BITTERE NOODZAAK OF NOODZAKELIJK KWAAD?

AI aan regels gebonden

Meer AI willen toepassen en een weg vinden naar passende compliance daarbij: voor velen een lastig proces binnen een wirwar aan regels. De toekomstige Europese AI-Verordening gaat daarin voor een nieuwe dimensie zorgen, constateert Leonie Gerding.

door Leonie Gerding beeld Shutterstock

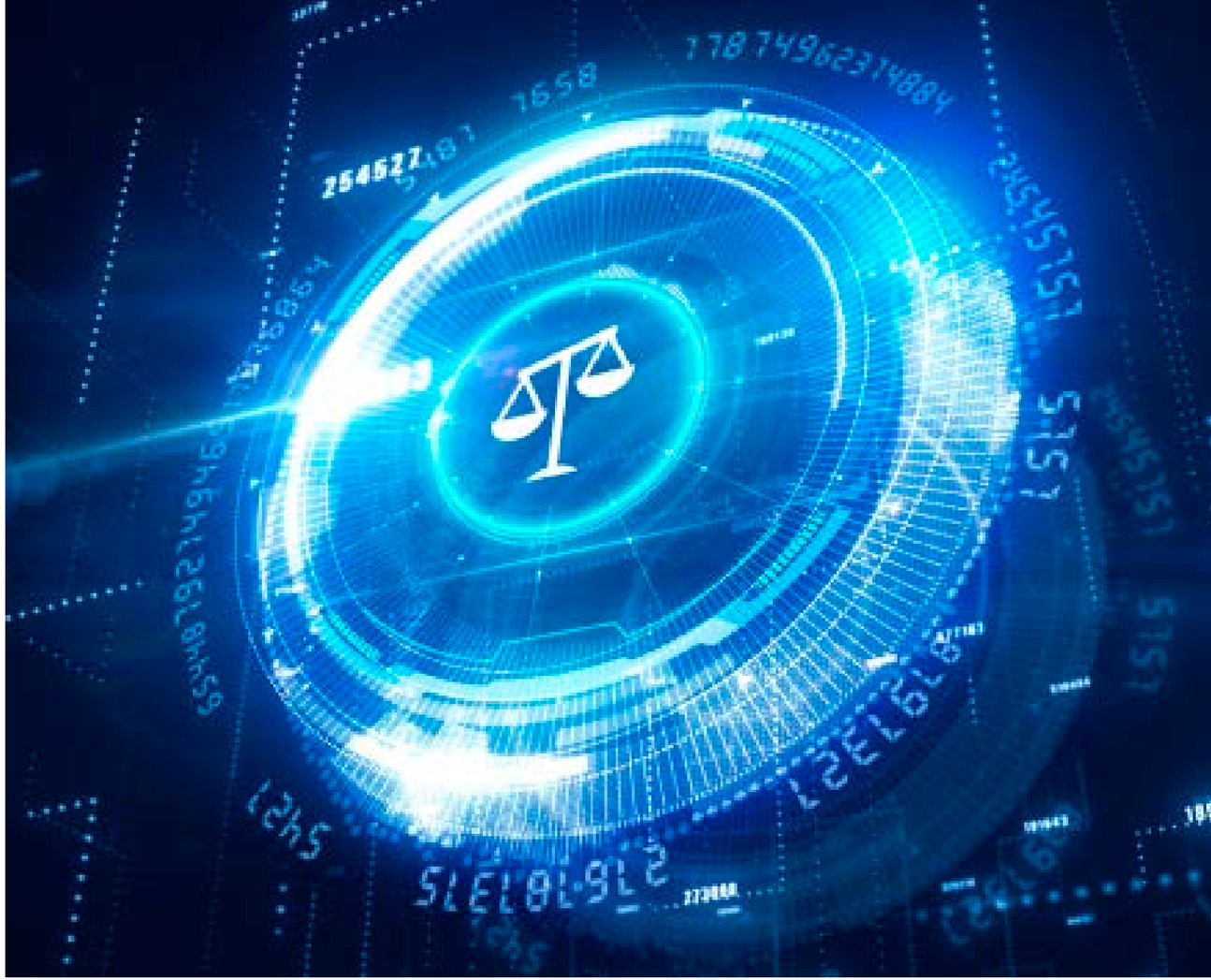
SOMMIGE TOEPASSINGEN VAN AI WORDEN DOOR DE VERORDENING VERBODEN. Voor andere toepassingen moet worden voldaan aan wettelijke verplichtingen, zowel in de techniek als op het niveau van de toepassende organisatie.
Wat levert meer AI-regelgeving ons op? Als jurist is het voor mij makkelijk om te zeggen: 'doe maar meer regels', want regels geven richting. Vanuit de business

