van risico's houdt dan ook in dat risico's ten aanzien van de ruimere omgeving van de gebruikers worden vermeden.

STANDAARDEN

Recent nam de IEEE ook een standaard aan betreffende impact van AI-systemen in het algemeen: IEEE P7010-2020 – IEEE Recommended Practive for Assessing the Human Impact of Autonomous and Intelligent Systems on Human Well-Being.

MILIEURECHT

De regels betreffende de impact op het **leefmilieu en de gezondheid** van mensen werden reeds besproken.

BEPERKINGEN OP SURVEILLANCE EN PROFILERING

Bescherming van persoonsgegevens – beperking van verwerking bepaalde gegevens

Voor elke vorm van verwerking van persoonsgegevens door private entiteiten is de **AVG** uiteraard van toepassing. Deze werd besproken onder Ethisch Vereiste 3: Privacy en databeheer. Hieronder worden enkele bepalingen aangehaald die van belang zijn voor de opmaak van psychometrische profielen en profilering.

Vooreerst dienen de beginselen van o.a. **doelbinding, minimale gegevensverwerking en juistheid** te allen tijde te worden nageleefd (art. 5, lid 1 AVG). Verder moet opgelet worden met de verwerking van **bijzondere categorieën persoonsgegevens**, waaronder gevoelige gegevens en gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten. Deze zijn maar in bepaalde gevallen toegestaan (art. 9).

Verwerkingen van strafrechtelijke gegevens zijn enkel toegestaan onder toezicht van de overheid.

Art. 23 van de AVG voorziet in de mogelijkheid bepaalde **uitzonderingen** te voorzien (bv. nationale en openbare veiligheid). Deze uitzonderingen zijn eveneens terug te vinden in de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Bescherming van persoonsgegevens – profilering en automatische besluitvorming

Verder zijn **automatische besluitvorming en profilering** onder de AVG aan bijzondere regels onderworpen (artikel 13, lid 2, e); artikel 14, lid 2, g)) en heeft de betrokkene het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering (art. 22). De betrokkene heeft ook een uitdrukkelijk recht om bezwaar te uiten tegen elke vorm van verwerking voor direct marketing (artikel 21 AVG). Verder is het in bepaalde gevallen nodig om een **GEB** uit te voeren (art. 35, lid 3 AVG). Niet

toevallig verwijzen deze gevallen naar situaties waarin private surveillance wordt gebruikt en waarin mensen op een systematische en uitgebreide manier worden geprofileerd. Bovendien moet ook een **functionaris van gegevensbescherming** in bepaalde gevallen worden aangesteld. Ook hier werd niet toevallig gekozen voor situaties waarin de verwerkingsverantwoordelijke of de verwerker zich schuldig maakt aan surveillance of waar het risico op surveillance groot is.

Bescherming van persoonsgegevens – geen doorgifte aan derde landen waar andere standaarden gelden

Risico's op inbreuken op mensenrechten of verstoringen van de democratie kunnen ook komen van landen buiten de EU – landen waar een andere standaard geldt. Voor **doorgiften van gegevens** naar derde landen voorziet de AVG eveneens in bijzondere regels (zie bv. art. 44-46).

Verbod op inhoud die op het apparaat van de eindgebruiker wordt geplaatst

In navolging van de e-Privacyrichtlijn verbiedt art. XII.12 van het WER het **opslaan van tekst- en andere berichten** op de apparatuur zonder de toestemming van de gebruiker. En uitzondering hierop geldt voor directe marketing voor bestaande klanten. Deze vindt men terug in het KB betreffende de reglementering van reclame per elektronische post.

Verwerking door ordediensten

Artikel 10 van Richtlijn 2016/680 bepaalt dat bijzondere categorieën van de gegevens mogen worden verwerkt indien deze met inachtneming van **passende waarborgen voor de rechten en vrijheden** van de betrokkene, en voor zover deze wettelijk is toegestaan, noodzakelijk is om de vitale belangen van de betrokkene te beschermen of indien de verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf werden openbaar gemaakt. Deze bepaling wordt overgenomen in de Kaderwet Gegevensbescherming (art. 34).

Profilering die leidt tot discriminatie van personen op grond van hun bijzondere persoonsgegevens is verboden. Verder is elk besluit dat louter op geautomatiseerde verwerking gebaseerd is en dat voor de betrokkene nadelige rechtsgevolgen heeft of hem in aanmerkelijke mate treft, maar toegestaan, indien een wettelijke bepaling voorziet in passende waarborgen voor de rechten en vrijheden, minstens het recht op een menselijke tussenkomst (art. 35). De doorgifte van persoonsgegevens betreffende een betrokkene in het kader van de opsporing en ordehandhaving is maar toegestaan onder de voorwaarden die gesteld worden in de art. 66 e.v.

STRAFRECHTELIJKE BEPERKINGEN OP GEBRUIK VAN AI-SYSTEMEN EN HET VERSPREIDEN VAN INFORMATIE DOOR MIDDEL VAN AI-SYSTEMEN

Geen gebruik maken van AI-systemen voor het plegen van misdrijven

AI-systemen mogen **niet gebruikt worden als middel om misdrijven** te plegen (zie ook art. 66 en 67

Strafwetboek). Men mag dus geen AI-systemen ontwikkelen die zouden dienen om misdrijven te plegen. Merk echter op dat deze bepaling enkel van toepassing is op zij die AI-systemen zouden ontwikkelen die bedoeld zijn om misdrijven te plegen of mensen die AI-systemen zouden opleren met de bedoeling er misdrijven mee te plegen (intentie).

Informaticamisdrijven mogen ook niet door AI-systemen worden gepleegd

Bij de strafbaarstelling van het gebruik van AI-systemen kan men denken aan de **informaticamisdrijven:** valsheid in informatica (artikel 210bis Strafwetboek), informaticabedrog (artikel 504quater Strafwetboek), alsook hacking en informaticasabotage (artikel 550bis en 550ter Strafwetboek).

Het strafrecht verbiedt bepaalde vormen van meningsuiting

Het principe is dat mensen vrij zijn hun mening te hebben en te uiten. In die zin zou men over het internet mogen zeggen wat men wil. Men mag ook zaken die door een AI-systeem verspreid zouden worden zomaar delen. Deze vrijheid is echter niet onbeperkt.

