ARTIFICIAL INTELLIGENCE KANSEN BENUTTEN IN DE VEILIGHEIDSZORG

Gebruik AI en werk aan vertrouwen

Auteurs: Ir. P.J. van Eck, Dr. R. van der Kleij,
Prof. Dr. J. Janssen, Dr. Ir. A. de Keijzer,
L. Bambach, M.M.C.M. Bastiaensen, R.M.G. de Beer,
A.C.C. van Erk, R.A.M. Korenromp,
Dr. L. Oudenhuijsen, E. ten Thij.

Datum: 7 juli 2025

avans hogeschool

MANAGEMENTSAMENVATTING

1. *Mogelijkheden nemen toe, net als uitdagingen en zorgen bij toepassen GenAI[1] in de veiligheidszorg[2].*
2. *Onderzoeksaanpak: gecodeerde analyse van een focusgroep en literatuurstudie van 20 artikelen.*
3. *Resultaten.*
    1. *Gebruik[3]: daadwerkelijk ingezette AI-toepassingen.*
        - *Focusgroep: Grote hoeveelheid gegevens begrijpen en voorspellen van veiligheidssituaties.*
        - *Literatuur: Data-analyse en cliëntsituatie specifieke taal. Waarnemen, signaleren en voorkomen van onveiligheidssituaties. Ook real time.*
    2. *Mogelijkheden[4]: verwachte AI-toepassingen en –ontwikkelingen.*
        - *Focusgroep: verder met gegevens begrijpen, kansen voor dossieropbouw en vergroten zelfredzaamheid cliënten.*
        - *Literatuur: verwacht persoonlijker, empathischer en efficiëntere toepassingen. Data combineren in besluitondersteuning.*
    3. *Hindernissen[5]: houden organisaties tegen in het gebruiken van AI-toepassingen.*
        - *Focusgroep: zien gebrek aan vertrouwen en kennis als belangrijkste hindernissen voor inzetten AI.*
        - *Literatuur: benoemt vertrouwen in AI en het willen toepassen van AI in clientgerichte zorg als hindernissen. Te ontwikkelen kennis, ervaring en leiderschap in een snel ontwikkelend AI-landschap en –regelgeving.*
    4. *Oplossingen[6]: de manieren om hindernissen aan te pakken.*
        - *Focusgroep: zien als oplossingen: kennis en oplossingen delen, leren met en van elkaar, experimenteren, en aanbrengen van focus door besturen.*
        - *Literatuur zegt: houd mensen eindverantwoordelijk, voldoe aan (EU) regelgeving, waarbij bestuurders het voortouw nemen en aantoonbaar opvolgen.*
    5. *Risico's[7]: bedreigingen bij toepassen AI in een organisatie.*
        - *Focusgroep. Systeem/gegevensaanvallen. Afhankelijkheid, vooroordelen, kennisverlies. Niet opvolgen regels. Verlies gevoelige persoonlijke info. Niet toepassen van AI.*
        - *Literatuur concretiseert de AI risico's sociaal, ethische, duurzaamheid, betrouwbaarheid, transparantie, afhankelijkheid, databescherming, aanvalsoppervlak*
    6. *Maatregelen[8]: aanpakken van AI-risico's.*
        - *Focusgroep belangrijke maatregelen mens blijft eindverantwoordelijk, samenwerken en leren, transparante afgeschermde systemen en regels opstellen en opvolgen.*
        - *Literatuur geeft maatregelen aan om AI met vertrouwen toe te passen op vier aspecten, sociale versterking, kennisontwikkeling, systeembeveiliging en besturen*
4. *Conclusie en aanbevelingen*
    - *AI-kansen benutten in de veiligheidszorg; focus op mensen die AI willen gebruiken, leren toepassen, en werk aan vertrouwen.*
    - *Aanbeveling voor vervolgonderzoek naar key drivers voor vertrouwen in AI, hoe deze te versterken en verantwoord gebruik van AI te stimuleren*

1 2 3 4 5 6 7 8 In bijlage 1 is een lijst opgenomen van definities.

INHOUDSOPGAVE

1. AANLEIDING

Toenemende mogelijkheden, uitdagingen en zorgen bij toepassen Artificial Intelligence in de veiligheidszorg

Gebruik van AI en zorgen hierover nemen toe

- Toenemende integratie van GenAI in diverse aspecten van ons leven[I].
- Toenemende complexiteit en kracht van AI systemen[I].
- Tegelijkertijd toenemende vatbaarheid voor aanvallen en misbruik van AI systemen[I].
- Gewenste (te) snelle invoering van AI met als gevolg vragen over betrouwbaarheid[II].
- Introductie van Cyber Resilience Act (CRA) en Digital Services Act (DSA) door EU bepaald[III].
- Veiligheidszorg: vertrouwelijkheid en gevoeligheid van informatie over mensen [IV].

Doel is achterhalen stand van zaken en behoeften

Doel is een dieper inzicht in de mogelijkheden en uitdagingen bij de inzet van GenAI binnen veiligheidszorg.

Onderzoeksvragen

1. Identificeren huidige stand van zaken;
2. Analyseren van de behoeften in de beroepspraktijk en belangrijkste kwetsbaarheden; en
3. Formuleren van aanbevelingen voor verdere actie en onderzoek.

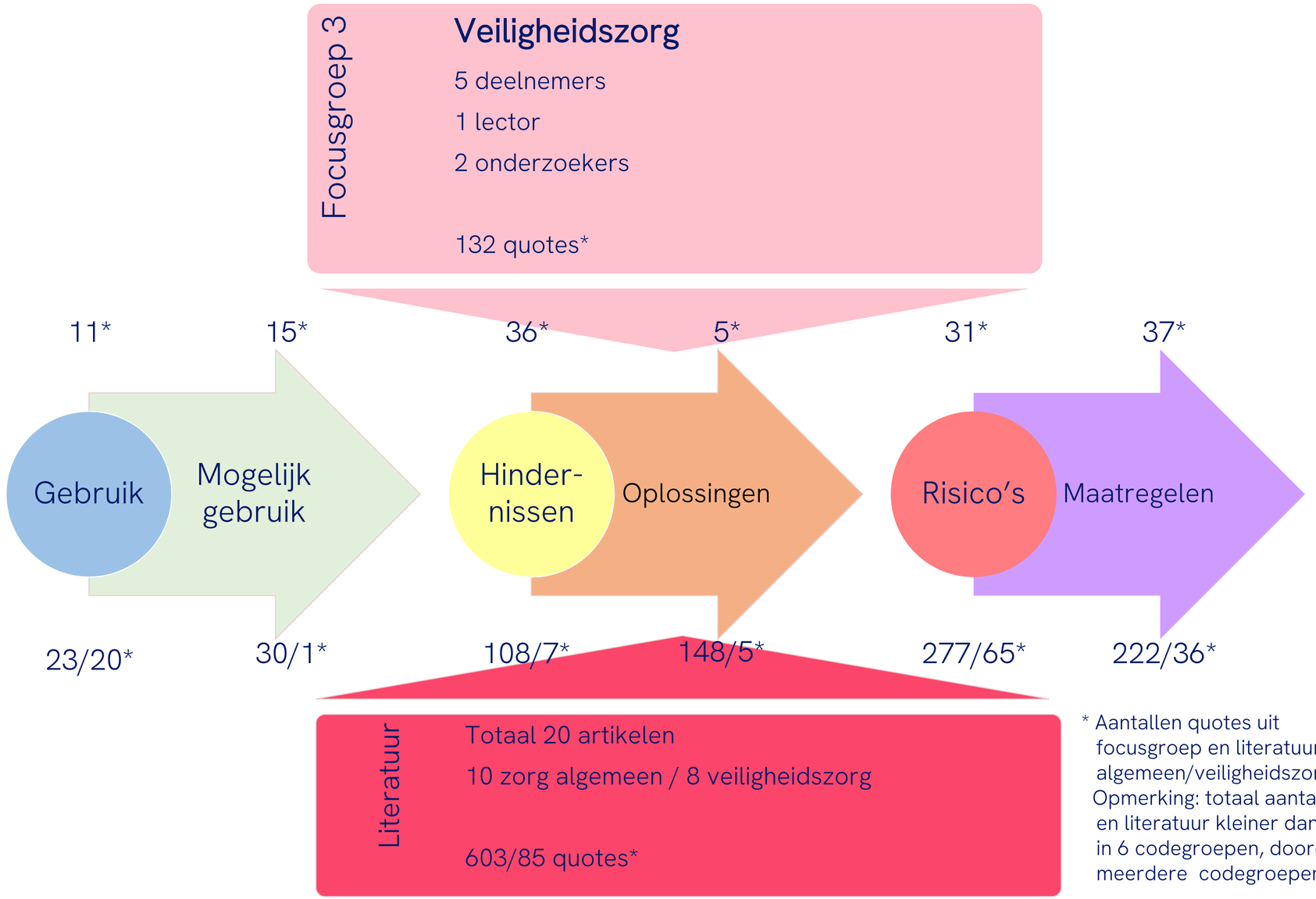
[I] Zie ook: : https://www.cybersecurityraad.nl/documenten/brieven/2023/12/22/informerende-brief-aan-de-staatssecretaris-van-bzk-over-generatieve-ai-en-cybersecurity
[II] Ibidem
[III] https://www.digitaleoverheid.nl/nieuws/dsa-voor-alle-digitale-diensten-van-kracht/
[IV] Algemene Inlichtingen- en Veiligheidsdienst & Rijksinspectie Digitale Infrastructuur. (2024). Generatieve AI: een transformatieve impact op cybersecurity. Den Haag: AIVD. Geraadpleegd op https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2024/10/17/generatieve-ai.-een-transformatieve-impact-op-cybersecurity/Generatieve+AI.+Een+transformatieve+impact+op+cybersecurity.pdf

2. ONDERZOEK OVERZICHT

Eén focusgroep in de veiligheidszorg. Daarna een literatuurstudie van 20 artikelen.
Uitgevoerd door drie lectoren en acht onderzoekers.

