Algemene reactie op het "Reflectiedocument algoritmische besluitvorming en de Awb".

Algoritmen zijn zo oud als de prehistorie.
"Als ik een dier zie, dan (als het dier een bron van voedsel is, dan ga ik erop jagen, anders (als het een roofdier is, dan vlucht ik))."
Dit is een voorbeeld van een op regels gebaseerd algoritme dat alleen bestond in het hoofd van een oermens.

Sinds de IT-revolutie wordt veelvuldig gebruik gemaakt van geautomatiseerde algoritmen in computerprogramma's om complexe berekeningen uit te voeren. Deze algoritmen lijken weliswaar complex (het computerprogramma is voor de leek niet te volgen!), maar ze zijn altijd op regels gebaseerd, en daarmee dus te valideren en navolgbaar, zolang de invoer, de uitvoer en de rekenparameters bekend zijn.
Een voorbeeld hiervan is het gebruik van AERIUS voor stikstofdepositieberekeningen. Het rekenmodel gebruik vast gedefinieerde (reken)regels die openbaar toegankelijk zijn. De rekenmethoden SRM1 en SRM2 zijn beschreven in de RIVM-rapporten 2014-0127 en 2014-0109. De rekenmethode NNM is een Gaussisch pluimmodel, beschreven door het KNMI in 1974.
In het reflectiedocument is in paragraaf 7 onder het kopje "jurisprudentie" het bespreken van de AERIUS-uitspraak en de Blankenburg-uitspraak dus niet relevant. De rekenmethoden van AERIUS zijn namelijk volledig transparant en navolgbaar. Bovendien is het verstrekken van invoergegeven, rekenparameters en uitvoer (resultaten) een gebruikelijke eis bij berekeningen in het kader van vergunningen en projecten. De resultaten van berekeningen met het computerprogramma AERIUS zijn daarmee ook verifieerbaar.
Deze systematiek geldt vergelijkbaar voor geluidberekeningen, bijvoorbeeld met het computerprogramma Geomilieu.

Sinds (ongeveer) 2010 is sprake van de AI-revolutie. Computers worden steeds krachtiger, zowel wat betreft rekencapaciteit als opslagcapaciteit. Hieronder ga ik op deze twee aspecten in.

Rekencapaciteit
Complexe berekeningen die voorheen uren, dagen, weken, of zelfs jaren duurden, kunnen nu in een fractie van die tijdspanne worden uitgevoerd. De "eenvoudige" op regels gebaseerde algoritmes blijven desondanks precies hetzelfde doen. Een mogelijk probleem is wel, dat zo ontzettende veel berekeningen kunnen worden uitgevoerd, dat het volledig verifiëren van de resultaten (menselijke supervisie) onmogelijk is. Een beperkte steekproef zal in deze gevallen echter kunnen volstaan.

Opslagcapaciteit (in combinatie met rekencapaciteit)
De enorm toegenomen opslag- en rekencapaciteit leidt tot zelflerende algoritmes, die op basis van enorm veel berekeningen en enorm grote datasets zelf nieuwe regels kunnen genereren: machine learning en deep learning. Het probleem daarvan is dat het genereren van deze nieuwe regels vaak een black-box is, zodat de uiteindelijke resultaten van de berekeningen niet te verifiëren zijn. De oplossing daarvan ligt echter niet bij de machine, maar bij de mens!

Alle problemen met op AI-gebaseerde systemen zijn terug te voeren op menselijke (gedachten)fouten. Deze fouten komen voor in twee categorieën.

1. Selectie van de datasets.
De datasets die worden gebruikt zijn vaak niet representatief, niet onafhankelijk, niet getoetst of niet volledig (genoeg). Bij regelgeving voor het toepassen van AI moeten daarom naar mijn mening eisen worden gesteld aan de selectie van datasets, zodanig dat voldoende waarborgen voor burgers gegarandeerd zijn.

2. Keuze van rekenparameters
Bij ieder AI-systeem worden algoritmen gebruikt. Rekenregels, die in de basis door de mens zijn opgesteld. In de praktijk gaat het opstellen van die regels vaak mis. Door welke oorzaak dan ook zijn de regels dan discriminerend of in strijd met privacy. Op zich is dat niet bijzonder of verontrustend. In de prehistorie kon het ook al misgaan, als de oermens gedood werd door een dier dat hij als resultaat van zijn hoofd-algoritme als bron van voedsel had gezien. En ook in de huidige tijd zijn er vele voorbeelden van onjuiste uitgangspunten, parameters met een factor 10 verkeerd en rekenfouten, waarbij algoritmes leiden tot onjuiste of afwijkende resultaten.
Wat wél verontrustend is, is het feit dat (foutieve) parameters bij machine learning en deep learning door de grote hoeveelheden data en berekeningen vrijwel niet meer geverifieerd kunnen worden.
Bij regelgeving voor het toepassen van AI moeten daarom naar mijn mening eisen worden gesteld aan de keuze van parameters, zodanig dat voldoende waarborgen voor burgers gegarandeerd zijn.

Hopelijk leidt mijn bijdrage tot een een zorgvuldige en weloverwogen aanpassing van wetgeving, waarbij wel regels gaan gelden voor problemen die zich kunnen aandienen bij het gebruik van AI-systemen ten aanzien van navolgbaarheid en herleidbaarheid, maar niet voor eenvoudige algoritmes waarbij de regels duidelijk zijn en deze problemen bovendien niet te verwachten zijn.