Het strafrecht **verbiedt verschillende vormen van meningen** die kunnen worden gedeeld. Een aantal daarvan kunnen ons inziens relevant zijn voor AI-systemen (bv. fake news, deepfakes): valsheid in informatica (art. 210bis Strafwetboek), laster, eerroof en belediging (art. 443 e.v. Strafwetboek), belaging (artikel 442bis Strafwetboek), aanzetten tot racisme (art. 20 e.v. Antiracismewet), het verspreiden van seksistische meningen (art. 2-3 van de Wet van 22 mei 2014 ter bestrijding van seksisme in de openbare ruimte), pornografie (art. 383bis Strafwetboek), delen van beeld of- geluidsopnames van een ontblote persoon (art. 371/1 Strafwetboek).

ZELFREGULERING IN DE PERS

Persvrijheid is een fundamenteel beginsel onder voorbehoud van beperkingen die hierboven werden genoemd. Naast het strafrecht geldt ook in principe de zelfregulering die voor België wordt uitgevaardigd door de Raad van de Journalistiek. Voor geschreven publicaties geldt de **Code van de Raad voor de Journalistiek**. Dit is geen bindende regelgeving, maar is wel een leidraad die in principe van toepassing is op alle publicaties, ongeacht het medium. Deze code is een vorm van zelfregulering en is dus niet direct afdwingbaar voor een rechtbank.

VERPLICHTINGEN OP GROND VAN HET MEDIARECHT VOOR AUDIOVISUELE BOODSCHAPPEN

In uitvoering van de **Richtlijn Audiovisuele Mediadiensten** voorziet het Mediadecreet in verschillende verplichtingen voor alle omroeporganisaties, maar ook bepalingen die van toepassing zijn op online platformen waarop gebruikers video's uploaden zoals Twitter, YouTube, etc. Art. 37-38 Mediadecreet bepalen dat de vrijheid van meningsuiting gewaarborgd wordt en dat omroepactiviteiten niet mogen aanzetten tot haat en tot geweld. De media-activiteit is echter naar deze platformen verschoven, wat ervoor zorgt dat heel wat 'filters' die bijvoorbeeld redacties zullen moeten toepassen niet automatisch gelden voor deze platformen.

Werden maatregelen ondernomen om de mogelijke maatschappelijke schade van het AI-systeem te beperken?

BESCHERMING VAN PERSOONSGEGEVENS (RISICO VAN SURVEILLANCE EN MANIPULATIE)

Dit werd hierboven reeds besproken.

VEILIGHEID EN MILIEU

Deze werden reeds hierboven besproken en onder "Hoofdstuk 2: Ethische vereiste 2 - technische robuustheid en veiligheid".

HANDHAVING

Er kan ook verwezen worden naar de bespreking onder "Hoofdstuk 7: Ethische vereiste 7 - verantwoording".

Werden maatregelen genomen die ervoor zorgen dat het AI-systeem geen negatieve impact heeft op de democratie?

BEVEILIGING VAN VERKIEZINGEN

Kort gezegd kan men stellen dat de risico's op bijvoorbeeld **stemfraude** beperkt zijn door AI-systemen in België. De reden is dat het huidige stelsel van stemmen nog quasi geheel is gebaseerd op het stemmen op papier of, als er wordt geautomatiseerd, met specifieke stemcomputers, die tot op heden niet verbonden zijn met een netwerk. De specifieke bepalingen zijn terug te vinden in het Decreet van 25 mei 2012 houdende de organisatie van de digitale stemming bij de lokale en provinciale verkiezingen ("Digitaal Kiesdecreet") en de Wet van 7 februari 2014 tot organisatie van de elektronische stemming met papieren bewijsstuk.

RISICO VAN CONCENTRATIE EN ANTWOORDEN VANUIT HET MEDEDINGINGSRECHT

Een ander risico van de opkomst van AI-systemen en de digitalisering in het algemeen is dat slechts een **handvol techbedrijven** – Facebook, Google, Amazon, Apple en Microsoft – de mogelijkheid krijgen om mee te bepalen wat wij zien en horen. Deze techbedrijven zijn ook zodanig groot dat zij stilaan groter worden dan de staten die hen zouden moeten reguleren. Om die reden is er een vrees dat zij hun marktmacht kunnen gebruiken om, onder meer door het gebruik van hun algoritmen, het maatschappelijk debat te sturen zoals zij willen (cf. surveillance capitalism). Deze groei is ook zeer moeilijk te stoppen. WhatsApp en Instagram zijn bijvoorbeeld al eigendom van Facebook.

Het **mededingingsrecht** is dan ook van groot belang. Het mededingingsrecht omvat regels die ervoor zorgen dat de vrije concurrentie tussen bedrijven gehandhaafd blijft. Dit komt ook de werking van de democratie ten goede.

Het mededingingsrecht wordt in België op twee niveaus toegepast. Op het federale niveau staan de bepalingen in boek IV van het WER. De handhaving gebeurt door de Belgische Mededingingsautoriteit. Verder is het mededingingsrecht voor alle zaken die de handel tussen de EU-lidstaten beïnvloeden geregeld op Europees niveau. Deze regels zijn terug te vinden in art. 101 e.v. van het Verdrag betreffende de Werking van de Europese Unie en in de daarbij omzettende verordeningen. De handhaving gebeurt in principe door de Europese Commissie met eventueel een beoordeling door het Hof van Justitie van de Europese Unie. De Commissie heeft bijvoorbeeld Google reeds veroordeeld tot boetes op grond van het koppelen van zijn zoekmachine en browser aan het besturingssysteem van zijn smartphones en voor abusieve praktijken in het beheer van zijn zoekmachine.

BEPERKINGEN OP SURVEILLANCE

Deze werden reeds besproken.

BEPERKINGEN VANUIT HET STRAFRECHT TER VRIJWARING VAN DE MAATSCHAPPELIJKE ORDE EN HET DEMOCRATISCH DEBAT

Deze werden reeds besproken.

REGELS INZAKE DE AANSPRAKELIJKHEID VAN ONLINE DIENSTVERLENERS

In navolging van de art. 12 t.e.m. 15 van de E-commercerichtlijn, voorzien de art. XII.17 t.e.m. XII.20 van het WER in een **algemene uitsluiting van aansprakelijkheid voor online tussenpersonen**. Hiermee wordt gedoeld op alle diensten van de informatiemaatschappij waarbij deze tussenpersonen een louter passieve rol spelen (cf. mere conduit-provider, caching-provider en hosting-provider).