Bijlage 2.1
Aanpak focusgroepen

Bijlage 2.2
Aanpak literatuurstudie



* Aantallen quotes uit focusgroep en literatuur algemeen/veiligheidszorg.
Opmerking: totaal aantal quotes focusroep en literatuur kleiner dan optelling aantallen in 6 codegroepen, doordat één quote in meerdere codegroepen kan voorkomen.

avans hogeschool

4.1 RESULTATEN – DAADWERKELIJK TOEGEPASTE AI

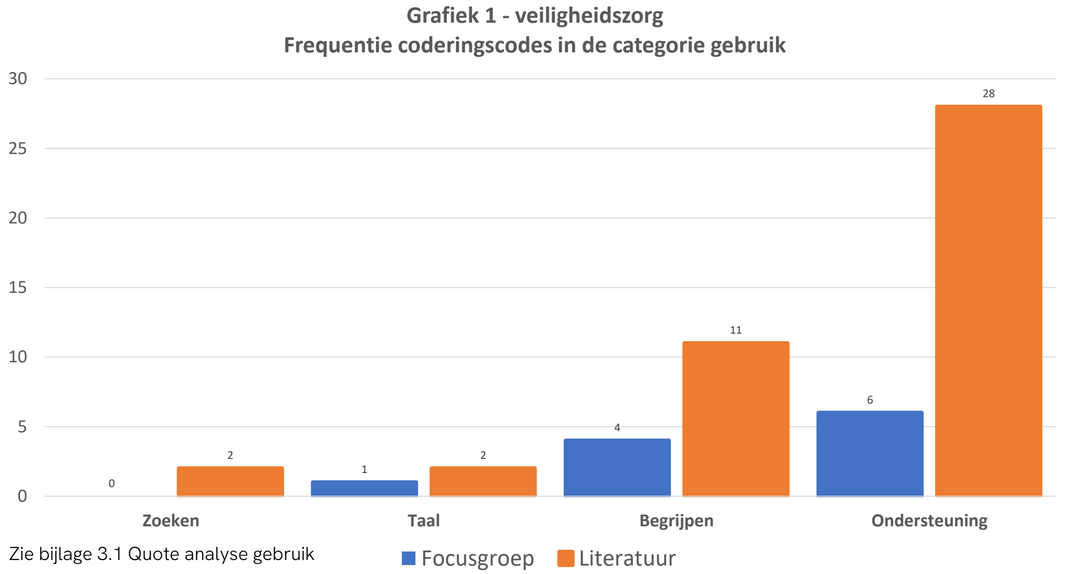
Focusgroepen, AI gebruikt om grote hoeveelheid gegevens te begrijpen en voor voorspellen van onveiligheidssituaties.

Literatuurstudie, data-analyse en taal clientsituatie specifiek. Waarnemen, signaleren en voorkomen van veiligheidssituaties. Ook real time

Focusgroepen

Veiligheidszorg gebruikt AI om grote hoeveelheden online gegevens te begrijpen en voor voorspellen van onveiligheidssituaties.

- Taal. Opslaan en verwerken van verslagen.
- Begrijpen. Hulpmiddel voor onderzoek. Voorbereiden van casuïstiek voor leren. Gebruik in VR.
- Ondersteuning. Verzamelen van informatie uit systemen. Grote hoeveelheden data analyseren, maken van situatieschetsen, scenario's voorspellen, beoordelen van onveiligheidssituaties.



Zie bijlage 3.1 Quote analyse gebruik

Literatuur

Cliënt specifiek beantwoorden van vragen en vertalen. Data-analyse en ondersteuning bij monitoring, voorspellen en besluiten/voorkomen van veiligheidssituaties, ook real time. Verbeteren behandeling van cliënten.

- Zoeken en taal. Doorzoeken gegevensdragers. Beantwoorden van cliëntvragen -met chatbots-, client specifiek gemaakt door AI-gebruik van cliëntgegevens. Vertalen van content.
- Begrijpen.
  - Diagnose. Gebruik van AI in extended reality/gedragsimulaties in diagnoses. Opsporen en handhaven, zowel voorspellend, real time en in retrospectief.
  - Leren. Gebruikte taal inzetten voor trainingsdata om werken beter en veiliger te maken. Genereren van realistische anonieme cliënttrainingsdata. Professionals informeren over laatste ontwikkelingen.
- Ondersteuning, literatuur maakt meer actuele gebruiksmogelijkheden concreet.
  - Data-analyse. Sneller, preciezer, effectiever en ook herkennen van zeldzaamheden. Ook real-time.
  - Besluitondersteuning en behandeling. classificeren, beoordelen en behandelkeuzes. Ondersteuning behandeling op afstand. Behandeling met immersieve technologie.
  - Toezicht houden en voorspellen. Cybersecurity monitoring en detecteren, b.v. van cyberpesten. Waarnemen, signaleren, voorspellen en vastleggen bewijs, b.v. voor ondersteuning meldkamer. Voorspellen van toekomstige situaties, ook mogelijkheden die zich niet eerder voordeden. Gedachten, voorkeuren, gedrag voorspellen en voorkomen.

avans hogeschool

4.2 RESULTATEN – VERWACHTE AI-TOEPASSINGEN EN -ONTWIKKELINGEN

Focusgroepen verder met gegevens begrijpen, kansen voor dossieropbouw en vergroten zelfredzaamheid cliënten.
Literatuurstudie verwacht persoonlijker, empathischer en efficiëntere toepassingen. Data combineren in besluitondersteuning.

Focusgroepen

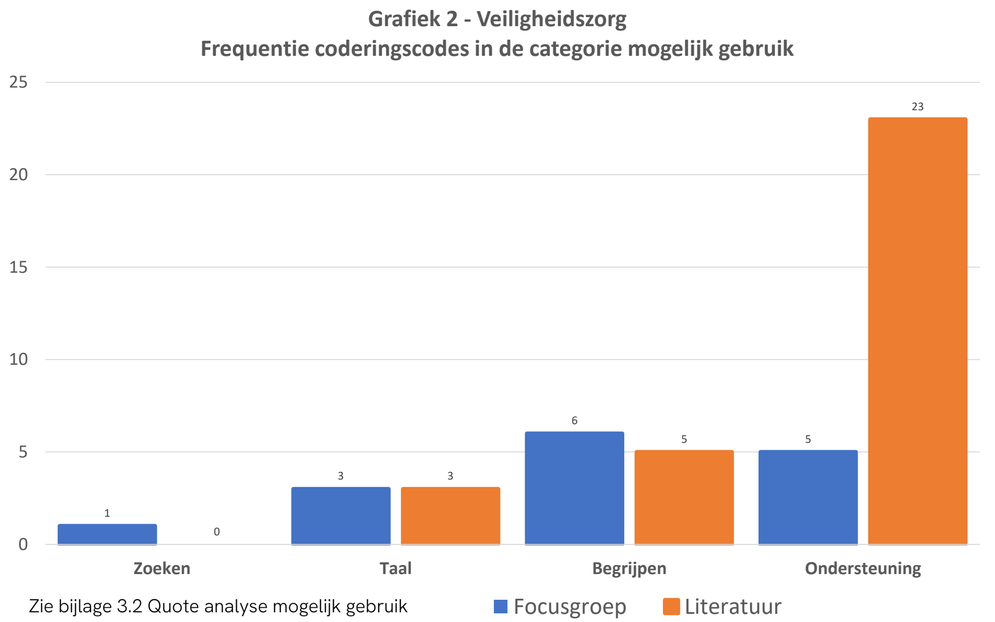
Verder met gegevens begrijpen, kansen voor dossieropbouw en zelfredzaamheid cliënten.

- Opvallende mogelijkheid voor AI, zoeken en ondersteuning, is met AI autonomie van cliënt vergroten.
- Taaltoepassingen voor spraak gestuurde verslaglegging in dossiers. Mogelijk biedt dat ook tijdwinst.
- Begrijpen. Vroegtijdig signaleren met AI. AI leren gebruiken en leren met AI.
- Ondersteuning. Data-analyse van grote hoeveelheden -online- gegevens. En werkdrukverlaging.

Literatuur

Taal eenvoudiger verslaglegging en persoonlijker vragen beantwoorden. In gegevensanalyse combineren van verschillende databronnen met persoonlijke/dossiergegevens in diagnoses en aanpak. Efficiëntere werkprocessen.

- Taal.
  - Toepassingen gericht op verminderen administratie, spraak naar tekst, vastleggen dialoog.
- Begrijpen, combineren van verschillende soorten data in analyses, diagnoses en voorspellingen
  - Analyseren en voorspellen op basis van grote hoeveelheden data.
  - Dossierkennis. Gebruik clientgegevens in analyses, diagnoses. Geschikte cliënten zoeken voor onderzoek.
  - Leren. Uitleg van complexe teksten, samenvatten. Koppelen aan persoonlijke leerpatronen.
- Ondersteuning, in aantallen het meest voorkomend in literatuur.
  - Data analyse. Herkennen/virtuele representatie van gegevens ook naar VR. Haptische toepassingen druk, warmte, kou. Meten emoties, stress. Combineren gegevensbronnen. Detecteren en signeren van aanvallen.
  - Besluitondersteuning. VR behandelingen i.p.v. of aanvullend op bestaande behandelingen. Persoonlijke maken diagnose/behandeling. GAI chatbots persoonlijker/vriendelijker/empathischer dan zorgprofessionals.
  - Plannen/werkdruk. Content genereren. Repetitieve taken verminderen. Efficiënter maken werkprocessen.
  - Client. Combineren van data, technologieën en sensoren. Vragen beantwoorden persoonlijker, beter, sympathieker.



