Introductie

Laat ik beginnen met 2 verduidelijkingen.

1. Waarom zit ik hier?

In het dagelijks leven studeer ik aan de Universiteit Twente, waar ik me momenteel specialiseer in ethische en veilige digitalisatie binnen de (semi-)publieke sector; dat wil zeggen, hoe kunnen overheden nieuwe technologieën inzetten om niet alleen efficiënter, maar ook veiliger en privacybewuster te worden. Momenteel ben ik bijvoorbeeld bezig met mijn afstudeeronderzoek naar het afdwingen van voorspelbare systematische veiligheidsgaranties in onvoorspelbare systemen, zoals AI.

Dat alles is een zeer technische manier om te vertellen dat dit onderwerp mij nauw aan het hart ligt, en in de stukken die voorliggen zie ik vanuit mijn expertise dingen die simpelweg niet kloppen, onrealistisch zijn, of rusten op misvattingen over de technologie. Ik heb mijn best gedaan de rest van mijn bijdrage niet te technisch te maken, maar heb ook een uitgebreidere versie met technische toelichting en bronvermelding, die ik hier op papier heb maar ook achteraf via de griffie met jullie zal delen.

Daarnaast kennen jullie mij misschien als lid van de jongerenraad, of binnen een van mijn andere vrijwilligersfuncties binnen verenigingen in de gemeente. Alhoewel ik hier vandaag als mezelf zit, en niet spreek namens enige organisatie, maar ik me ook daarom zorgen over dit voorstel. De zaken die er in staan — en vooral ook de zaken die er niet in staan — gaan impact hebben op mij als inwoner en de organisaties waarbij ik betrokken ben. AI wordt gebruikt in de communicatie met mij, het beoordelen van mijn aanvragen, het opstellen van beleid wat impact op mij heeft, en het komt in aanraking met mijn gevoelige gegevens.

2. Ben ik tegen AI?

Nee. Integendeel zelf, ik denk dat het een technologie is die enorme kansen biedt, ook binnen de gemeente. Sterker nog, ik heb na het schrijven van een eerste versie van deze inspraak de voorliggende stukken als experiment door AI gehaald, met de vraag om de stukken te analyseren. Aan de hand daarvan heb ik zelfs nog enige wijzigingen doorgevoerd.

Uitwijding: gebruik van AI in deze inspraak

Eerst heb ik, als mens, de stukken doorgelezen, waar nodig extra onderzoek gedaan door bronnen als de Autoriteit Persoonsgegevens te raadplegen, en een eerste versie van mijn inspraak geschreven.

Na dit alles heb ik het raadsvoorstel, collegevoorstel, beleidskader en de vuistregels ingevoerd in Gemini 3.1 Pro Extended op Deep Research modus, met de volgende prompt:

“Beoordeel dit beleidskader en de gerelateerde stukken. Wees kritisch, maar realistisch. Wees uitgebreid, leg verbanden tussen verschillende secties, en behandel alle relevante onderwerpen. Besteed daarnaast speciale aandacht aan wat niet in deze stukken staat, maar wat er wel in zou moeten staan, of zaken die kort genoemd worden, maar waar uitwijding op ontbreekt. Waar relevant mag je concrete suggesties voor verbetering geven. Hou er wel rekening mee dat dit een beleidskader is.”

Vervolgens heb ik, in een nieuwe chat (= verse context), de stukken, mijn inspreektekst en de analyse van AI zelf ingevoerd in Gemini 3.1 Pro Extended op reguliere modus, met de volgende prompt:

“De gemeente Zutphen heeft een beleidskader opgesteld over AI. Ik ga over dit onderwerp inspreken bij de gemeenteraad. Hiervoor heb ik een inspraaktekst geschreven. Ook heb ik Gemini 3.1 Pro Extended op Deep Research mode een analyse van de stukken laten schrijven. Vergelijk deze met je de inspraak, en ligt toe waar de verschillen en overeenkomsten in zitten. Beoordeel ze ook inhoudelijk. Geef aan of en hoe de inspraak versterkt kan worden met punten uit de beoordeling, en of en hoe de beoordeling aangevuld kan worden aan de hand van de inspraaktekst.”