Ten gevolge van de toenemende verspreiding van illegale informatie, schadelijke informatie en onder andere valse informatie, komen deze regels steeds meer onder vuur te staan. In haar mededeling 'De bestrijding van illegale online-inhoud' stelde de Europese Commissie dat onlineplatformen **doeltreffende proactieve maatregelen** moeten nemen voor het opsporen en verwijderen van illegale online-inhoud en niet alleen mogen reageren op meldingen die zij ontvangen. Dit creëert het sterke vermoeden dat onlineplatformen in de toekomst zullen worden verplicht om zelf illegale inhoud te filteren.

6.3. Waar zitten mogelijke punten van verbetering/ aandachtspunten?

Omvangrijke regelgeving over milieu en energie

Voor milieu en energie is er reeds heel wat **regelgeving** die alle omvattende risico's onderwerpt aan toezicht door de overheid. Bovendien legt die regelgeving ook verplichtingen op omtrent het ontwerp

en gebruik van producten, alsook van inrichtingen en installaties. Deze regels bevatten vrij omvangrijke procedures die gebaseerd zijn op algemene normen. Deze normen zijn niet noodzakelijk specifiek geënt op AI-systemen.

Dit hoeft ook niet. De regelgeving hoort geënt te zijn op de risico's die alle installaties en/of processen hebben op het milieu en op de leefomgeving. Er werden echter ook bepaalde zaken geïdentificeerd die een **verdere convergentie** vereisen ten gevolge van AI-systemen. De wetgeving inzake productnormen is bijvoorbeeld uitsluitend toegespitst op lichamelijke roerende zaken. Dit zou dus enkel op AI-systemen van toepassing zijn indien zij ingebed zijn in hardware.

Energie-efficiëntie mag niet ten koste van alles

Bij het gebruik van AI-systemen om een betere energie-efficiëntie te bekomen moet worden gezorgd dat alle andere rechten van gebruikers worden nageleefd, daarin begrepen hun recht op veiligheid en privacy. Een algemeen probleem dat ontstaat bij het toevertrouwen aan onderling met elkaar verbonden systemen is dat zij vatbaarder worden voor externe manipulatie.

Gebruik AI-systemen, sociale vaardigheden en arbeid

Vooral het consumentenrecht en de regels inzake verwerking van persoonsgegevens leggen informatieverplichtingen op aangaande de **impact die AI-systemen op ons sociaal leven** kunnen hebben. Inzake arbeid is er een beperkt **juridisch kader** dat niettemin voldoende de nood aan opleiding, overleg en veiligheid benadrukt. Toch moet blijvend worden geïnvesteerd in de nodige opleidingen/bijscholingen en het aanleren van de vereiste digital skills. Kortom, iedereen moet mee in het digitaliserings/AI-verhaal.

Ordehandhaving op het web

De werking van AI-systemen stopt niet aan de nationale grenzen. Dit kan voor problemen zorgen omdat de rechtsmacht van de overheden wel aan nationale grenzen stopt. Dit maakt het moeilijk om daders van strafbare gedragingen op het internet aan te pakken. Er moet daarom blijvend worden nagedacht over preventieve maatregelen (zoals bv. versterking van de filterverplichtingen van platformen en ondernemingen die informatie delen).

6.4. Welke tools kunnen worden gebruikt om aan de ethische vereiste te voldoen?

De reeds aangehaalde tools bij de andere ethische vereisten zijn relevant om betrouwbare AI te verzekeren. Daardoor wordt ook de maatschappelijke impact in rekening gebracht. Er zijn bovendien een aantal specifieke cursussen die helpen om maatschappelijke gewaarwording rond AI te verhogen. Voorbeelden zijn:

- Elements of AI
- Vlaamse AI cursus
- AI in business (Agoria)

Hoofdstuk 7: Ethische vereiste 7 - verantwoording

7. Ethisch Vereiste 7: Verantwoording

7.1. Wat betekent de ethische vereiste?

De vereiste van verantwoording vormt een aanvulling op de bovenstaande vereisten en is nauw verbonden aan het beginsel van rechtvaardigheid. Op grond van deze vereiste moeten mechanismen worden ingesteld om de **verantwoordelijkheid en verantwoording voor AI-systemen** en de resultaten daarvan te garanderen, zowel voor als na de toepassing. De nodige maatregelen moeten dus worden genomen om verantwoordelijkheid te verzekeren en aan te moedigen bij het ontwikkelen of gebruik van AI-systemen. Deze vereiste impliceert dat de potentiele risico's van AI-systemen op een transparante manier worden geïdentificeerd en gemitigeerd. Wanneer er sprake is van onrechtvaardige of nadelige gevolgen moeten toegankelijke verantwoordingsmechanismen bestaan die voorzien in een adequate verhaalsmogelijkheid. Het komt er dus eigenlijk op neer om te zorgen dat iemand verantwoordelijk kan worden gesteld indien AI-systemen schade veroorzaken en dat er een adequate schadeloosstelling wordt voorzien.

De ethische vereiste bestaat uit **twee sub-componenten** (1) controleerbaarheid en (2) risicobeheersing.

Controleerbaarheid houdt in dat het mogelijk wordt gemaakt om de algoritmen, gegevens en ontwerpprocessen te controleren. Dat betekent niet noodzakelijkerwijs dat informatie over bedrijfsmodellen en intellectuele eigendom in verband met het AI-systeem altijd openbaar beschikbaar moet zijn. Evaluatie door interne en externe actoren en de beschikbaarheid van dergelijke evaluatieverslagen kunnen bijdragen aan de betrouwbaarheid van de technologie. Bij toepassingen die een invloed hebben op grondrechten, met inbegrip van veiligheidskritieke toepassingen, moeten AI-systemen onafhankelijk kunnen worden gecontroleerd.

Risicobeheersing impliceert dat het vermogen om verslag te doen van handelingen of beslissingen die bijdragen aan een bepaald resultaat van het systeem, alsook het vermogen om op de gevolgen van een dergelijk resultaat te reageren, moet worden gewaarborgd. De vaststelling, beoordeling, verslaglegging en minimalisering van de potentiële negatieve effecten van AI-systemen is in het bijzonder cruciaal voor degenen die er (in)direct de gevolgen van ondervinden. Er moet gedegen bescherming beschikbaar zijn voor klokkenluiders, ngo's, vakverenigingen of andere entiteiten wanneer zij melding maken van legitieme zorgen over een op AI gebaseerd systeem. Wanneer zich een negatief effect voordoet, moeten toegankelijke mechanismen bestaan ter waarborging van geschikte beroepsmogelijkheden.