De toeslagenaffaire leert: dit nooit weer

hoor ik vaak een ander geluid: regels belemmeren data-innovatie. Een ander niet te vergeten aspect binnen de discussie 'regels vs. innovatie' is de impact van AI op de maatschappij. Effecten op democratie, overheidsbeleid & bestuur, de vrijheden van mensen, maar ook de ongekende mogelijkheden die AI burgers kan bieden. Hoe kan je de vruchten plukken van AI-toepassingen en tegelijkertijd publieke waarden bewaken en toch ethische valkuilen voorkomen en onbedoelde neveneffecten vermijden? Maakt regelgeving daarin het verschil? Wil je als organisatie verantwoord je AI-innovatiestrategie bepalen, dan doe je er goed aan om inzicht te krijgen in het snel veranderende regelgevingslandschap rondom AI.

SLEUTELTECHNOLOGIE

De Europese Commissie (EC) en het kabinet zien AI als een sleuteltechnologie voor de toekomst: essentieel om maatschappelijke opgaven aan te pakken – van toekomstbestendige zorg tot duurzame energie – en essentieel voor de Nederlandse en Europese economie. Investeringen in AI kunnen het verschil



gaan maken in de positie van Nederland en de EU ten opzichte van de rest van de wereld. Tegelijkertijd erkennen de overheden ook dat AI-systemen maatschappelijke uitdagingen opleveren. Als je gebruik maakt van unieke lichaams- of gedragskenmerken en mensen in de openbare ruimte op afstand kunnen identificeren wordt de anonimiteit van burgers goeddeels opgeheven. Ook de toepassing van deepfakes en deepnudes baart veel zorgen, net als de groeiende mogelijkheden om mensen te profileren en te beïnvloeden. Hoe kan AI-regelgeving balans brengen tussen kansen en risico's?

NOODZAKELIJK KWAAD

De aankondiging van de AI-regelgeving heeft de kritiek losgemaakt dat de regelgeving de innovatie van AI zou kunnen afremmen en Europa zou kunnen belemmeren in zijn concurrentiestrijd met de VS en China om het leiderschap op het gebied van AI. Snelle technologische ontwikkeling van AI en een mondiale beleidscontext waarin landen fors in AI investeren; dat maakt dat de EU als één moet handelen. Alleen dan kan de EU haar kansen benutten en de uitdagingen van AI op een toekomstbestendige manier aanpakken. Uit onderzoeken is gebleken dat goed doordachte "harde