Zie bijlage 3.2 Quote analyse mogelijk gebruik

4.3 RESULTATEN – HINDERNISSEN VOOR GEBRUIKEN AI

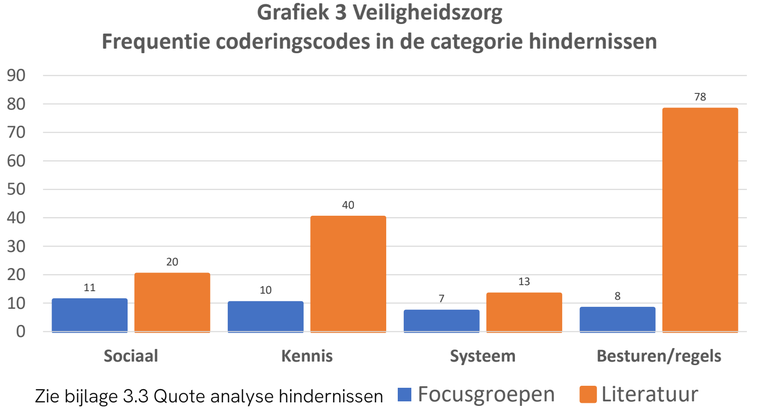
Focusgroepen zien gebrek aan vertrouwen en kennis als belangrijkste hindernissen voor inzetten AI.

Literatuur benoemt vertrouwen in AI en het willen toepassen in clientgerichte zorg als hindernissen. Te ontwikkelen kennis, ervaring en leiderschap in een snel ontwikkelend AI-landschap en –regelgeving.

Focusgroepen

Zoektocht naar kennis en vertrouwen om AI in te zetten. Weerstand door afname menselijk contact. Geld nodig voor opschalen AI.

- Sociaal. Gebrek aan vertrouwen: angst, voorzichtigheid, juistheid van de uitkomsten, beheersbaarheid, draagvlak bij cliënten. Initiële weerstand tegen AI gebruik. En ook na ervaringen met toepassen AI. Niet willen werken met AI, doordat dit naar verwachting leidt tot steeds minder menselijk contact.
- Kennis. Verschillen in en tussen organisaties. Onbekendheid met mogelijkheden, risico's en aanpak van deze transformatie. Ontbreken van AI-vaardigheden. Soms versterkt door beperkte Engelse taalvaardigheid en geestelijke / fysieke beperkingen.
- Systeem. Omvang en tempo van de AI ontwikkelingen weerhouden organisaties; het gevoel steeds verder achter te lopen.
- Besturen/regels. Geld voor AI-Pilots is er, maar opschalen kostbaar.



Zie bijlage 3.3 Quote analyse hindernissen

Literatuur

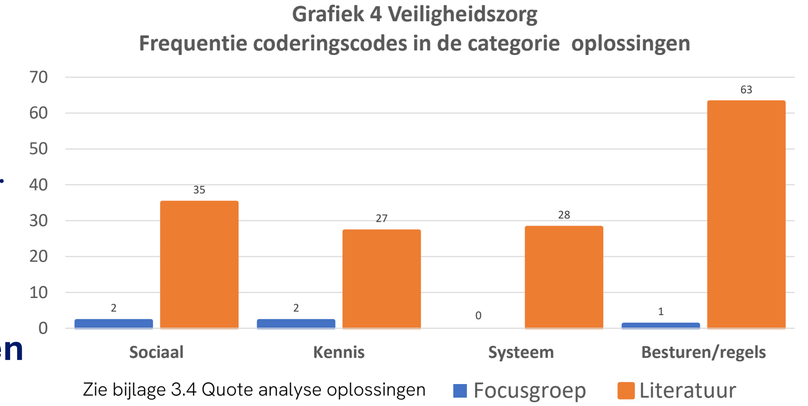
Vertrouwen in AI vraagt om betrouwbare uitkomsten. Alle stakeholders hierbij betrekken, kennis en ervaring opdoen. Snelheid van AI-ontwikkelingen en regelgeving maken het moeilijk bij te benen. Bestuurders moeten een voortrekkersrol nemen.

- Sociaal.
  - Vertrouwen. Digitale beveiliging, zeker als het gaat om persoonlijke gegevens, is cruciaal voor vertrouwen in alle digitale toepassingen. Opbouwen vertrouwen is multidimensionaal o.a. geheimhouding, beveiliging, juistheid, consistentie, kosten, werkgelegenheid, gebruiksvriendelijkheid, transparantie.
  - Willen. Medewerkers in de veiligheidszorg hebben een ambivalente houding als het gaat om toepassen van digitale technologie en inpassen daarvan binnen hun werkzaamheden. Algemeen denken economen dat AI werkgelegenheid niet zal beïnvloeden. Op de korte termijn mogelijk wel doordat sommige werkzaamheden of sectoren door AI beïnvloed worden; zoals creatief werk, data analyse, kantoorwerkzaamheden. Mogelijk versterkt doordat veiligheidszorgprofessionals niet willen of kunnen veranderen.
- Kennis.
  - Ontbreken van kennis en ervaring over gebruik van AI-toepassingen en het interpreteren van de AI-resultaten staat gebruik van AI in de weg. Algemeen versterkt door personeelstekorten. En meer specifiek door tekorten aan personeel met kennis van AI en tegelijkertijd toename van vraag naar AI-kennis en -ervaring.
- Systeem.
  - Snelheid, omvang, technische ontwikkelingen belemmeren de inzet van AI. Europa loopt hierbij achter op Amerika en China, zowel in toepassen maar ook in investeren in toepassingen en hardware.
- Bestuur/regels.
  - Voldoen aan regelgeving bij gebruik van AI toepassingen is een hindernis voor gebruik. Net als zich nog verder ontwikkelende regelgeving. Nog te beantwoorden vragen zijn of ontstaan rondom aansprakelijkheid bij gebruik van AI, intellectuele eigendomsrechten, betrouwbaarheid, privacy, beveiliging, energieverbruik.
  - Andere en de hoeveelheid aan andere prioriteiten, denk aan klimaat en energie, is een te overwinnen obstakel voor toepassen AI. Hierbij spelen capaciteit, tijd en budget beperkingen een rol. Deze beperkingen gelden niet alleen voor het gaan gebruiken van AI, maar ook gaan ook over het blijven voldoen aan zich ontwikkelende regelgeving.
  - Ondernemerschap en organisatie-inrichting. Durf, overtuiging, motivatie en leiderschap om AI te gebruiken ontbreken soms.
  - Zorgen rondom privacy vragen continue aandacht bij toepassen van AI. Controle over gevoelige persoonlijke gegevens, databeveiliging, transparantie over opslag gebruik en in lerende AI-modellen

4.4 RESULTATEN – OPLOSSINGEN PAKKEN DE HINDERNISSEN AAN

Focusgroepen kennisdelen en leren gebruiken.

Literatuur houdt mensen eindverantwoordelijk, voldoe aan (EU) regelgeving, bestuurders neem het voortouw en aantoonbaar opvolgen.



Focusgroepen

Zien oplossingen in kennis delen en leren gebruiken.

- Kennis delen en leren gebruiken worden genoemd als oplossingen voor gebrek aan kennis en vergroten van het vertrouwen.
- Hierbij is samenwerking binnen en buiten de organisaties cruciaal. Zowel binnen het eigen netwerk als ook met leveranciers.

Literatuur

Eindverantwoordelijkheid voor AI bij mensen en laat hen samenwerken. Stimuleer leren en experimenteren. Focus op gedegen bescherming van gebruikte data en systemen. Voldoe aan (EU) wet en regelgeving. Laat bestuurders het voortouw nemen en volg aantoonbaar op.

- Sociaal
  - Menselijke expertise, interactie, overzicht en eindverantwoordelijkheid zijn randvoorwaarden voor de inzet van AI-toepassingen. Dit geldt zowel in de AI-model-trainingsfase en –toepassingsfase.
  - Samenwerken en delen, van kennis en gegevens, over zorgverlening met behulp van AI en tijdens het ontwikkelen van toepassingen en modellen is essentieel voor creëren van vertrouwen. Betrek hierbij alle stakeholders, zoals eindgebruikers, bestuurders, leveranciers, toezichthouders. Nationaal en internationaal.
- Kennis.
  - Leren. Integreer kennis en expertise van professionals en -managers en hun begrip van de werking en validatie van AI-modellen en -toepassingen. Investeer in leren en training van digitale vaardigheden, om daarmee vertrouwen en weerbaarheid te vergroten van betrokkenen, organisatie en toepassing. Benadruk en zet in op voortdurend verbeteren door anticiperen, monitoring, reageren en evalueren.
  - Experimenteren. Experimenteer en maak proof-of-concept studies onderdeel van AI-integratie in zorgprocessen, AI-gebruikersacceptatie en AI-validatie. Een “public-space” voor het delen van kennis en ervaring helpt in alle fase van AI-ontwikkelingen: ontwerp, oplossingen voor belemmeringen, beleid, gebruikersrichtlijnen en standaardisatie.
- Systeem.
  - Techniek. Voorkom fouten door gebruik van (AI)detectieprogramma’s en laat experts meldingen nagaan. Train alle professionals in het bestaan en herkennen van synthetische realiteiten en hoe hiermee om te gaan. Voldoen aan wet en regelgeving vraagt om opt-out, machine unlearning mechanismen, risicobeheersing.
  - Transparantie. De overheid moet een voortrekkersrol nemen in het activeren van digitale bewustwording en burgerschap, bijvoorbeeld door het voeren van sociale dialogen over inzet en gebruik van AI en de mogelijke impact. Vooraf consulteren, achteraf monitoren en borgen van AI gebruik zoals bedoeld is een belangrijke taak van toezichthouders.
  - Standaardisatie. Laat overheden, NL en EU, het voortouw nemen in opstellen van (inter)nationale standaarden en de opvolging hiervan in AI, bijvoorbeeld door certificering.
- Bestuur/regels.
  - Regelgeving. Voldoen aan EU wetgeving en richtlijnen, zoals General Data Protection Regulation, AI-Act, Cyber Resiliance Act, Product Liability Directive, voorgestelde AI Liability Directive, rulings of the EU Court of Justice. Bij rechtspraak moeten alle professionals leren om vooral te twijfelen aan het geleverde bewijsmateriaal.
  - Beleid. Opstellen van beleid en richtlijnen door organisaties voor het in goede banen leiden van AI initiatieven. Bestuurs laten aansluiten op initiatieven zoals Strategisch Actie Plan AI, NL digitaal, NCSC onderzoek agenda.
  - Monitoren. Regelmatig updaten, screenen en valideren van systemen. Proactieve risico inventarisaties. Afstemmen op publieke normen en waarden en voorkomen dat deze onder druk komen te staan.
  - Afschermen. Afschermen en encryptie van gevoelige informatie gebruiken. Cruciaal voor het vertrouwen in toepassingen en voor het respect en vertrouwen van cliënten en hun autonomie.