7.2. Welke regels zijn een uitdrukking van de ethische vereiste of kunnen dienen als inspiratiebron?

De ALTAI lijst voorziet per aangehaald sub-component verschillende vragen. We geven hieronder een overzicht van de (gebundelde) vragen per sub-component met een overzicht van relevante wetgeving of wetgeving die als inspiratie kan dienen bij de ontwikkeling en het gebruik van AI-systemen.

7.2.A. Controleerbaarheid

Werden de nodige maatregelen genomen die de controleerbaarheid van het AI-systeem verzekeren/vereenvoudigen (zoals de traceerbaarheid van het ontwikkelingsproces, de herkomst/bron van de gebruikte trainingsdata en de logging van de processen, uitkomsten en negatieve of positieve impact van het AI-systeem).

ALGEMEEN

Deze vereiste moet samen worden gelezen met de bespreking van de "Hoofdstuk 4: Ethische vereiste 4 - transparantie". Ook **contractuele afspraken** tussen de betrokken actoren zijn aangewezen om de nodige waarborgen rond controleerbaarheid te voorzien.

GEGEVENSBESCHERMING

Er zijn verschillende bepalingen in de **AVG** die elders al aan bod kwamen rond transparantie (art. 12 en 13-14) en het recht van inzage voor de betrokkene (art. 15). Ook de verplichting voor de verwerkingsverantwoordelijke om een register van de verwerkingsactiviteiten bij te houden met o.a. een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen indien mogelijk (art. 30) kwam eerder al aan bod. Ook moet elke organisatie die persoonsgegevens verwerkt nagaan of daar risico's aan verbonden zijn. Indien een organisatie vermoedt dat een AI-systeem naar alle waarschijnlijkheid een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen moet zij een GEB uitvoeren.

CONSUMENTENBESCHERMING

Ook de **informatieplichten** in Richtlijn 2011/83 over consumentenrechten kwamen reeds ter sprake en zijn in dit verband eveneens relevant. Er moet onder andere worden aangegeven of er een mogelijkheid is van toegang tot buitengerechtelijke klachten- en geschilbeslechtingsprocedures waaraan de handelaar is onderworpen (art. 6 en art. VI.45 WER).

Het invoeren van **adequate logging procedures** zal in de toekomst vermoedelijk aan belang winnen bijvoorbeeld binnen aangepast wetgevende kader rond aansprakelijkheid en AI-systemen.

Binnen het **WER** zijn een aantal bepalingen te vinden die relevant zijn die de controleerbaarheid van

het AI-systeem verzekeren/vereenvoudigen. De producenten bijvoorbeeld geven binnen het bestek van hun activiteiten de gebruiker de informatie die hem in staat stelt zich een **oordeel te vormen over de aan een product inherente risico's** gedurende de normale of redelijkerwijs te verwachten gebruiksduur, indien deze risico's zonder passende waarschuwing niet onmiddellijk herkenbaar zijn, en zich tegen deze risico's te beschermen. De producenten nemen binnen het bestek van hun activiteiten, maatregelen die zijn afgestemd op de kenmerken van de door hen geleverde producten en diensten om 1) op de hoogte te kunnen blijven van de risico's van deze producten en diensten en 2) de passende acties te kunnen ondernemen om deze risico's te voorkomen, waaronder het uit de handel nemen, het aangepast en doeltreffend waarschuwen van de gebruikers en het terugroepen (art. IX. 8).

De producenten en distributeurs moeten ook het **Centraal Meldpunt voor Producten** onmiddellijk in kennis stellen wanneer zij weten, of op grond van de hun ter beschikking staande gegevens beroepshalve behoren te weten, dat een product of dienst die door hen op de markt werd gebracht voor de gebruiker risico's met zich meebrengt die onverenigbaar zijn met de algemene veiligheidsverplichting (Art. IX.8. § 4 WER). Zij moeten daarbij bepaalde informatie geven (bv. gegevens waardoor het product exact kan worden geïdentificeerd en alle beschikbare informatie aan de hand waarvan het product kan worden getraceerd).

Daarnaast is ook tal van **sectorale regelgeving** relevant waarin maatregelen worden opgelegd die de controleerbaarheid van producten die gebruik maken van AI verzekeren/vereenvoudigen, zoals bv. technische documentatie. Denk aan de Verordening Medische Hulpmiddelen (art. 10.4, 10.5, 10.9 en 10.13). Ook de regelgeving rond machines stelt dat de fabrikant alvorens een machine in de handel te brengen en/of in bedrijf te stellen zich ervan moet vergewissen dat het technisch dossier beschikbaar is (art. 7). Ook onder de NIS-wet moeten technische en organisatorische beveiligingsmaatregelen worden genomen die incidenten kunnen vermijden of hun impact kunnen beperken (art. 20-23).

	Werd voorzien dat het AI-systeem kan worden onderworpen aan audits en externe controles door onafhankelijke derden?

De **certificering** van AI-systemen werd in tal van beleidsdocumenten reeds onderstreept. Stemmen gaan bijvoorbeeld op om AI-systemen met een hoog risico te onderwerpen aan een verplichte certificering. Een vrijwillige certificering wordt ook vooropgesteld als een optie voor de regulering van AI.

Toch bestaan er al heel wat andere mogelijkheden om labels te verkrijgen.

- De **CE-markering** bijvoorbeeld geeft aan dat een product volgens de fabrikant aan alle EU-eisen voldoet qua veiligheid, gezondheid en milieubescherming. De markering is verplicht voor bepaalde categorieën producten die in de EU verkocht worden, ook als ze elders gemaakt zijn. De CE-markering is alleen verplicht voor producten waarvoor EU-specificaties bestaan en die specificaties

bovendien bepalen dat de betrokken producten van een CE-markering moeten zijn voorzien. Voor sommige producten moet een onafhankelijke aangemelde instantie worden betrokken die nagaat of een product conform is en dus een CE label kan krijgen. Dit is terug te vinden in regels per productcategorie. Als een product niet door een onafhankelijke instantie gecontroleerd moet worden, is het aan de producent om te controleren of het aan alle technische eisen voldoet. Dit houdt in dat de mogelijke gebruiksrisico's van het product worden ingeschat en gedocumenteerd.