Op basis van dit en de analyse heb ik enkele wijzigingen en toevoegingen doorgevoerd in mijn inspreektekst. In de geschreven versie staan wijzigingen op basis van wat door AI is voorgesteld *cursief*. Hierbij heb ik suggesties van de AI niet woordelijk overgenomen, maar heb ik op basis van de suggesties zelf nog verder onderzoek gedaan, en wijzigingen in mijn eigen woorden en op basis van mijn eigen onderzoek opgeschreven.

Wel denk ik dat we realistisch en kritisch moeten blijven over wat het is: een inherent vrij complexe technologie die nog actief ontwikkeld wordt. Net als elke andere technologie brengt dit kansen, maar ook risico's, met zich mee. Bij AI zijn deze kansen en risico's minder duidelijk dan bij andere technologieën. Daar moeten we dus extra op letten.

Wat is het probleem?

1. Voor het beleidskader

In de inleiding van het raadsvoorstel staat het volgende:

"Parallel hieraan onderzoekt het team Informatiemanagement welke AI toepassingen voldoen aan wetgeving en dit AI beleidskader. Een belangrijk onderdeel daarvan is een chatbot voor de gehele gemeente die hetzelfde doet als bijvoorbeeld Chatgpt of copilot maar die we wel veilig kunnen inzetten en beheren. Als we dat hebben kunnen we de toegang tot de onveilige openbare chatbots zoals Chatgpt dicht zetten."

Dit betekent dat binnen de gemeente gebruik wordt gemaakt van openbare chatbots zoals ChatGPT en Microsoft Copilot, waarvan de gemeente erkent dat zij deze niet "veilig kunnen inzetten en beheren" en waarvan het onduidelijk is of deze voldoet aan de wetgeving. Ook lees ik hier dat er een overwogen keuze wordt gemaakt om de toegang hiertoe niet dicht te zetten totdat er een gemeentelijk alternatief is.

Ik heb aan de hand hiervan contact gehad met de gemeente, waarbij ik vragen heb gesteld over waarom deze keuze is gemaakt, maar ook aan welke kaders dit gebruik momenteel getoetst wordt, en of retroactief geëvalueerd wordt of er onveilig gebruik is gemaakt. Ook vroeg ik me af wat dit voor impact zou hebben op stukken en besluiten die in de afgelopen jaren zijn gemaakt, gezien die mogelijk dus mede of volledig door AI gemaakt zijn.

De gemeente heeft mij toen laten weten dat er momenteel geen kaders zijn, dat het gebruik van AI niet retroactief geëvalueerd zal worden, en dat er enkel vuistregels zijn vastgesteld over de risico's bij het gebruik van AI.

Daarnaast lees ik in het raadsvoorstel dat er in oktober een governance-richtlijn wordt opgesteld, en dat in november een leergang AI-geletterdheid voor ambtenaren wordt opgestart. Graag wijs ik jullie erop dat onder de AI-verordening (EU verordening 2024/1689) het sinds 2 februari 2025 verplicht is voor organisaties om ervoor te zorgen dat hun werknemers 'AI-geletterd' zijn als ze AI-systemen gebruiken. De Autoriteit Persoonsgegevens handhaaft hier sinds augustus op.

Dit wordt ook onderstreept in een enorm uitgebreid rapport van de VNG, de 'Uitvoeringsanalyse Digital Decade AI-verordening', gepubliceerd in januari 2025. In dit rapport van 76 pagina's gaan ze in detail in op de concrete stappen die gemeenten moeten zetten om veilig met AI om te gaan en te voldoen aan de AI-verordening. Hierin staat onder andere: "Op de korte termijn is het van belang dat gemeenten hun AI-systemen gaan inventariseren en de AI-geletterdheid gaan organiseren". De gemeente Zutphen lijkt met deze oproep niets te hebben gedaan.