4.5 RESULTATEN – RISICO'S BIJ TOEPASSEN AI IN ORGANISATIES (1/2)

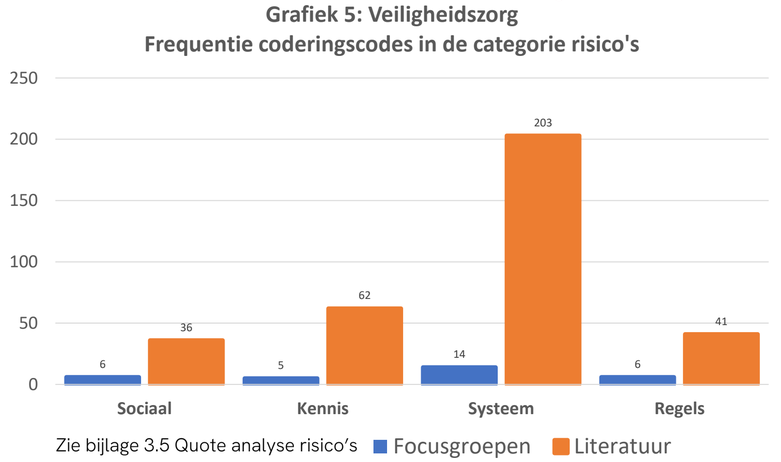
Focusgroepen. Systeem/gegevensaanvallen. Afhankelijkheid, vooroordelen, kennisverlies. Niet opvolgen regels. Verlies gevoelige persoonlijke info. Niet toepassen van AI

Literatuur concretiseert de AI risico's sociaal, ethische, duurzaamheid, betrouwbaarheid, transparantie, afhankelijkheid, databescherming, aanvalsoppervlak.

Focusgroepen

Systeembescherming, menselijke afhankelijkheid en vooroordelen, niet opvolgen van regelgeving, verlies gevoelige persoonlijke informatie, databetrouwbaarheid en acceptatie.

- Sociaal. Medewerkers die zo niet willen werken. Vooroordelen van mensen. Acceptatie door cliënten.
- Kennis. Onmogelijkheid om AI-resultaten te verklaren en afhankelijkheid van AI.
- Systeem. Databescherming, databetrouwbaarheid en feitelijke juistheid van de uitkomsten van de gebruikte AI-toepassingen.
- Regels. Privacy en non compliance in relatie tot gevoelige persoonlijke informatie waarmee de sector werkt.



Literatuur

Grootschalig toepassen van AI leidt tot ongewenste ontwikkelingen; sociaal, ethische en op duurzaamheid. Onjuistheid van AI uitkomsten en hoe hier mee om te gaan door kennisverlies, verkeerde of gemanipuleerde gegevens. Grote zorgen over toename van vertrouwelijke gegevens.

- Sociaal
  - Ontwikkeling. AI systemen die menselijke interactie vervangen vergroten sociale isolatie en bedreigen zo mentaal en fysiek welzijn. Grootschalig toepassen AI kan ook slechts enkele superstar bedrijven bevoordelen en sociale en economische ongelijkheid veroorzaken. Sociaal engineering bedreigt AI-toepassingen en –gegevens.
  - Ethiek. Balanceren van economische drijfveren en cliënt-veiligheid. Ook afwegen van cognitieve, sociale, en culturele aspecten; omgang met creativiteit, normen, emoties en eerlijke verdeling van kosten en opbrengsten.
  - Duurzaamheid. Grootschalige inzet van computers voor AI bedreigend voor energie, water, emissie en zeldzame materialen. Mensgerichte waarden onder druk, zoals cognitieve, sociale, culturele en interpersoonlijke ontwikkeling.
  - Winstgedrevenheid. Zorgen over eerlijke verdeling eigenaarschap, duurzaamheid, werkgelegenheid, kwaliteit van banen, kosten van arbeid. Winner takes all mentaliteit en machtsconcentratie van grote ondernemingen met lock in van cruciale sectoren zoals onderwijs, zorg en journalistiek.
- Kennis.
  - Transparantie. AI-black boxes bedreigen o.a. juistheid, betrouwbaarheid, veiligheid, transparantie, traceerbaarheid, gelijkwaardigheid, duurzaamheid en verlagen menselijke controle over besluitvorming.
  - Bias. Beschikbaarheid en kwaliteit van gegevens bepalen uitkomsten van AI-toepassingen. Hierdoor staan betrouwbaarheid en validiteit van de uitkomsten en bruikbaarheid van deze toepassingen mogelijk onder druk. Denk bijvoorbeeld aan niet of nauwelijks beschikbare data van (sub)doelgroepen die leiden tot verkeerde conclusies: voorbeeld kindertoeslagaffaire. Beïnvloeding van de mentale autonomie door de combinatie van AI en VR.
  - Afhankelijkheid. Van enkele grote leveranciers van AI-toepassingen, afnemende kennis binnen organisaties, en tekorten aan AI- en cybersecurity-experts. Mogelijk versterkt door gebrekkige kwaliteit van gegevens. Dit werkt mogelijke menselijke fouten in de hand.

4.5 RESULTATEN – RISICO'S BIJ TOEPASSEN AI IN ORGANISATIES (2/2)

Literatuur (vervolg)

- Systeem.
  - Databescherming. Data-gijzeling, -hacks, -misbruik, -vervuiling, -manipulatie, niet-gegarandeerde data-opt-out. Niet voldoen aan wettelijke strikte vertrouwelijkheidvereisten van persoonlijke gegevens. Wedloop om de grootste, rijkste, meeste data-sets te realiseren als bedrijfsstrategie vergroot de impact van aanvallen op leveranciers, AI-blackout of verlies van data-controle.
  - Feitelijke juistheid. AI is gebaseerd op statistische voorspelbaarheid en introduceert daarmee een foutkans in de uitkomsten. Die mogen professionals niet klakkeloos als feiten aannemen, want deze kunnen leiden tot foutieve conclusies of aanbevelingen. De waarheidsgetrouwheid van gegenereerde uitkomsten maakt het moeilijk om echt van vals te onderscheiden, waarbij intuïtief soms juist de valse uitkomst meer vertrouwd wordt.
  - Aanvallen. Centrale dataopslag, maar ook de toename van opgeslagen data en plaatsen waar data wordt verzameld, maakt systemen kwetsbaar voor aanvallen. AI zelf ook steeds beter te gebruiken om aanvallen uit te voeren.
  - Beschikbaarheid. Toenemende integratie van fysieke en digitale processen maakt processen kwetsbaar voor het niet beschikbaar zijn van systemen.
  - Manipulatie. Misinformatie, beïnvloeding, data-manipulatie, aanvallen, mengen van persoonlijke en generieke informatie maken allerlei bewuste en onbewuste fouten mogelijk.
- Bestuur/regels.
  - Privacy. Cliënten en professionals bezorgd over bescherming en datalekken van gevoelige persoonlijke gegevens en betrouwbaarheid van AI-uitkomsten. Versterkt door gebrek aan transparantie in gebruikte training- en gebruiksdata. Alsmaar toenemende mogelijkheden om gedetailleerd fysieke, mentale en gedragsgegevens te verzamelen, combineren, controleren, misbruiken.
  - Non compliance. Negeren van voorgeschreven minimaliseren datagebruik en dataopslag. Negeren wet- en regelgeving, zoals AI Act en General Data Protection Regulation.
  - Aansprakelijkheid. Wettelijk onduidelijke aansprakelijkheid, ook (nog) niet vanuit jurisprudentie, van ontwikkelaars, instellingen, professionals bij onjuiste uitkomsten AI en of AI gebruik bij aanvallen.

4.6 RESULTATEN – MAATREGELEN AANPAKKEN VAN AI-RISICO'S (1/2)

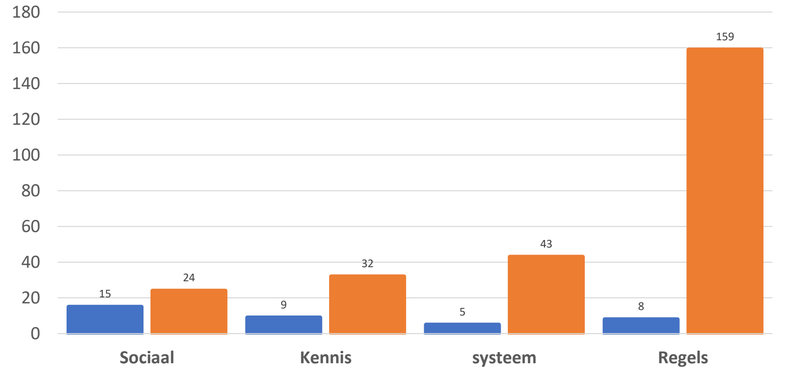
Focusgroepen zien als belangrijke maatregelen mens blijft eindverantwoordelijk, samenwerken en leren, transparante afgeschermde systemen en regels opstellen en opvolgen.

Literatuur geeft maatregelen aan om AI met vertrouwen toe te passen op vier aspecten, sociale versterking, kennisontwikkeling, systeembeveiliging en besturen.

Focusgroepen mens eindverantwoordelijk, samenwerken, leren en kennisdelen, transparante afgeschermde systemen en regels opstellen en opvolgen.