- **Sectorale bepalingen** spelen een belangrijke rol om na te gaan of certificering of een andere conformiteitbeoordeling nodig is (zie bv. art. 52-60 Verordening Medische Hulpmiddelen).

7.2.B. Risicobeheersing

Werd voorzien in enige vorm van externe begeleiding of audits door derden om toezicht te houden op ethische kwesties en verantwoordingsmaatregelen?

Werden risicotrainingen georganiseerd en zo ja, werd dan ook informatie over het mogelijke wettelijke kader dat van toepassing is op AI-systemen gegeven?

Werd overwogen om een AI ethics review board of een soortgelijk mechanisme op te richten om de algemene verantwoordings- en ethische praktijken te bespreken?

Werden de nodige mechanismes en processen voorzien om de conformiteit van AI-systemen met de vereisten van ALTAI lijst te verzekeren, op te volgen en te bespreken?

ALGEMEEN

De bedoeling is om de ethische aspecten van AI bij het ontwerp, de ontwikkeling en het gebruik **in kaart te brengen**. Op die manier kunnen betrouwbare AI-systemen worden ontwikkeld.

Hier is momenteel nog niet veel wetgeving over te vinden, net omdat het concept ethiek en de 'juridische vertaling' ervan niet altijd eenvoudig is. Wel is onder de toepasselijke regelgeving soms vereist dat actoren een risicoanalyse uitvoeren die in een AI-context kan worden gebruikt als vertrekpunt en inspiratiebron. Denk bijvoorbeeld aan de verplichting onder de **AVG** om een GEB uit te voeren indien een organisatie vermoedt dat een AI-systeem naar alle waarschijnlijkheid een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

SECTORALE WETGEVING

Ook in **sectorale wetgeving** kan inspiratie worden gevonden, bijvoorbeeld in de Verordening Medische Hulpmiddelen door middel van het kwaliteitsmanagementsysteem (art. 10). Het systeem omvat alle delen en onderdelen van de organisatie van de fabrikant die over de kwaliteit van de processen, procedures en hulpmiddelen gaan. Het regelt de structuur, verantwoordelijkheden, procedures, processen en managementmiddelen vereist voor de toepassing van de beginselen en maatregelen die nodig zijn om de bepalingen van de Verordening te kunnen naleven.

Ook de regeling rond productveiligheid in het WER bevat een aantal relevante bepalingen over het nemen van de nodige maatregelen om op de hoogte te kunnen blijven van de risico's van producten en diensten en om de passende acties te kunnen ondernemen om deze risico's te voorkomen.

Werden er een processen/maatregelen geïmplementeerd ten aanzien van derde partijen (zoals leveranciers, verdelers, gebruikers) om potentiële kwetsbaarheden, risico's of vooroordelen in het AI-systeem te melden?

ALGEMEEN

Contractuele afspraken en de **Wet van 4 april 2019** zijn relevant voor deze waarborgen.

GEGEVENSBESCHERMING

De betrokkene heeft onder de **AVG** **verschillende mogelijkheden** om deze zaken te melden. Denk aan het recht op rectificatie van onjuiste gegevens en het recht om vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door een aanvullende verklaring te verstrekken (art. 16 AVG). De betrokkene heeft ook het recht op gegevenswissing (art. 17 AVG). Onder bepaalde omstandigheden heeft de betrokkene ook het recht om van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen (art. 18). De betrokkene heeft ook een recht van bezwaar tegen de verwerking van persoonsgegevens, met inbegrip van en geautomatiseerde individuele besluitvorming van profilering (art 21). De betrokkene heeft 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 anderszins in aanmerkelijke mate treft (art. 22).

CONSUMENTENBESCHERMING

Daarnaast zijn er ook verschillende relevante bepalingen te vinden in consumentenwetgeving. Zo voorziet art. VI.47 **WER** op basis van de Richtlijn Consumentenbescherming in een herroepingsrecht van 14 dagen. Alvorens een consument verbonden is door een overeenkomst moet de handelaar op een duidelijke en begrijpelijke wijze ook informatie verstrekken over o.a. de toegang tot buitengerechtelijke klachten- en geschilbeslechtingsprocedures waaraan de handelaar is onderworpen, en de wijze waarop daar toegang toe is (art. VI.45 WER).

Ook art. 1649ter-1649sexies BW voorzien op basis van de Richtlijn betreffende bepaalde aspecten van de verkoop van en de garanties voor consumptiegoederen een recht van verhaal voor de consument, alsook andere rechten bij een conformiteitsgebrek. Er zijn ook een aantal remedies voorzien voor consumenten in Richtlijn over digitale inhoud en Richtlijn verkoop van goederen in geval van leveringsverzuim of conformiteitsgebrek.

INDIENEN KLACHTEN

Ook bij overheden kunnen in bepaalde gevallen klachten worden ingediend, denk bijvoorbeeld aan melding van **incidenten met medische hulpmiddelen bij FAGG**. Verder kan ook bij het **Meldpunt** een klacht worden ingediend bij misleiding, bedrog, fraude en oplichting. Onder de productveiligheid bepalingen in het WER stellen producenten en distributeurs het **Centraal Meldpunt voor Producten** onmiddellijk in kennis wanneer zij weten, of op grond van de hun ter beschikking staande gegevens beroepshalve behoren te weten, dat een product of dienst voor de gebruiker risico's met zich meebrengt die onverenigbaar zijn met de algemene veiligheidsverplichting (art. IX.8). Ook onder de **NIS-wet** wordt een mogelijkheid voorzien om melding van incidenten te maken (art. 24-31).

SECTORALE WETGEVING

Ook in sectorale wetgeving kunnen de nodige processen/maatregelen worden geïmplementeerd of zijn ze voorzien. Denk bijvoorbeeld aan de **post-market surveillance verplichtingen** voor fabrikanten van medische hulpmiddelen. Het plan voor post-market surveillance moet bepalingen bevatten over o.a. het verzamelen en aanwenden van de beschikbare informatie, met inbegrip van feedback en klachten van gebruikers, distributeurs en importeurs.

Zijn er verhaalmogelijkheden en/of opties voor het bekomen van compensatie indien AI-systemen individuen negatief beïnvloeden (en schade veroorzaken)?

ALGEMEEN

De kans dat AI-systemen schade veroorzaken is reëel. Denk bijvoorbeeld aan ongevallen veroorzaakt door autonome motorvoertuigen of een robot die lichamelijke schade veroorzaakt tijdens een chirurgische ingreep. Er zijn **verschillende mogelijkheden** waardoor slachtoffers hun schade kunnen verhalen.