De gemeente loopt dus niet alleen achter de feiten aan, en neemt niet alleen al 3.5 jaar risico's zonder verantwoordelijkheid hiervoor te nemen, maar overtreedt momenteel ook de wet, en volgt expliciete, concrete adviezen van de VNG niet op.

Daarom wil ik graag vragen aan het college: waarom hebben jullie ervoor gekozen om dit beleidskader nu pas op de agenda te plaatsen?

Uitwijding: waren er aanwijzingen dat dit eerder gedaan had kunnen/moeten worden?

AI is een technologie die al ontzettend lang bestaat. Generatieve AI (de versie die zaken 'genereert') begon een wereldwijde 'AI boom' met de release van ChatGPT eind 2022.[1]

Al snel waren er echter zorgen; de Autoriteit Persoonsgegevens maakte in juni 2023 al bekend dat er zorgen waren over de omgang van AI met persoonsgegevens binnen organisaties zoals gemeenten.[2]

In december 2023 vroegen ze organisaties expliciet om kritisch te kijken naar hoe ze AI gebruiken.[3]

In juli 2024 schreef de AP in haar Rapportage AI- & Algoritmerisico's Nederland[4] dat het vertrouwen in AI laag was, de risico's en kans op misbruik hoog, en er grote kans was voor privacyschendingen en discriminatie bij gebruik hiervan. Hun specifieke bevinding voor gemeentelijke organisaties was toen dat er maar beperkt zicht is op AI-systemen, raadsleden onvoldoende kennis hadden om de controle hierop te waarborgen, en dat er maar sporadisch onderzoek wordt gedaan naar de inzet van AI.

Op 1 augustus 2024 trad de Europese AI-verordening in werking. Daarmee werd het verplicht om risico's te inventariseren, AI-kennis op peil te brengen en actie te ondernemen.[5]

Diezelfde maand meldde de AP dat AI-chatbots leidden tot meer datalekken, ook als daar afspraken tegen gemaakt zijn. Zij adviseren daarom om niet alleen regels te verduidelijken, maar ook te kijken naar de supply chain en om te monitoren of de regels wel goed gevolgd worden.[6]

---

[1] https://doi.org/10.48550/arXiv.2402.05122
[2] https://autoriteitpersoonsgegevens.nl/actueel/ap-vraagt-om-opheldering-over-chatgpt
[3] https://autoriteitpersoonsgegevens.nl/actueel/blogpost-zorgen-om-generatieve-ai
[4] https://autoriteitpersoonsgegevens.nl/documenten/rapportage-ai-algoritmerisicos-nederland-ran-voorjaar-2024
[5] https://eur-lex.europa.eu/eli/reg/2024/1689/oj
[6] https://autoriteitpersoonsgegevens.nl/actueel/let-op-gebruik-ai-chatbot-kan-leiden-tot-datalekken

Waarschuwingen, adviezen en oproepen om kritisch te kijken naar AI-gebruik blijven maar komen. In december 2025 wordt duidelijk waarom; openbare chatbots zorgen voor een groot datalek bij de gemeente Eindhoven, waarbij duizenden bestanden met persoonsgegevens van inwoners gelekt worden.[7] Verwachting is dat zij bij verre na niet de enige zijn.

In oktober 2025 blijkt uit onderzoek uitgevoerd door Motivaction (ten behoeve van reclame voor Uniserver, dat wel), dat meer dan de helft (55%) van gemeentelijke ambtenaren AI-tools op eigen initiatief gebruikt, zonder formele richtlijnen, ondersteuning, beleid of regels. Bijna alle gemeenten (90%) erkennen dat dit grote kans heeft te leiden tot datalekken of gebrekkige veiligheid.[8]

2. Het beleidskader

In het beleidskader staan drie richtinggevende principes: ‘de mens eerst’, ‘betrouwbaar’ en ‘toekomstbestendig’. Laten dit nou net drie zaken zijn die AI niet is; het is fundamenteel geen mens, onbetrouwbaar, en ik zal de economische analyse over de AI-bubble achterwege laten, maar er zijn ook duidelijke aanwijzingen dat het in de huidige vorm niet toekomstbestendig is. Dit wijst mij direct op een misvatting van de onderliggende technologie, wat in de rest van het document bevestigd wordt.