- Sociaal. Eindverantwoordelijkheid door stimuleren kritisch denken, context meewegen, zelf advies schrijven, testen, evalueren, rapporteren fouten. Samenwerken intern/extern, expertise netwerk, met onderwijs, planmatig, leverancierscontracten.
- Leren. Herhaalde opleidingen, blijven communiceren, protocollen, oefenen kritisch en reflectief denken en handelen, kleine experimenten met positief kritische koplopers, expertise concentreren.
- Systemen. Transparantie, op hoofdlijnen hoe het werkt en wat er met data gebeurt, herleidbare data en bronnen, regressie. Afschermen noodzakelijke functies en toepassingen, minimaliseer modellen en datagebruik, filter op persoons- en bedrijfsgegevens, encryptie, anonimiseren.
- Regels. Stimuleer gebruik en AI geletterdheid, DPIA en IAMA assessments, responsible AI principes, opvolging wetgeving, richtlijnen AI-tools, afspraken over gegevens en gebruik, dossiers en data op orde, toestemming van cliënten.

Grafiek 6: Veiligheidszorg
Frequentie coderingscodes in de categorie maatregelen



Zie bijlage 3.6 Quote analyse maatregelen ■ Focusgroepen ■ Literatuur

Literatuur

Benoemt, net als focusgroepen, maatregelen om met vertrouwen AI toe te passen. Benadrukt eindverantwoordelijkheid van mensen en het belang van vastgelegde afspraken hierover. Actief kennis verwerven door experimenteren, educatie en kwaliteitsborging. Focus op explainable AI in alle systeemaspecten. En als organisatie toepassen van AI stimuleren, en met behulp van tools en raamwerken AI-inzet monitoren en bijsturen waar nodig.

- Sociaal
  - Eindverantwoordelijkheid. Toepassen van AI vereist eindverantwoordelijkheid van mensen in alle fase van ontwikkeling, testen tot gebruik. Professionals leren hoe publieke normen en waarden toe te passen in het gebruik van data en AI.
  - Samenwerken. Multidisciplinaire samenwerking. Binnen een organisaties, zoals veiligheidszorgprofessionals, ICT, kwaliteit en veiligheidsmedewerkers. Ook met externe betrokkenen, zoals cliënten en leveranciers. Hierbij gaat het ook over ethisch verantwoord gebruik van AI met methodes zoals Rapid Ethical Deliberation of Ethical Legal Societal Aspects.
  - Vertrouwen. Vertrouwen is gedeeltelijk gebaseerd op het land van herkomst van een leverancier. Dit bepaalt de wetten en regels waaraan moet worden voldaan.
- Kennis.
  - Educatie. Besteed aandacht aan ontwikkelen van vaardigheden om AI-toepassingen en –uitkomsten te doorgronden, te beoordelen en gepast te handelen, o.a. fact-checken. Het gaat hierbij aan het tegelijk ontwikkelen van AI technieken en het toepassen hiervan in de werkprocessen. Niet om het simpelweg automatiseren van bestaande taken, maar ontdekken en ontwikkelen van nieuwe betrouwbare en bewezen werkwijzen uitgevoerd door veiligheidszorgprofessionals ondersteund door AI.
  - Kwaliteit. Verdedig de kwaliteit van AI toepassing door data-kwaliteit, gevalideerde input, veilige supply-chain, beveiligde systemen modellen en data, en traceerbaarheid. Maak capaciteit en middelen vrij voor kwaliteitswerkzaamheden, zoals valideren en borging. Hanteer een multidisciplinaire aanpak om fundamentele rechten te borgen en discriminatie te voorkomen. Pas methodes zoals Rapid Ethical Deliberation of ELSA toe; identificeer ethische kwesties, discussie vanuit verschillende perspectieven en benoem vervolgacties. Zo onstaan ethisch robuuste AI toepassingen die zich ook continue verbeteren.

avans hogeschool

4.6 RESULTATEN – MAATREGELEN AANPAKKEN VAN AI-RISICO'S (2/2)

Literatuur (vervolg)

- Systeem.
  - Transparantie. Explainable AI-toepassingen vraagt om begrijpelijke, uitlegbare en gevalideerde systemen. Door leveranciers, gebruikers, cliënten en toezichthouders. Dit betreft alle onderdelen van AI, zoals data, modellen, statistieken, algoritmes, ontwikkelaanpak, testen, trainingen.
  - Technologie. Hanteer bestaande en bewezen betrouwbare tools, technieken en systeemcomponenten om de juiste werking van AI toepassingen te garanderen en te monitoren.
  - Dataset. Gedurende de gehele levenscyclus van een AI –toepassing is gestructureerde en planmatig aandacht nodig voor datamanagement. Externe en interne validatie, voorafgaande en gedurende het gebruiken van AI-toepassingen. Bij kleinere datasets is dit nog uitvoerbaar door professionals. Grotere datasets hebben nieuwe technieken nodig.
  - Gedistribueerde systemen. Bij praktische toepassing van AI is beschikbaarheid cruciaal. Met gedistribueerde systemen worden single points of failure verminderd en blijft een systeem functioneren, ook als componenten uitvallen.
- Bestuur/regels.
  - Beleid. Organisaties moeten richtlijnen opstellen om aan wetten en regels te voldoen. Voor integratie van AI in software, hardware, toepassingen en workflows. Hierin moet de organisatieleiding het voortouw nemen en stakeholders betrekken. Een AI governance vraagt om integratie van richtlijnen voor AI op ander organisatiebeleid.
  - Privacy. Hanteer en geef invulling aan de volgende principes: respecteer fundamentele rechten, discrimineer niet, garandeer kwaliteit, certificeer modellen, beveilig de gebruikte modellen en data, zorg voor modeltransparantie, informeer gebruikers en cliënten en laat hen de ultieme controle over toepassingen.
  - Controleren en monitoring. Gedurende alle fase van ontwikkeling en gebruik van AI-toepassingen is monitoring en bijsturen noodzakelijk. Denk aan vastlegging van onderhoud, defecten, opvolging van verbeterdoelstellingen. Menselijke eindverantwoordelijkheid voor al deze onderdelen blijft de maatstaf.
  - Management/framework/tools. Kiezen en praktisch invullen van raamwerk modellen en tools voor betrouwbaar toepassen van AI. Zoals NIST cybersecurity framework, NL AIVD veilig toepassen van AI, Googles Open Frontier Safety Framework, OpenAI's Preparedness Framework, Gladstone's proposed AI Obervatory, framworks in ontwikkeling van Dcypher/TNO/Tue.
  - Ontwikkeling stimuleren en organiseren. Om de toegevoegde waarde die AI kan leveren te benutten moeten bestuurders ontwikkeling en toepassing van AI stimuleren. Ongewenste effecten voorkomen is daar een onderdeel van, maar zeker ook gewenste effecten actief stimuleren. Om zo het risico van niet gebruiken van AI te voorkomen. En om snel en effectief in te spelen op onbekende en ongewenste effecten die zich abrupt kunnen voordoen.

5. CONCLUSIE & AANBEVELINGEN (1/3)

Onderzoeksvraag

Wat is de huidige stand van zaken met betrekking tot de cybersecurity van Generatieve AI-systemen in de gezondheidszorg, en welke specifieke behoeften en kwetsbaarheden spelen een rol bij het waarborgen van de veiligheid van deze systemen?

Door het gebruik van GenAI ontstaan risico's op vier gebieden:

- Sociaal. Systemen die menselijke interactie vervangen;
- Kennis. Afname van kennis nodig om uitkomsten van systemen kritisch te beschouwen;
- Systemen. Afhankelijkheid van systemen, zorgen om feitelijke juistheid en bescherming van persoonlijke gegevens;
- Regels. Voldoen aan wet- en regelgeving en aansprakelijkheid.

Deelvragen

1. **Identificeren huidige stand van zaken.**
2. **Analyseren van de behoeften in de beroepspraktijk en belangrijkste kwetsbaarheden;**
3. **Formuleren van aanbevelingen voor verdere actie en onderzoek.**

Beantwoord op de volgende pagina's

5. CONCLUSIE & AANBEVELINGEN (2/3)

Ad. 1. Identificeren huidige stand van zaken.

Onderverdeeld in nu al gebruikte en mogelijk gebruikte AI-toepassingen.

- Gebruik: daadwerkelijk ingezette AI-toepassingen.
  - Focusgroepen: benoemt gebruik AI om grote hoeveelheden online gegevens te begrijpen en voor voorspellen van onveiligheidssituaties.
  - Literatuur: vult aan met toepassingen die cliënt specifiek vragen beantwoorden en vertalen. Data-analyse en ondersteuning bij monitoring, voorspellen en besluiten/voorkomen van veiligheidssituaties, ook real time. Verbeteren behandeling van cliënten.
- Mogelijkheden: verwachte AI-toepassingen en –ontwikkelingen.
  - Focusgroepen: verder gaan met gegevens begrijpen, kansen voor dossieropbouw en zelfredzaamheid cliënten bevorderen.
  - Literatuur: vereenvoudigen verslaglegging en persoonlijker vragen beantwoorden. In gegevensanalyse combineren van verschillende databronnen met persoonlijke/dossier-gegevens in diagnoses en aanpak. Efficiëntere werkprocessen.

Ad. 2. Analyseren van de behoeften in de beroepspraktijk en belangrijkste kwetsbaarheden.

Beantwoord door eerst in te zoomen op behoeften en daarna op kwetsbaarheden.

Behoeften in de beroepspraktijk onderverdeeld door eerst hindernissen in kaart te brengen en vervolgens oplossingen voor deze hindernissen te benoemen.

- Hindernissen: houden organisaties tegen in het gebruiken van AI-toepassingen.
  - Focusgroepen: Zoektocht naar kennis en vertrouwen om AI in te zetten. Weerstand door afname menselijk contact. Geld nodig voor opschalen AI.
  - Literatuur: Vertrouwen in AI vraagt om betrouwbare uitkomsten. Alle stakeholders hierbij betrekken, kennis en ervaring opdoen. Snelheid van AI-ontwikkelingen en regelgeving maken het moeilijk bij te benen. Bestuurders moeten een voortrekkersrol nemen.
- Oplossingen: de manieren om hindernissen aan te pakken.
  - Focusgroepen: zien als oplossingen kennis delen en leren gebruiken.
  - Literatuur: houdt eindverantwoordelijkheid voor AI bij mensen en laat hen samenwerken. Stimuleer leren en experimenteren. Focus op gedegen bescherming van gebruikte data en systemen. Voldoe aan (EU) wet en regelgeving. Laat bestuurders het voortouw nemen en volg aantoonbaar op.