CONTRACTUELE EN BUITENCONTRACTUELE REGIMES

Er kan **contractueel** al het één en andere worden opgenomen. Denk bijvoorbeeld aan een contractuele schadevergoeding of de ontbinding van de overeenkomst bij wanprestatie.

Naast contractuele aansprakelijkheid kan een slachtoffer ook een vordering indienen op grond van een **buitencontractuele aansprakelijkheidsregimes**. Denk aan de foutaansprakelijkheid van een AI producent of software ontwikkelaar (art. 1382 BW) of aansprakelijkheid van de bewaarder van een gebrekkige zaak (art. 1384 BW).

Ook de **regelgeving rond productaansprakelijkheid** is van belang. Volgende deze wet is een producent aansprakelijk voor de schade veroorzaakt door een gebrek in zijn product.

CONSUMENTENBESCHERMING

Het **herroepingsrecht** voor consumenten en de beschikbare remedies/rechten ingeval van een leveringsverzuim of conformiteitsgebrek werden reeds aangehaald.

Ook de Richtlijn over oneerlijke handelspraktijken en de relevante bepalingen in het WER voorzien in **verhaalmogelijkheden**. Oneerlijke handelspraktijken van ondernemingen jegens consumenten zijn verboden. De lidstaten moeten zorgen voor de invoering van passende en doeltreffende middelen ter bestrijding van oneerlijke handelspraktijken, zodat de naleving van de Richtlijn in het belang van de consumenten kan worden afgedwongen (art. 11).

Onlangs werd ook Richtlijn 2019/2161 betreft **betere handhaving en modernisering van de regels voor consumentenbescherming** aangenomen. Lidstaten moeten ervoor zorgen dat er remedies beschikbaar zijn voor consumenten die door oneerlijke handelspraktijken schade hebben geleden om op die manier alle gevolgen van die oneerlijke handelspraktijken teniet te doen. De consument moet toegang hebben tot schadevergoeding en, in voorkomend geval, prijsvermindering of beëindiging van de overeenkomst op een manier die evenredig en doeltreffend is.

Bedrijven kunnen zich beroepen op de bepalingen in het WER over **misleidende en vergelijkende reclame** (art. VI.17 en verder) die gebaseerd zijn op Richtlijn 2006/114 inzake misleidende reclame en vergelijkende reclame. De bedoeling is om beroepsbeoefenaars te beschermen tegen misleidende reclame door andere bedrijven die wordt beschouwd als een oneerlijke handelspraktijk. Volgens de Richtlijn moeten de lidstaten zorgen voor de invoering van passende en doeltreffende middelen ter bestrijding van misleidende reclame en voor de naleving van de bepalingen inzake vergelijkende reclame in het belang van handelaren en concurrenten (art. 5). Verder kan ook de **Belgische B2B wet van april 2019** met betrekking tot misbruiken van economische afhankelijkheid, onrechtmatige bedingen en oneerlijke marktpraktijken tussen ondernemingen worden gebruikt. Indien de rechten als consument of onderneming niet werden gerespecteerd, of indien iemand het slachtoffer is van misleiding, bedrog, fraude of oplichting, kan een procedure worden ingesteld bij het **Meldpunt**.

GERECHTELIJK WETBOEK

Juridische procedures kunnen worden ingesteld conform de bepalingen van het **Gerechtelijk Wetboek**. De rechtsvordering kan evenwel niet worden toegelaten indien de eiser geen hoedanigheid en geen belang heeft om ze in te dienen. De **bewijslast** voor schade veroorzaakt door AI-systemen kan zwaar zijn (bv. 'gebrekkige' AI).

ALTERNATIEVE GESCHILLENPROCEDURES

Daarnaast zijn ook **alternatieve geschillenprocedures** zoals arbitrage of bemiddeling soms mogelijk. Het Europese platform voor onlinegeschillenbeslechting (ODR) wordt door de Europese Commissie beschikbaar gesteld om online winkelen veiliger en eerlijker te maken door toegang te bieden tot goede

instrumenten voor geschillenbeslechting. Op EU niveau werd onlangs ook een voorstel aangenomen voor een Richtlijn betreffende representatieve vorderingen ter bescherming van de collectieve belangen van consumenten en tot intrekking van Richtlijn 2009/22/EG.

RECHTSVORDERING COLLECTIEF HERSTEL

In dit verband is ook de **regelgeving over de rechtsvordering tot collectief herstel** relevant. Een rechtsvordering tot collectief herstel is ontvankelijk indien aan verschillende voorwaarden is voldaan. De ingeroepen oorzaak betreft bijvoorbeeld een mogelijke inbreuk door de onderneming op een van haar contractuele verplichtingen, op een van de Europese verordeningen of de wetten bedoeld in art. XVII. 37 WER of op een van hun uitvoeringsbesluiten. Er zijn ook een aantal vereisten voor de verzoeker en het beroep op een rechtsvordering tot collectief herstel moet meer doelmatig lijken dan een rechtsvordering van gemeen recht. De mogelijkheid om een vordering tot collectief herstel in te stellen werd ondertussen ook voorzien voor KMO's.

SECTORALE BEPALINGEN

Ook in bepaalde (sectorale) wetgeving worden soms **verhaalmogelijkheden** voorzien. Onder de voorwaarden in de **AVG** heeft de betrokkene te allen tijde het recht om vanwege met zijn specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van persoonsgegevens (art. 21). Bovendien voorziet de AVG in een specifiek aansprakelijkheidsregime (art. 82).

7.3. Waar zitten mogelijke punten van verbetering/ aandachtspunten?

Bewijsproblemen identificeren en (desgevallend) remediëren

De analyse toont aan dat er al **heel wat verhaalmogelijkheden** beschikbaar zijn wanneer schade wordt veroorzaakt door AI-systemen. Het probleem zal echter liggen in het aantonen van constitutieve elementen van de vordering. Het is daarom nuttig om het **bewijsrecht** in een AI-context verder te onderzoeken. Op die manier kan worden nagegaan of het aangepast is aan de realiteit van AI en het slachtoffer in geen geval in de kou blijft staan.