Zo wordt bijvoorbeeld meermaals gezegd dat de beslissing bij de mens zelf moet blijven, maar je wel AI kan gebruiken om informatie op te zoeken, of als inspiratiebron. Maar laten we eerlijk zijn: **als de feiten op basis waarvan een ambtenaar een beslissing neemt, zijn samengesteld door een chatbot, wie neemt er dan feitelijk de beslissing?** Deze gang van zaken creëert enkel schijnveiligheid. De ‘menselijke maat’ wordt onzichtbaar gestuurd door een niet-controleerbaar algoritme.

[7] https://eindhoven.raadsinformatie.nl/document/16415812/1
[8] https://persportaal.anp.nl/artikel/ae4fd0a4-1639-4e21-9482-be6a35adfc35

Uitwijding: AI als beslisser of zoekmachine, en poisoning-the-well aanvallen

Twee citaten uit de stukken:

“Gebruik een AI-programma niet om een beslissing te nemen. Vraag bijvoorbeeld niet aan de AI-tool of iemand een boom mag kappen. Je kunt wel informatie opzoeken over bomen kappen met behulp van de AI-tool”

“Gebruik een AI-programma alléén als hulpmiddel en inspiratiebron. Bijvoorbeeld om informatie te verzamelen.”

Als op basis van informatie die door AI is opgezocht over of iemand een boom mag kappen de keuze wordt gemaakt, is de AI toch alsnog eigenlijk de beslissing aan het maken? Verder is dit een zeer risicovolle toepassing van AI; ChatGPT heeft geen rechtenstudie gedaan, kan je niet vertellen welke wetten hier van toepassing zijn, en kan zeker niet ingaan op de lokale, Zutphense, context.

Daarnaast is informatie verzamelen juist een van de grootste zwaktes van AI. Superversimpeld: AI werkt als een soort enorm geavanceerde autocomplete; hij kiest op basis van de tekst die de gebruiker invoert (de context) de meest probabilistische volgende woorden, zinnen en paragrafen. Nieuwere tools voegen daar allemaal snufjes aan toe, zoals het stapsgewijs iteratief opstellen van antwoorden, maar de technologie blijft fundamenteel hetzelfde. Bij het gebruik van AI is het daarom enorm belangrijk om zelf nieuwe context te blijven introduceren; anders blijft de AI maar door genereren op basis van datgene wat die zelf eerder gezegd heeft. AI helpt je dus ook alleen met dat waar je naar vraagt; niet met datgene waarvan je niet weet dat je ernaar moet vragen. Dat is waarom onderzoek door mensen en het raadplegen van experts zo belangrijk is.

Door AI op deze manier toe te passen, ben je als gemeente ook extra gevoelig voor een aanvalsstrategie waar de initiële context ‘vergiftigd’ wordt; dit kan gebeuren op heel subtiele, soms onzichtbare manieren. De output van de AI kan daarmee gevormd worden naar de zin van de aanvaller, en doordat er geen nieuwe context wordt geïntroduceerd blijft dit effect maar doorbouwen. Dit staat bekend als een ‘data poisoning’ of ‘poisoning the well’ aanval.[9,10,11]

[9] https://doi.org/10.48009/4_iis_2025_135
[10] https://doi.org/10.48550/arXiv.2202.10276
[11] https://doi.org/10.1007/s00146-024-01876-5

Ook is er een groot onderliggende probleem met het meest gebruikte tegenargument op dit alles: “een mens heeft het daarna nog gecontroleerd”. In het uitwijdingskader zal ik hier dieper op ingaan, maar de korte versie luidt als volgt: er zitten gigantische verschillen tussen een mens die iets schrijft en een mens die controleert wat een AI heeft geschreven. Door deze controle achteraf als gelijkwaardige optie toe te staan, zet je je ambtenaren op om een zeer menselijke fout te maken en hier de volledige verantwoordelijkheid voor te nemen. Hierbij negeer je wel bewezen feiten over hoe mensen psychologisch werken, creëer je enkel schijnveiligheid, en plaats je ambtenaren in de metaforische vuurlinie.