Kwetsbaarheden zijn allereest uitgewerkt in risico's waarvoor vervolgens mogelijke maatregelen in kaart zijn gebracht.

- Risico's: bedreigingen bij toepassen AI in een organisatie.
  - Focusgroepen: systeembescherming, menselijke afhankelijkheid en vooroordelen, niet opvolgen van regelgeving, verlies gevoelige persoonlijke informatie, databetrouwbaarheid en acceptatie.
  - Literatuur: grootschalig toepassen van AI leidt tot ongewenste ontwikkelingen; sociaal, ethische en op duurzaamheid. Onjuistheid van AI-uitkomsten en hoe hier mee om te gaan door kennisverlies, verkeerde of gemanipuleerde gegevens. Grote zorgen over toename van vertrouwelijke gegevens.
- Maatregelen: aanpakken van AI-risico's.
  - Focusgroepen: houdt mens eindverantwoordelijk, samenwerken, leren en kennisdelen, transparante afgeschermde systemen en regels opstellen en opvolgen.
  - Literatuur: benoemt, net als focusgroepen, maatregelen om met vertrouwen AI toe te passen. Benadrukt eindverantwoordelijkheid van mensen en het belang van vastgelegde afspraken hierover. Actief kennis verwerven door experimenteren, educatie en kwaliteitsborging. Focus op explainable AI in alle systeemaspecten. En als organisatie toepassen van AI stimuleren, en met behulp van tools en raamwerken AI-inzet monitoren en bijsturen waar nodig.

avans hogeschool

5. CONCLUSIE & AANBEVELINGEN (3/3)

Ad. 3. Formuleren van aanbevelingen voor verdere actie en onderzoek.

De belangrijkste overeenkomsten en verschillen tussen de focusgroepen en de literatuur.

- De focusgroepen en literatuur kennen en beschrijven beide dezelfde vier risicogebieden; sociaal, kennis, systemen en regelgeving.
- De literatuur is gedetailleerder in de uitwerkingen.
- Bijvoorbeeld: focusgroepen denken aan betere taaltoepassingen. De literatuur maakt dit concreet met voorbeelden van efficiënter en cliëntgericht-taalgebruik in AI-toepassingen.

Advies aan zorgprofessionals om Artificial Intelligence kansen te benutten in de gezondheidszorg

- Werk aan vertrouwen;
- Dat begint met en draait om mensen, die AI willen gebruiken;
- Daarvoor is kennisontwikkeling door experimenteren noodzakelijk;
- Om te leren en te weten wat veilig werkt; en
- Als organisatie, medewerker en cliënt te kunnen wat daarvoor nodig is.

De behoefte en kansen voor vervolgonderzoek uit de beroepspraktijk en de wetenschap

Vragen uit de beroepspraktijk zijn vooral hoe-vragen, zoals:

- Op welke manier vergroot AI de autonomie van cliënten in de zorg?
- Welke mogelijkheden biedt AI voor leren in de zorg?
- Wat bepaalt het succes van een AI-experiment in de zorg?
- Wat zijn randvoorwaarden voor opschalen van succesvolle AI-experimenten?
- Aan welke transparantievereisten moet AI voldoen om weerbaarheid van mens en organisatie te vergroten?
- Welke (anti)neutralisatietechnieken werken om gebruik van AI te stimuleren?
- Wat zijn de key drivers voor vertrouwen in AI en hoe deze te versterken?

Vragen uit de wetenschap richten zich op meer inzicht, zoals:

- Welke factoren bepalen menselijke eindverantwoordelijkheid bij toepassing van AI en hoe deze inzichtelijk te maken?
- Op welke manier is AI risico te meten?

Hoe nu verder?

- Stap 1: Met de stakeholders prioriteren van de onderzoeksvragen; en
- Stap 2: Samenwerkingsverbanden starten voor het indienen van subsidieaanvragen om deze vragen te beantwoorden.

avans hogeschool

BIJLAGEN

avans hogeschool

1. DEFINITIES

Term	Definitie	Bron
1. Generatieve AI	Generatieve AI verwijst naar een type kunstmatige intelligentie dat in staat is nieuwe inhoud te creëren. Het is daarmee een onderdeel van een nieuwe generatie van AI, in tegenstelling tot meer klassieke AI welke gericht is op het leren herkennen en voorspellen van patronen in cijfermatige data (ook wel bekend als machine learning), het begrijpen van tekst (bekend als natural language processing) en beeld (ook wel computer vision genoemd). Het genereren van nieuwe inhoud kan variëren van tekst en beelden tot muziek en video's. De kern van GAI-modellen is het vermogen patronen, stijlen of regels uit bestaande datasets te leren en deze kennis te gebruiken om nieuwe, unieke en realistische output te genereren die past binnen de geleerde context. In de laatste jaren is GAI in drie vormen sterk ontwikkeld: het genereren van beelden, genereren van teksten en genereren van synthetische data	Stokkum, R. v., Bouwman, J., & Kamstra, R. (2024). Generatieve AI in de Nederlandse zorg. TNO, TNO Healthy Living & Work. Delft: TNO Public. Opgeroepen op januari 29, 2025
2. Veiligheidszorg	Ik neem geregeld het woord 'veiligheidszorg' in de mond. Daarmee bedoel ik professionals en organisaties in verschillende sectoren die zich bezighouden met diverse aspecten van veiligheidsvraagstukken: van preventie tot en met aanpak en van behandeling tot en met de tenuitvoerlegging van sancties. Het aantrekkelijke van het woord 'veiligheidszorg' is voor mij gelegen in het gegeven dat het niet alleen om de justitiële sector gaat – politie, OM, rechterlijke macht, reclassering en gevangeniswezen – maar ook sectoren includeert die zich met (medische) zorg, hulpverlening en opvang bezighouden, alsmede sectoren die een belangrijke rol kunnen spelen bij het tijdig herkennen van veiligheidsvraagstukken. In dit verband denk ik bijvoorbeeld aan het onderwijs en de (geestelijke) gezondheidszorg.	Janssen, J. H. L. J. (2021). De toren van Babel: een (rechts) antropologische blik op samenwerking bij de aanpak van geweld in afhankelijkheidsrelaties. Boom juridisch.
3. Gebruik	Daadwerkelijk ingezette AI-toepassingen.	
4. Mogelijkheden	Verwachte AI-toepassingen en –ontwikkelingen.	
5. Hindernissen	Houden organisaties tegen in het gebruiken van AI-toepassingen.	
6. Oplossingen	Manieren om hindernissen aan te pakken.	
7. Risico's	Bedreigingen bij toepassen AI in een organisatie.	
8. Maatregelen	Aanpakken van AI-risico's.	

2.1 AANPAK FOCUSGROEPEN

Doelgroep bepalen

- Focus op zorg zoals opgenomen in preseed-onderzoeksaanvraag.
- In kernteamoverleg is onderscheid gemaakt tussen gezondheidszorg en veiligheidszorg.

5 deelnemers
1 lector
2 onderzoekers

Uitnodiging

- LinkedIn uitnodigingen gericht op AI geïnteresseerden uit de gezondheidszorg en veiligheidszorg.
- Persoonlijke benadering van deelnemers voor de focusgroep veiligheidszorg om voldoende deelnemers te verkrijgen.

Voorberiding focusgroep

- Opbouw van de werksessie in PowerPoint format. Review en aanscherpingen van concept naar definitieve versie in meerder rondes door onderzoekers en lectoren.
- Voorbereiding van de vragen: gebruik, mogelijk gebruik, hindernissen, oplossingen, risico's en maatregelen.
- Bij risico's en maatregelen eerste vraag gesteld en ongeholpen – top of mind – antwoorden, daarna geholpen met een overzicht uit vooronderzoek gevraagd naar herkenning / aanvullingen.

Veiligheidszorg
5 deelnemers

Focusgroepen

- 1 focusgroep met deelnemers uit de veiligheidszorg.
- Moderatie van de sessie door onderzoeker / doorvragen door moderator en lector.

Veiligheidszorg
132 quotes

Analyse

- Transcriptie van de focusgroepen met behulp van Teams.
- Transcripties gecodeerd door 1 onderzoeker met behulp van Atlas.ti, met een review door een 2e onderzoeker.
- Sorteren en waar nodig samenvoegen van codes.