Vertaal normen in praktische stappen voor naleving

wetgeving" juist de innovatie daadwerkelijk kan bevorderen, vooral wanneer zij gepaard gaat met stimulansen die de invoering versnellen. De EC beoogt dit te doen door de AI-Verordening samen met het gecoördineerde AI-plan (zie kader) in te voeren.
Tegelijkertijd zorgen nog meer regels voor een remmende factor om AI-oplossingen toe te passen: wie heeft nog het overzicht over het reguleringslandschap? Gaat het om persoonsgegevens: AVG toepassen. Gaat het om zorginformatie: een heel scala aan wetgeving én de NEN7510 toepassen. Overheidsinformatie: WOB en WOO toepassen. Zo is er voor iedere sector een oerwoud aan regelgeving bij het gebruik van data. Ondanks dat ik goed begrijp dat het lastig is hier een rechtmatige weg door te banen, wil ik ervoor pleiten dat meer (en bovenal duidelijkere!) regels noodzakelijk zijn. AI-systemen kunnen leiden tot onnavolgbare besluiten en discriminerende uitkomsten, we moeten kunnen uitleggen hoe iets tot stand is gekomen wanneer AI is gebruikt. Dat dit lastig is, werd (pijnlijk) zichtbaar in een recente rechterlijke uitspraak met een hoog "computer-says-no-gehalte". De rechter bevestigde hierin een WOZ-waarde die als enige onderbouwing de uitkomst van een black box algoritme had, zonder dat kon worden uitgelegd waarop de uitkomst gebaseerd was. Als we begrip[1] hebben van welk effect AI heeft op onze samenleving, waarom en wat de gevolgen zijn, kunnen we beter uitleggen waarom regelgeving noodzakelijk is.

Meer en duidelijkere regels bittere noodzaak

De AI-Verordening richt zich op de verantwoordelijkheid die het gebruik van AI-systemen met zich meebrengt. Het bevat een verbod op AI-systemen met onaanvaardbare risico's en richtlijnen voor systemen met hoge risico's. De nieuwe wetgeving verplicht ontwikkelaars van AI-systemen om een systeem voor kwaliteitsbeheer van AI in te voeren dat voldoet aan eisen inzake hoge kwaliteit van gegevensverzamelingen, het bijhouden van registers, transparantie, menselijk toezicht, nauwkeurigheid, robuustheid en beveiliging. Aanbieders van AI-systemen die (nog) niet als risicovol zijn aangemerkt, worden aangemoedigd vrijwillige gedragscodes op te stellen om vergelijkbare doelen te bereiken. Regelgeving zou zelfs nog een stap verder kunnen gaan door onzekerheid over de tenuitvoerlegging van de Europese wetgeving verder te verminderen, bijvoorbeeld door de ontwikkeling van meer specifieke normen rond kwaliteitsbeheer en eerlijkheid en transparantie van AI. Hoe waardevol zou het zijn voor zowel de innovators als de samenleving wanneer een coalitie van aanbieders van AI-technologie en gebruikersorganisaties samen deze normen vertalen in praktische stappen voor naleving?

BALANS

In de AI-Verordening zie ik een balans terug tussen regulering en innovatie. Wanneer je naar een van beide kanten doorslaat zet je óf de bescherming van burgers aan de kant, óf je maakt elke vorm van innovatie onmogelijk. Voor de goede orde: besluiten van de overheid moeten altijd gemotiveerd worden, ook als hierbij een algoritme gebruikt wordt. De bittere noodzaak van meer regels voor het toepassen van AI wordt het duidelijkst door de toeslagenaffaire bij de Belastingdienst. Door een risicomodel te hanteren waarin o.a. nationaliteit een bepalende rol had, zijn duizenden ouders onterecht als fraudeur aangemerkt. Met ongekend grote gevolgen voor de levens van de slachtoffers.
Na het zien van de documentaire 'Alleen tegen de staat' houd ik als professional in het achterhoofd dat het mede mijn taak is dat zoiets nooit meer moet kunnen gebeuren en dat we daarvoor waarborgen moeten inbouwen.
Regels invoeren die verantwoording en transparantie eisen, binnen de gehele keten van AI-gebruikers, gaat daarbij zeker helpen. Het toepassen van AI, op welke manier dan ook, brengt een grote verantwoordelijkheid met zich mee voor de gebruiker ervan.