Een tweede luik dat hier ook bij komt kijken is **digitale geletterdheid**. De vraag is of het slachtoffer in staat om problemen effectief als problemen te identificeren en in staat om bewijs te verzamelen. Bij gepersonaliseerde diensten erkennen we het probleem van de zogenaamde filter bubble. Mensen zijn zich niet bewust van de personalisatie die zij ondergaan en of deze verschilt voor andere mensen. De vraag is dus of een negatieve beïnvloeding wel herkend kan worden.

Ethisch AI-kader concretiseren

Er moet worden nagedacht over **concrete maatregelen rond een ethisch kader** voor AI in Vlaanderen. Beleidsmakers in Europa bevinden zich op dit moment nog vaak op een abstract niveau van principes en de vraag om nieuwe wetgeving te overwegen. Deze initiatieven zijn te abstract om ingang te vinden in de huidige innovatie en ontwikkeling met betrekking tot AI in Europa (of Vlaanderen). Concrete maatregelen zijn dus nodig zoals bv. het aanstellen van een Chief AI Ethics Officer in een bedrijf dat AI-systemen ontwikkelt. Een aantal vragen zijn hierbij o.a. over welke skills deze persoon moet beschikken en wat het functieprofiel van een dergelijke officer moet zijn.

Bij het creëren van een ethisch kader bestaande uit concrete maatregelen of zelfs wetgeving stellen wij alvast voor om dit kader te beschermen tegen checkbox ticking, een negatieve tendens bij persoonlijke gegevensbescherming die we reeds bij privacy en databeheer noteerden.

Een andere mogelijkheid is bv. dat AI- en data-innovatietrajecten die gesteund worden met overheidsgeld ethische aspecten met betrekking tot innovatie mee moeten nemen als selectie- of ontvankelijkheidscriterium. Ethische assessments kosten tijd en middelen. Daarom moeten deze niet mee worden genomen nemen als aparte hoofding in een projectvoorstel, maar als een verplicht werkpakket. Wat er in dit werkpakket moet komen kan besproken worden met de verschillende subsidieorganen, beleidsmakers, NGO's die de rechten van ALTAI uitdragen en het Kenniscentrum Data & Maatschappij.

Verder kan ook worden nagedacht over een soort van gedragscode voor AI, waarbij het te verwachten gedrag van AI-ontwikkelaars, organisaties en producenten kan worden omschreven. Daarnaast kan ook worden bepaald welke maatregelen nodig zijn om de controleerbaarheid van het AI-systeem te verzekeren/vereenvoudigen, alsook mogelijke processen/maatregelen die kunnen worden aangenomen om potentiële kwetsbaarheden, risico's of vooroordelen in het AI-systeem te melden. Dit systeem werkt reeds voor andere ontwikkelaars in software en sociale media. Een deontologie installeert een soort van erecode en ontwikkelaars durven praktijken van zichzelf en anderen in vraag stellen van zodra een gedeelde code beschikbaar is. De vele ingenieursprotesten bij Google en Facebook zijn hier voorbeelden van.

Inzetten op certificering

Certificeringsmechanismes voor betrouwbare AI kunnen in de toekomst een belangrijke rol spelen. Hier moeten beleidsmakers verder op inzetten om zo een kader rond certificering verder uit te stippelen. Een multidisciplinair platform opzetten met andere actoren lijkt alvast aangewezen (cf. ETAMI). Bij certificering raden wij aan om certificatie steeds voorbij het machine learning proces en model te ontwikkelen.

De ALTAI-vragen richten zich vaak naar een gebruiker en de context waarin AI wordt gebruikt. Een certificering die dit laatste proces niet in kaart brengt, zal onvoldoende zekerheden verschaffen.

Verspreiden van kennis

Het **verspreiden van kennis** is opnieuw cruciaal. Het blijft nodig om workshops te organiseren waarbij informatie wordt verstrekt over het wettelijke kader dat van toepassing is op AI-systemen (cf. educate your leaders). Verder kan ook verduidelijking worden gebracht bij de toepasselijke wetgeving, vooral met betrekking tot AI op zichzelf (dus niet embedded). Denk aan de vraag of software een product is of wanneer software gebrekkig is. Ook kan het ontwerpen van een contractuele template in de context van AI en standaardbepalingen over de verdeling van aansprakelijkheid/verantwoordelijkheid nuttig zijn in de AI supply chain.

7.4. Welke tools kunnen worden gebruikt om aan de ethische vereiste te voldoen?

- Data Ethics Guide wil de problematiek rondom ethiek belichten en behapbaar maken voor bedrijven die werken met AI-technologie. Verschillende concepten worden geïntroduceerd over hoe ethiek binnen een bedrijf kan worden onderzocht. Dit wordt gedaan door middel van vragen die helpen bepalen wat de huidige ethische situatie is.
- AI systems Ethics Self-Assessment Tool
- Principles for Accountable Algorithms en Social Impact Statement for Algorithms
- Data Ethics Decision Aid (DEDA)
- SDoC of Supplier's Declarations of Conformity
- Ethics framework van Machine Intelligence Garage
- Data Collection Bias Assessment formulier
- AI Explainability 360
- Ethical OS tool kit
- Data Ethics Canvas
- Artificiële Intelligentie Impact Assessment
- Aequitas
- Building an Algorithm Tool

Hoofdstuk 8: Evaluatie

8. Evaluatie

Voor elke ethische vereiste werden al een aantal tekortkomingen geïdentificeerd en een aantal aanbevelingen gefromuleerd. In dit deel besluiten we dan ook met een korte evaluatie over de relatie tussen de ethische richtlijnen en het wetgevende kader. We gaan na waar er lacunes zitten met betrekking tot de 'vertaling' van ethische vereisten in het wetgevende kader. Kortom, we geven een overzicht van waar er voor beleidsmakers nog werk aan de winkel is en rond welke vereisten verder kan worden nagedacht. Een ding wordt meteen duidelijk: wie de ethische vereisten wil linken aan het wetgevende kader moet een heel brede kennis hebben van zo goed als alle rechtsdomeinen. In tijden van toenemende specialisatie, lijkt een all round juridische kennis dus zeker een voordeel te bieden met betrekking tot de ontwikkeling van betrouwbare AI-systemen. Bovendien vergen deze vereisten ook een soort van reflex en mentaliteit die niet steeds te vertalen valt in wetgeving (bv. milieu, maatschappelijk, duurzaamheid).