Uitwijding: controle en automation bias

Het klinkt logisch: wat maakt het uit of een ambtenaar iets heeft geschreven, of heeft gecontroleerd wat een AI heeft geschreven? In beide gevallen draagt de ambtenaar verantwoordelijkheid voor wat er in de tekst staat.

In de praktijk blijkt dat hier een wezenlijk verschil in zit, en dat heeft alles te maken met de ‘automation bias’. Dit is een academisch veelvuldig bewezen psychologisch effect (het heeft zelfs een Wikipedia-pagina[12]) waarbij mensen de neiging hebben om geautomatiseerde processen blindelings te vertrouwen.

Daar komt nog een effect bij dat je vast ook bij jezelf kan herkennen: als de werkdruk hoog oploopt en je wat krap in de tijd zit, word je slordiger. Je leest over details heen, scant teksten snel, maakt fouten die je normaal niet zou maken.

Deze twee effecten samen maken dat een controle achteraf van AI-werk vaak degradeert tot een snelle, onzorgvuldige scan, of zelfs een blind stempel.[13] Door controle achteraf toe te staan, wetende wat deze effecten en de hoge werkdruk op ambtenaren gaan veroorzaken, ben je ze effectief naar het hakblok aan het lopen, terwijl je je eigen controlerende functie in de voet schiet.

[12] https://en.wikipedia.org/wiki/Automation_bias
[13] https://doi.org/10.1007/s00146-025-02422-7

Verder zie ik weinig richtinggevende principes die het doel van transparantie ondersteunen. Transparantie is bij andere onderwerpen meermaals genoemd als kernwaarde van de gemeente Zutphen. Het gebrek aan transparantie wordt gelinkt aan het groeiende gebrek aan vertrouwen in de overheid, zowel lokaal als nationaal. Dit heeft de lokale context ook meermaals getoond (zie ook: dienstencentrum). Ik wil pleiten voor het belang van proactieve publieke transparantie over niet alleen dat, maar ook hoe AI is gebruikt. De motivatie hiervoor zit, weereens, verscholen in een uitwijdingskader.

Uitwijding: het belang van transparantie

Een begrijpelijke reflex is om te willen verbergen dat je AI hebt gebruikt om een stuk te (helpen) schrijven. Het gebruik van AI wordt veelal nog geassocieerd met luiheid, dat je zelf niet de moeite wil doen om het te schrijven. Ik ben hier niet immuun voor: ook ik voelde een sterke neiging om dit kader niet cursief te maken, om te doen alsof ik deze argumenten helemaal zelf had bedacht. Maar dat is niet zo, en er is een vrij goede reden om dit niet te verbergen.

Maar eerst, de wettelijke verplichting. Hier kan ik vrij kort over zijn: de AI-verordening stelt bepaalde transparantie-eisen. De juridische afdeling zal je beter kunnen informeren over welke hiervan voor de gemeente van toepassing zijn.

Daarbovenop wil ik echter nog stellen dat transparantie juist meer vertrouwen zal wekken. Door proactief open te zijn over hoe AI is gebruikt, toont de gemeente dat ze haar digitale transformatie zorgvuldig doet, en open is over hoe ze dat doet. Dit zal inwoners juist het gevoel geven dat je hen respecteert en niets te verbergen hebt.

Het tegenovergestelde is ook waar: als je verbergt dat er en hoe AI gebruikt is, of hier niet open over bent (wat effectief hetzelfde is), en dit wordt achteraf openbaar … ik denk dat iedereen kan inzien wat de schade daarvan zou zijn. Stel dat ik had gedaan alsof ik deze punten volledig zelf had bedacht, en je er daarna pas achter kwam dat deze door een AI waren bedacht. Je zou je, terecht, bedrogen voelen. Ik denk niet dat we willen dat onze inwoners zich bedrogen gaan voelen.