INGREDIËNTEN KWALITEITS-MANAGEMENTSYSTEEM

AI-regelgeving is er niet alleen voor de bescherming van burgers. Ook producenten en gebruikers van AI kunnen hun voordeel doen met nieuwe Verordening, zelfs al nu deze nog de conceptstatus heeft. De technische en organisatorische eisen die de Verordening aan hoog-risico toepassingen stelt, kunnen de ingrediënten zijn van het kwaliteitsmanagementsysteem op AI-toepassingen.
Als organisatie hoef je op een aantal terreinen niet zelf meer het wiel uit te vinden, maar kun je aansluiten bij de basis die de Verordening legt: specifieke eisen aan gebruikte data, het testen van de AI en het monitoren van een werkend systeem in productie. Begin direct al met het vastleggen van de uitgangspunten en gemaakte keuzes. Dan heb je een deel van je compliance al op orde en ben je goed bezig met je data ethiek. Kortom: door je vandaag al in deze eisen te verdiepen, sorteer je niet alleen voor op de wettelijk eisen van morgen, maar kun je ook nu al de AI-volwassenheid van je organisatie verbeteren.

[1] Zie bijvoorbeeld het initiatief van de Universiteit van Amsterdam: FMG Platform Citizens, Society and Artificial Intelligence (CiSAI)

VERORDENING EN 'GECOÖRDINEERD PLAN' EC

De Europese Commissie heeft een wetsvoorstel gedaan voor het harmoniseren van regelgeving voor 'het in de handel brengen, in gebruik stellen en gebruiken' van AI-systemen: de AI-Verordening. Om de ontwikkeling van AI te bevorderen en de potentiële grote risico's ervan voor de veiligheid en de grondrechten aan te pakken, heeft de Commissie naast nieuwe regelgeving ook het gecoördineerd plan inzake AI geactualiseerd. Samen moet dit de voorwaarden scheppen om de kansen die AI biedt te benutten, risico's te adresseren en tegelijk een Europese aanpak van AI te vergemakkelijken. In de AI-Verordening worden zowel regels gesteld ten aanzien van de techniek, als aan organisaties. AI-systemen worden in de volgende categorieën ingedeeld:

ONAANVAARDBAAR RISICO
Deze categorie bevat een aantal AI-systemen dat verboden wordt. Denk hierbij aan AI-systemen die mensen of groepen manipuleren of die 'social crediting' faciliteren.

HOOG RISICO
Deze categorie bevat AI-systemen die aanzienlijke risico's opleveren voor de gezondheid, veiligheid of grondrechten van personen. Hoog risico AI-systemen moeten voordat ze in de handel kunnen worden gebracht, worden onderworpen aan een beoordeling. Voor hoog risico AI-systemen gelden zowel technische als organisatorische verplichtingen waaraan moet worden voldaan. Deze verplichtingen worden opgelegd aan gebruikers en andere deelnemers aan de AI-waardeketen (bv. importeurs, distributeurs, gemachtigde vertegenwoordigers).

LAAG TOT MINIMAAL RISICO
Wanneer AI-systemen niet als een hoog risico worden beschouwd, moet er rekening worden gehouden met de mogelijkheid tot manipulatie. In die gevallen gelden er ook verplichtingen, zoals het informeren van mensen als ze interactie hebben met een AI-systeem of een AI-systeem hun emoties op automatische wijze herkent.

Naast verboden en verplichtingen voor AI-systemen en organisaties die ze toepassen, zorgt de AI-verordening ook voor handhavingsmogelijkheden. De handhaving is vergelijkbaar met die van de Algemene Verordening Gegevensbescherming: o.a. toezichthouders en hoge boetes worden in de AI-Verordening wettelijk vastgelegd. De AI-Verordening is nog in concept en moet het normale EU-wetgevingsproces nog doorlopen. Zicht op de daadwerkelijke datum van inwerkingtreding is er nog niet.

REACTIES EN BIJDRAGEN

Voor reacties en nieuwe bijdragen van IT-experts:
Tanja de Vrede
020-2356415
t.d.vrede@agconnect.nl

AUTEUR

LEONIE GERDING is expert op het gebied van privacy, ethiek en data & regulering. Ze adviseert organisaties bij complexe vraagstukken, de data en techniek die daarvoor nodig zijn en de geldende regels.