VEREISTE 1 (MENSELIJKE CONTROLE EN TOEZICHT)

Deze ethische vereiste weerklinkt reeds in vele en verscheidene wettelijke vereisten en het is daarom voornamelijk een kwestie van bestaande regels te verduidelijken en met elkaar in verband te brengen. Zo is huidige regelgeving nog niet voorzien op systemen die kunnen 'leren' of door de ontwerper/gebruiker onvoorziene handelingen kunnen stellen. Het is daarom aan te raden om (i) eventueel relevante wettelijke vereisten of technische standaarden aan te passen/aan te vullen zodat ze met dit autonome karakter van AI-systemen rekening kunnen houden en (ii) na te kijken in welke mate het toepassingsgebied van bepaalde wetgeving zou moeten worden aangepast. Anderzijds betreft dit vereiste juridisch minder aflijnbare onderwerpen als 'afhankelijkheid' en 'aanhankelijkheid' die (nog) geen weerklank vinden in het huidige recht. Vraag is hier of, en in welke mate, de (Europese of Belgische) wetgever kan of moet optreden om dergelijke concepten in wettelijke vereisten om te zetten en dit niet alleen voor AI-systemen, maar ook voor andere producten.

VEREISTE 2 (TECHNISCHE ROBUUSTHEID EN VEILIGHEID)

Op het vlak van technische robuustheid en veiligheid bestaan er al meerdere uitgewerkte juridische kaders die verplichten om een adequate beveiliging te voorzien. De digitalisering – en bij uitstek het toenemend gebruik van AI-systemen – stellen deze regels op meerdere vlakken op de proef. Veel bestaande regelgeving is gericht op lichamelijke producten (bv. productveiligheid en productaansprakelijkheid). Het cyberveiligheidsregime is vooral gericht op het verhinderen van aanvallen door hackers. Bijkomend interdisciplinaire samenwerking lijkt dan ook nodig om na te gaan of en hoe deze wetgeving en/of regulering moet worden verfijnd in een AI-context.

VEREISTE 3 (PRIVACY EN DATABEHEER)

Op het vlak van privacy en databeheer bestaat er al een uitgewerkt wetgevend kader vanuit het

gegevensbeschermingsrecht. Niettemin blijkt de effectieve en nuttige toepassing hiervan vaak tot problemen te leiden en is het moeilijk om in de praktijk tot een werkbare privacy-cultuur te komen. Dit kan vermoedelijk worden opgelost door een betere bewustmaking en een duidelijker toelichting van de impact en toepassing van het gegevensbeschermingsrecht in AI-context. Ook een betere handhaving lijkt daarvoor onvermijdelijk. Problematisch is dat enkel verwerkers en verwerkingsverantwoordelijken onderworpen zijn aan de AVG en de ontwikkelaars en aanbieders strikt gezien niet gehouden zijn om hun (AI-)producten te laten voldoen aan bijv. de vereisten omtrent gegevensbescherming door ontwerp en standaardinstellingen. Regulerend initiatief hieromtrent kan maar nuttig zijn indien dat minstens op EU-niveau gebeurt.

VEREISTE 4 (TRANSPARANTIE)

Op het vlak van transparantie en informatieverplichtingen bestaat al heel wat regelgeving, zeker ten aanzien van consumenten. Bijkomende afzonderlijke wetgeving lijkt dus niet nodig, al kan de bestaande wetgeving (in de toekomst) op sommige vlakken licht worden aangepast en/of verduidelijkt. Met enkele kleine toevoegingen specifiek gericht op AI-systemen (bv. rond invoerdata en de werking van AI-systemen) kan al heel wat worden bereikt op vlak van conformiteit met de ALTAI lijst. Een alternatief is om op basis van die wetgeving bijkomende richtlijnen aan te nemen specifiek voor AI-systemen (cf. 'AI bijsluiter').

VEREISTE 5 (DIVERSITEIT, DISCRIMINATIE EN RECHTVAARDIGHEID)

Op het gebied van non-discriminatie is er al een omvattend kader. Toch lijkt het er op dat mogelijke nieuwe vormen van discriminatie niet onder de bestaande wetgeving zouden vallen. Daarom moet nagegaan worden of dit door een aanvulling op de bestaande wetgeving kan opgelost worden. Participatie van belanghebbenden in een AI-context is daarentegen nog niet voorzien in specifieke wetgeving. Een voorbeeld hiervan is wel al te vinden in de context van de AVG. Voor AI-systemen dient onderzocht te worden hoe een dergelijke regelgeving er uit zou kunnen zien.

VEREISTE 6 (MAATSCHAPPELIJK EN MILIEUBEWUSTZIJN)

Inzake milieubewustzijn is er al een omvangrijk lappendeken aan juridische kaders die zich toespitsen op specifieke risico's die kunnen worden veroorzaakt. Er zijn ook normen om de ontwikkeling van producten duurzamer te maken. Deze zijn vooral gericht op hardware. Het is nuttig om na te gaan of dergelijke vereisten ook zouden moeten gelden voor de ontwikkeling van software. Uit deze vereiste volgt ook dat de betrokken actoren voldoende moeten worden ingelicht over de impact op het milieu en de maatschappij bij het ontwikkelen en gebruik van AI-systemen. Ook wat betreft de impact van AI-systemen op democratische waarden lijkt het vooral een kwestie van bewustzijn. Inzake arbeid en sociale zaken is het noodzakelijk dat de bevolking met AI-systemen leert omgaan zonder daarbij evenwel te grote (administratieve) kosten op bedrijven te leggen. Er zijn reeds juridische mechanismen voorzien voor overleg en het verstrekken van informatie aan werknemers. Toch kan opnieuw meer aandacht worden gegeven aan specifieke opleidingsprogramma's, en zeker aan het ontwikkelen en behouden van

digitale vaardigheden om met AI-systemen om te gaan. Het voorzien van verdere beroepsopleidingen is dan ook cruciaal.

VEREISTE 7 (VERANTWOORDING)

Voor deze vereiste werden reeds een aantal aanknopingspunten gevonden in het bestaande recht. Indien schade veroorzaakt wordt door AI-systemen zijn er een aantal mogelijkheden voor slachtoffers om vergoeding te krijgen. Toch zijn bijkomende verfijningen aan het wetgevende kader nodig, bijvoorbeeld rond bepaalde juridische concepten (bv. kwalificatie software) of procedurele aspecten (bv. bewijslast slachtoffers).

Kenniscentrum
Data & Maatschappij

Kenniscentrum Data & Maatschappij
Pleinlaan 9
1050 Brussels

info@data-en-maatschappij.ai
www.data-en-maatschappij.ai