Rapportage

- Tabellenoverzicht met observaties uit gecodeerde quotes op elk van de zes deelvragen: gebruik, mogelijk gebruik, hindernissen, oplossingen, risico's en maatregelen.
- Samenvatting van observaties uit de focusgroepen geformuleerd.
- Kernboodschap geformuleerd voor elk van de zes deelvragen.

avans hogeschool

2.2 AANPAK LITERATUURSTUDIE

	Onderzoeks-vraag	▪ "Wat is de huidige stand van zaken met betrekking tot de cybersecurity van Generatieve AI-systemen in de gezondheids- en veiligheidszorg, en welke specifieke behoeften en kwetsbaarheden spelen een rol bij het waarborgen van de veiligheid van deze systemen?
176 37 dubbel 139 netto	Zoektermen	▪ Generatieve kunstmatige intelligentie, toepassing, risico, veiligheid, zorg, veiligheidszorg (en synoniemen) ▪ Nederlands, Engels ▪ Gezocht in Google Scholar
139 122 afgevallen 17 netto	Aanscherpen zoektermen	▪ Inclusiecriteria: (peer)reviewed, maximaal 3 jaar oud, gericht op Nederlandse gezondheidszorg/veiligheidszorg ▪ Exclusiecriteria: opniestukken, scripties, ongepubliceerd werk, ouder dan 3 jaar, gezondheidszorg/veiligheidszorg buiten Nederland
17 12 toegevoegd 29	Databases	▪ Pubmed, IEE Xplore, SpringerLink, ScienceDirect, Medline
29 7 toegevoegd 36	Experts	▪ Door lectoren aangeleverde artikelen
36 10 algemeen 16 gezondheidszorg 8 veiligheidszorg 36	Sorteren	▪ Artikelen sorteren in drie subcategoriën: zorg algemeen, gezondheidszorg, veiligheidszorg
10 algemeen 8 veiligheidszorg	Onderzoekers	▪ Lezen 10 artikelen algemeen 603 quotes en 8 artikelen veiligheidszorg met 85 quotes. Quotes in 6 categorieën: gebruik, mogelijk gebruik, hindernissen, oplossingen, risico's en maatregelen ▪ Samenvatting van observaties uit de literatuur en kernboodschap geformuleerd voor elk van de zes categorieën. ▪ Quote analyse met behulp van ChatGPT voor categorieën hindernissen, oplossingen, risico's en maatregelen.

avans hogeschool

3.1 QUOTE ANALYSE FOCUSGROEPEN EN LITERATUUR

Tabel 1. Frequentie coderingscodes in de categorie gebruik: daadwerkelijk ingezette AI-toepassingen.

	Veiligheidszorg	Focusgroep						
		Focusgroep 3 - Cybersecurity GenAI in de Veiligheidszorg Gr=131	subtotal		Literatuur beide Gr=603; GS=10	Literatuur veiligheidszorg Gr=85; GS=10	subtotal	Totals
Zoeken	• Gebruik: Zoeken Gr=7			• Gebruik: Zoeken Gr=8	1	1	2	2
Taal	• Gebruik: Verslaglegging Gr=13	1	1	• Gebruik: Verslaglegging Gr=14			2	3
	• Gebruik: Schrijven Gr=8			• Gebruik: Schrijven Gr=8				
				• Gebruik: Antwoorden Gr=6	1			
	• Gebruik: Vertalen Gr=5			• Gebruik: Vertalen Gr=6	1			
Begrijpen	• Gebruik: Diagnostiek Gr=27	2	4	• Gebruik: Diagnostiek Gr=38	1	2	11	15
	• Gebruik: Leren Gr=17	2		• Gebruik: Leren Gr=30	8			
	• Gebruik: Dossierkennis-EPD Gr=5			• Gebruik: Dossierkennis-EPD Gr=17				
Ondersteuning	• Gebruik: Data analyse Gr=12	5	6	• Gebruik: Data analyse Gr=22	2	4	28	34
	• Gebruik: Besluitondersteuning Gr=16	1		• Gebruik: Besluitondersteuning Gr=20	1	1		
				• Gebruik: Toezichthouden Gr=7	2	4		
				• Gebruik: Behandeling Gr=17	3			
	• Gebruik: Plannen Gr=8			• Gebruik: Plannen Gr=8				
				• Gebruik: Voorspellen Gr=17	3	8		
	Totals	11	11	Totals	23	20	43	54

Noot: Overgenomen uit Cybersecurity GenAI in de (veiligheids)zorg, Atlas.ti, 4-4-2025

Legenda frequentieverdeling: minst | minder | meer | meest

avans hogeschool

3.2 QUOTE ANALYSE FOCUSGROEPEN EN LITERATUUR

Tabel 2. Frequentie coderingscodes in de categorie mogelijk gebruik: verwachte AI-toepassingen en –ontwikkelingen.

	Veiligheidszorg	Focusgroepen			Literatuur			
		Focusgroep 3 - Cybersecurity GenAI in de Veiligheidszorg Gr=131	subtotal		Literatuur beide Gr=603; GS=10	Literatuur veiligheidszorg Gr=10; GS=85	subtotal	Totals
Zoeken	• Mogelijk gebruik: Zoeken Gr=5	1	1	• Mogelijk gebruik: Zoeken Gr=5			0	1
Taal	• Mogelijk gebruik: Verslaglegging Gr=9	3	3	• Mogelijk gebruik: Verslaglegging Gr=9	2		3	6
	• Mogelijk gebruik: Schrijven Gr=1			• Mogelijk gebruik: Schrijven Gr=1	1			
	• Mogelijk gebruik: Vertalen Gr=4			• Mogelijk gebruik: Vertalen Gr=4				
Begrijpen	• Mogelijk gebruik: Diagnostiek Gr=25	1	6	• Mogelijk gebruik: Diagnostiek Gr=25	1		5	11
	• Mogelijk gebruik: Leren Gr=14	3		• Mogelijk gebruik: Leren Gr=14	3			
	• Mogelijk gebruik: Dossierkennis-EPD Gr=12	2		• Mogelijk gebruik: Dossierkennis-EPD Gr=12	1			
Ondersteuning	• Mogelijk gebruik: Data analyse Gr=3	3	5	• Mogelijk gebruik: Data analyse Gr=3			23	28
				• Mogelijk gebruik: Extende reality Gr=4	4			
				• Mogelijk gebruik: Kwaliteit Gr=10	2			
				• Mogelijk gebruik: Ontwikkeling Gr=6				
				• Mogelijk gebruik: Veiligheid Gr=2	1			
	• Mogelijk gebruik: Besluitondersteuning Gr=2			• Mogelijk gebruik: Besluitondersteuning Gr=2				
				• Mogelijk gebruik: Behandeling Gr=16	5			
	• Mogelijk gebruik: Plannen Gr=5			• Mogelijk gebruik: Plannen Gr=5	1			
	• Mogelijk gebruik: Werkdruk Gr=14	1		• Mogelijk gebruik: Werkdruk Gr=14	2			
				• Mogelijk gebruik: Administratie Gr=16	2	1		
				• Mogelijk gebruik: Kosten Gr=4	2			
	• Mogelijk gebruik: Client Gr=25	1		• Mogelijk gebruik: Client Gr=25	3			
	Totals	15	15		30	1	31	46

Noot: Overgenomen uit Cybersecurity GenAI in de (veiligheids)zorg, Atlas.ti, 16-5-2025

Legenda frequentieverdeling: minst | minder | meer | **meest**

avans hogeschool

3.3 QUOTE ANALYSE FOCUSGROEPEN EN LITERATUUR

Tabel 3. Frequentie coderingscodes in de categorie hindernissen: houden organisaties tegen in het gebruiken van AI-toepassingen.

	Veiligheidszorg	Focusgroep		Literatuur			
		Focusgroep 3 - Cybersecurity GenAI in de Veiligheidszorg Gr=132	subtotal	Literatuur beide Gr=603; GS=10	Literatuur veiligheidszorg Gr=85; GS=10	subtotal	Totals
Sociaal	• Hindernis: Vertrouwen Gr=45	8	11	7	1	9	20
	• Hindernis: Behoefte Gr=9						
	• Hindernis: Niet willen Gr=6	3		1			
Kennis	• Hindernis: Kennis Gr=37	9	10	15	1	30	40
	• Hindernis: Vaardigheden Gr=12	1		4	4		
	• Hindernis: Gebrek aan ervaring Gr=5			5			
	• Hindernis: Niet kunnen Gr=10			1			
Systeem	• Hindernis: Omvang Gr=14	1	7	1		6	13
	• Hindernis: Snelheid ontwikkelingen Gr=16	6		4			
	• Hindernis: Beschikbaarheid Gr=1						
	• Hindernis: Dataset Gr=9						
	• Hindernis: Techniek Gr=13			1			
Besturen/regels	• Hindernis: Regelgeving Gr=65	2	8	43	1	70	78
	• Hindernis: Andere prioriteiten Gr=5	1		2			
	• Hindernis: Geld Gr=12	5		7			
	• Hindernis: Tijd Gr=7			1			
	• Hindernis: Gebrek aan regels Gr=5			4			
	• Hindernis: Ondernemerschap Gr=8			3			
	• Hindernis: Opschalen gebruik Gr=1						
	• Hindernis: Organisatie inrichting Gr=9			1			
	• Hindernis: Privacy Gr=17			4			
	• Hindernis: Veiligheid Gr=7			4			
	Totals	36	36	108	7	115	151

Noot: Overgenomen uit Cybersecurity GenAI in de (veiligheids)zorg, Atlas.ti, 16-4-2025

Legenda frequentieverdeling:

minst	minder	meer	**meest**

3.4 QUOTE ANALYSE FOCUSGROEPEN EN LITERATUUR

Tabel 4. Frequentie coderingscodes in de categorie oplossingen: de manieren om hindernissen aan te pakken.

	Veiligheidszorg	Focusgroep			Literatuur			
		Focusgroep 3 - Cybersecurity GenAI in de Veiligheidszorg Gr=132	subtotal		Literatuur beide Gr=603; GS=10	Literatuur veiligheidszorg Gr=85; GS=10	subtotal	Totals
Sociaal	• Oplossing: Samenwerken Gr=42	2	2	• Oplossing: Mens blijft eindverantwoordelijk Gr=21	13		35	37
	• Oplossing: Interesse Gr=2			• Oplossing: Samenwerken Gr=42	21	1		
Kennis	• Oplossing: Kennis Gr=32	2	2	• Oplossing: Kennis Gr=32	17		27	29
	• Oplossing: Leren gebruiken Gr=17			• Oplossing: Leren gebruiken Gr=17	7			
	• Oplossing: Klein houden Gr=6							
	• Oplossing: Experimenteren Gr=7			• Oplossing: Experimenteren Gr=7	2	1		
Systeem	• Oplossing: Techniek Gr=20			• Oplossing: Techniek Gr=20	12	1	28	28
	• Oplossing: Transparantie Gr=10			• Oplossing: Transparantie Gr=10	3			
				• Oplossing: Standaardisatie Gr=14	12			
Besturen/regels	• Oplossing: Beleid Gr=17	1	1	• Oplossing: Regelgeving Gr=63	41	2	63	64
				• Oplossing: Beleid Gr=17	12			
				• Oplossing: Monitoren Gr=5	1			
				• Oplossing: Opletten Gr=15	6			
				• Oplossing: Afschermen Gr=4	1			
				• Oplossing: Geld Gr=1				
	Totals	5	5	Totals	148	5	153	158

Noot: Overgenomen uit Cybersecurity GenAI in de (veiligheids)zorg, Atlas.ti, 8-5-2025

Legenda frequentieverdeling: minst | minder | meer | **meest**

avans hogeschool

3.5 QUOTE ANALYSE FOCUSGROEPEN EN LITERATUUR

Tabel 5. Frequentie coderingscodes in de categorie risico's: bedreigingen bij toepassen AI in een organisatie.