Als laatste vind ik het gebrek aan specifieke aandacht voor de cyberveiligheid van de toepassingen erg teleurstellend. Omwille van vooral

mijn eigen tijd laat ik een uitgebreide analyse van dit onderwerp achterwege, maar ik druk iedereen graag op het hart dat deze systemen in de praktijk vaak veel informatie verwerken en erg kwetsbaar zijn. Neem het gebruik van AI als grammatica- en spellingscontrole. Indien dit geautomatiseerd wordt toegepast op alle documenten, betekent dit ook dat deze AI toegang heeft tot ALLE documenten die de gemeente produceert. Sta stil bij de implicaties daarvan.

3. Na het beleidskader

Omwille van de tijd, en omdat het als inwoner niet mijn rol is om te bepalen wat wel en niet kan, zal ik hier niet al te diep op ingaan, maar globaal: een hoop zaken die in het beleidskader staan, zijn mijn inziens lastig of onuitvoerbaar, en ondermijnen de controlerende functie van de gemeenteraad.

Zo wordt er gesproken over het gebruik van data van hoge kwaliteit en het waarborgen van inclusieve modellen, wat momenteel in de AI-sector nog grote discussiepunten zijn waar nog geen oplossingen voor bestaan.

Daarnaast wordt beweerd dat “AI leert en verandert”. (Zijnoot: voor zover ik weet bestaat er nog geen enkele AI-toepassing die, terwijl het in gebruik is, zichzelf door blijft trainen.) Daarom “bevat het systeem feedbackloops van gebruikers, monitoring op bias en fouten, aanpasbaarheid van modellen en worden governance en escalatiepaden mogelijk gemaakt.” Dit klinkt op papier heel mooi, maar in de praktijk verwacht ik dat dit lastig tot niet bereikbaar zal zijn.

Als laatste de financiële uitvoerbaarheid. In het raadsvoorstel staat dat dit beleidskader ‘geen financiële consequenties’ heeft. Bestuurlijk klopt dit natuurlijk, die komen pas bij de uitvoeringsagenda. Wel dring ik er graag op

aan om de financiële realiteit in het behandelen van dit stuk mee te nemen. De VNG noemde dit in 2025 niet voor niets een "urgente uitdaging".

Zij stellen daarnaast ook dat, om enkel de maatregelen te treffen die nodig zijn om te voldoen aan de eisen uit de AI-verordening, "het niet de verwachting [is] dat gemeenten voldoende financiële middelen uit hun eigen begrotingen kunnen vrijmaken voor dekking van deze extra uitvoeringskosten." Ik ben daarom benieuwd waarom dit raadsvoorstel stelt dat Zutphen, ondanks nog veel verdergaande ambities, dit wel kan.

Hoe nu verder?

In het beleidskader staat dat de gemeente blijft ontwikkelen, maar "nooit ten koste van controle, zorgvuldigheid en publieke waarden". Dit lijkt mij een prachtig uitgangspunt om bij het behandelen van dit stuk in het achterhoofd te houden.

Graag verzoek ik jullie om daarom verder te kijken dan alleen dit beleidskader, maar ook de realiteit waarin het zich bevindt.

- Wees je bewust van de risico's die de gemeente gelopen heeft en loopt door dit stuk zo laat pas op te stellen, nadat AI al een goede 3.5 jaar binnen de gemeente gebruikt wordt. **Biedt duidelijkheid aan inwoners en organisaties over hoe dit is gedaan, en evalueer of dat wel veilig is gebeurd. *Breng in kaart welke processen en besluiten onbenoemd door het gebruik van onveilige publieke AI-tools tot stand zijn gekomen.***

- Kijk kritisch naar hoe je AI wilt inzetten, en of dit past bij de technologie, of je juist kwetsbaar maakt. **Onthoud dat de informatie waarmee je een keuze maakt, de keuzes die je kan maken vormt.**

- Wees realistisch in de ambities die je hebt, en waarborg daarin controle op een werkbare manier. AI is een ‘black box’ systeem; we zien alleen dat wat we erin stoppen, en dat wat eruit komt, niet hoe het daartoe komt. **Zorg daarom voor transparantie op wat erin is gestopt.**