	Veiligheidszorg	Focusgroep			Literatuur			
		Focusgroep 3 - Cybersecurity GenAI in de Veiligheidszorg Gr=135	subtotal		Literatuur beide Gr=603; GS=10	Literatuur zorg Gr=720; GS=16	subtotal	Totals
Sociaal	• Risico: Sociale ontwikkeling Gr=11	5	6	• Risico: Sociale ontwikkeling Gr=11	10		36	42
	• Risico: Ethiek Gr=6	1		• Risico: Ethiek Gr=6	5	1		
	• Risico: Werkdruk Gr=3			• Risico: Werkdruk Gr=3	1			
				• Risico: Duurzaamheid Gr=8	5	1		
				• Risico: Winstgedrevenheid Gr=20	10	3		
Kennis	• Risico: Verlies van transparantie Gr=22	1	5	• Risico: Verlies van transparantie Gr=22	5	1	62	67
	• Risico: Bias Gr=33	1		• Risico: Bias Gr=33	10	7		
	• Risico: Afhankelijkheid Gr=31	3		• Risico: Afhankelijkheid Gr=31	34			
	• Risico: Verlies van kennis Gr=4			• Risico: Verlies van kennis Gr=4	3			
				• Risico: Menselijke fout Gr=5	2			
Systeem	• Risico: Databescherming Gr=57	4	14	• Risico: Databescherming Gr=57	27	1	203	217
	• Risico: Feitelijke juistheid Gr=46	6		• Risico: Feitelijke juistheid Gr=46	13	8		
	• Risico: Databetrouwbaarheid Gr=32	4		• Risico: Databetrouwbaarheid Gr=32	20	6		
	• Risico: Aanvallen Gr=19			• Risico: Aanvallen Gr=19	16			
	• Risico: Beschikbaarheid Gr=8			• Risico: Beschikbaarheid Gr=8	12	1		
				• Risico: Kwaliteit Gr=8	2	2		
				• Risico: Manipulatie Gr=55	29	18		
				• Risico: Misbruik Gr=16	9	2		
				• Risico: Samenwerking Gr=2				
				• Risico: Veiligheid Gr=62	30	7		
Regels	• Risico: Privacy Gr=53	4	6	• Risico: Privacy Gr=53	29	4	41	47
	• Risico: Non compliance Gr=29	2		• Risico: Non compliance Gr=29	5			
				• Risico: Aansprakelijkheid Gr=6		3		
	Totals	31	31	Totals	277	65	342	373

Noot: Overgenomen uit Cybersecurity GenAI in de (veiligheids)zorg, Atlas.ti, 29-4-2025

Legenda frequentieverdeling:

minst	minder	meer	**meest**

3.6 QUOTE ANALYSE FOCUSGROEPEN EN LITERATUUR

Tabel 6. Frequentie coderingscodes in de categorie maatregelen: aanpakken van AI-risico's.

	Veiligheidszorg	Focusgroep			Literatuur			
		Focusgroep 3 - Cybersecurity GenAI in de Veiligheidszorg Gr=135	subtotal		Literatuur beide Gr=603; GS=10	Literatuur veiligheidszorg Gr=85; GS=10	subtotal	Totals
Sociaal	• Maatregel: Mens blijft eindverantwoordelijk Gr=25	10	15	• Maatregel: Mens blijft eindverantwoordelijk Gr=34	1	1	24	39
	• Maatregel: Samenwerken Gr=17	5		• Maatregel: Samenwerken Gr=29	6	4		
				• Maatregel: Samenwerking Gr=15	7	4		
				• Maatregel: Vertrouwen Gr=15	1			
Kennis	• Maatregel: Educatie Gr=31	6	9	• Maatregel: Educatie Gr=59	10	5	32	41
	• Maatregel: Experimenteren Gr=5	2		• Maatregel: Experimenteren Gr=5				
	• Maatregel: Kennis Gr=4	1		• Maatregel: Kennis Gr=22	2	3		
				• Maatregel: Kwaliteit Gr=66	8	4		
systeem	• Maatregel: Transparantie Gr=31	2	5	• Maatregel: Transparantie Gr=67	11	3	43	48
	• Maatregel: Afschermen Gr=9	3		• Maatregel: Afschermen Gr=10	1			
	• Maatregel: Technologie Gr=29			• Maatregel: Technologie Gr=34	23			
				• Maatregel: Dataset Gr=11	1			
				• Maatregel: Gedistribueerde systemen Gr=2	2			
				• Maatregel: Klein houden Gr=2	1			
				• Maatregel: Opt out Gr=4				
				• Maatregel: Tegenaanval Gr=1	1			
Regels	• Maatregel: Beleid Gr=18	4	8	• Maatregel: Beleid Gr=61	7	1	159	167
	• Maatregel: Regels Gr=35	3		• Maatregel: Regels Gr=138	88	4		
	• Maatregel: Privacy Gr=11	1		• Maatregel: Privacy Gr=25	8	1		
				• Maatregel: Controleren Gr=7	1	1		
				• Maatregel: Managementsysteem/framework Gr=14	12			
				• Maatregel: Monitoring Gr=16	6			
				• Maatregel: Ontwikkeling stimuleren Gr=16	8	2		
				• Maatregel: Organisatieinrichting Gr=32	1	3		
				• Maatregel: Tool Gr=6	5			
				• Maatregel: Toezicht Gr=12	11			
	Totals	37	37	Totals	222	36	258	295

Noot: Overgenomen uit Cybersecurity GenAI in de (veiligheids)zorg, Atlas.ti, 29-4-2025

Legenda frequentieverdeling:

minst	minder	meer	**meest**

BRONNENLIJST

Zorg algemeen

- Boheemen, P. van, Munnichs, G., Kool, L., Diercks, G., Hamer, J., & Vos, A. (2020). Cyberweerbaar met nieuwe technologie: kans en noodzaak van digitale innovatie.
- Brink, N.W.T., Gijsen, B.B.M., Kamphuis, Y.N., Liebergen, N.M., van Opheikens, D.D., Stijn, J.J. van, Wijnja, S. Verkenning van het raakvlak van cybersecurity en AI. (2024)
- Novelli, C., Casolari, F., Hacker, P., Spedicato, G., Floridi, L., Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity,Computer Law & Security Review,Volume 55,2024,106066,ISSN 0267-3649,https://doi.org/10.1016/j.clsr.2024.106066.
- Hamer, J., Kool, L., Hijstek, B., van Eeden, Q., & Das, D. (2023). Generatieve AI: Rathenau Scan.
- Kleij, R. van der, & Hof, T. (2024, June). Why Do Organizations Fail to Practice Cyber Resilience?. In International Conference on Human-Computer Interaction (pp. 126-137). Cham: Springer Nature Switzerland.
- Ministerie van Binnenlandse Zakenen Koninkrijksrelaties. Overheidsbrede visie Generatieve AI. (2024)
- Nieuwenhuizen, W., Hijstek, B., Roolvink, S., & van Huijstee, M. (2023). Immersieve technologieën: Rathenau Scan.
- Piersma, N. (2024). Hyperscenario's van het gebruik van artificiele intelligentie: een essay.
- Stokkum, R. v., Bouwman, J., & Kamstra, R. (2024). Generatieve AI in de Nederlandse zorg. TNO, TNO Healthy Living & Work. Delft: TNO Public. Opgeroepen op januari 29, 2025
- Sutton, A., & Tompson, L. (2025). Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review. Computers & Security, 104110.

Veiligheidszorg

- Bemelmans, J. H. B., & Ligthart, S. (2024). Artificiële delinquentie? Een verkenning van strafrechtelijke aansprakelijkheid voor en van kunstmatige intelligentie in het Nederlands strafrecht. Delikt en Delinkwent, 549- 572. Article DD 2024/37
- Goudsmit Samaritter, M.L.R.; Aksay, R.F.; Oerlemans, J.J. (2023). Strafbaarstelling van seksuele deepfakes. Boom Strafblad, 4(5), 239-247
- Kaur, M., Saini, M. Role of Artificial Intelligence in the crime prediction and pattern analysis studies published over the last decade: a scientometric analysis. Artif Intell Rev 57, 202 (2024). https://doi.org/10.1007/s10462-024-10823-1
- Landman, W. (2024). Samenwerken met politiemachines: politievakmanschap in een tijd van artificiële intelligentie. Justitiële verkenningen, 50(1), 30-46. doi: 10.5553/JV/016758502024050001003
- Prins, C., & van Ettekoven, B.-J. (2023). Artificiële intelligentie en de rechtspraak: Implicaties van de EuropeseAI Act en de noodzaak van een kompas voor toepassing en beoordeling van AI-systemen. Nederlands Juristenblad, 98(36), 3153-3162
- Schuilenburg, Marc; Soudijn, Melvin; ‚AI-criminaliteit: een verkenning van actuele verschijningsvormen, Justitiële Verkenningen,50,1,,2024,Boom Uitgevers Den Haag
- Sloot, B. van der (2024). De impact van AI op de rechtspraak: Is het bewijsrecht klaar voor de 21ste eeuw? Rechtstreeks, 2024(2), 33-40.
- Steen, M. (2024). Ethische aspecten bij het ontwikkelen en toepassen van AI: Een methode voor reflectie en deliberatie. Justitiële verkenningen, 50(1), 109-126.

avans hogeschool