

Digitale

Ethiek

voor
veiligheidsregio's

Position Paper - November 2025

Inleiding

Veiligheidsregio's gebruiken steeds vaker nieuwe technologieën zoals Artificiële Intelligentie (AI), virtuele en geaugmenteerde reality (VR en AR) en sensoren. Ook maken zij steeds meer complexe analyses vanuit bestaande en nieuwe databronnen en gebruiken zij algoritmen om hun werk beter te doen. Deze technologieën en gecombineerde datasets bieden kansen, maar kunnen ook op gespannen voet raken met publieke waarden zoals privacy, autonomie, transparantie en vertrouwen in de overheid. Deze nieuwe technologieën zijn vaak minder zichtbaar, werken op mondiale schaal en nemen in toenemende mate zelfstandig beslissingen of beïnvloeden menselijk gedrag. Daardoor worden de ethische vragen urgenter en complexer. Digitale ethiek helpt om technologie verantwoord in te zetten en het vertrouwen van burgers en partners te behouden. Deze paper laat zien waarom digitale ethiek belangrijk is en hoe veiligheidsregio's hier richting aan kunnen geven.

Waarden aan het werk, digitale ethiek als kompas



Brutus, de blusrobot is een voorbeeld van een innovatieve oplossing op basis van nieuwe technologie die inmiddels al niet meer weg te denken is bij de brandweer.



Steeds meer technologie helpt veiligheidsregio's hun kerntaken uit te voeren. Met digitale ethiek zorgen we voor transparantie en veilig gebruik.

Wat is digitale ethiek?

Ethiek draait om *het goede doen*. Digitale ethiek gaat dus om het goede doen met data en digitale technologieën. Waarden spelen een centrale rol: ze helpen ons bepalen of we het juiste doen.

Digitale ethiek maakt waarden transparant en onderzoekt hoe nieuwe data of technologie deze waarden beïnvloeden – positief of negatief. Via dialoog worden afwegingen gemaakt en handelingsperspectieven ontwikkeld om ervoor te zorgen dat data en technologie zó ingezet wordt dat het bijdraagt aan waar wij als organisatie voor staan, en om nadelige effecten te beperken. Digitale ethiek helpt dus in het maken van keuzes, waarbij er niet geredeneerd wordt vanuit de nieuwe technologische mogelijkheden zelf, maar vanuit de bijdrage dat het levert aan wat onze organisatie belangrijk vindt. Daarbij is het belangrijk om een brede groep stakeholders te betrekken, waarbij soms verder gekeken moet worden dan alleen naar medewerkers van de veiligheidsregio.



Ethische vragen worden
urgenter en complexer



Waarom is digitale ethiek belangrijk?

Vaak wordt gedacht dat technologie neutraal is, maar dat is niet het geval. Zonder bewuste afweging kunnen technologieën onbedoeld effecten hebben die ethisch ongewenst zijn, zoals:

- Aannames (bias) en discriminatie in AI-modellen
- Verlies van autonomie als besluitvormers te veel vertrouwen op algoritmes
- Privacy problemen door cameratoezicht of datadeling

Door ethiek vanaf het begin mee te nemen in technologie- en dataprojecten, worden risico's zoals discriminatie, uitsluiting, onterechte afhankelijkheid van technologie of verlies van transparantie vroegtijdig gesignaleerd en kunnen oplossingen direct worden ingebouwd (*ethics by design*). Dit versterkt de publieke waarden én behoudt het vertrouwen van burgers en partners.



Veiligheid en
gezondheid

Samenwerking

Solidariteit

Betrouwbaarheid

Slagvaardigheid

Aandacht voor digitale ethiek

Digitale ethiek is nog jong en volop in ontwikkeling. Toch besteden steeds meer (overheids)organisaties er aandacht aan. Binnen het programma Interbestuurlijke Datastrategie (IBDS)^[1] is een Community of Practice (CoP) gestart met overheids- en uitvoeringsorganisaties, waarin ook de veiligheidsregio's meedoen. Samen werken deze organisaties aan digitale ethiek.

Uit gesprekken met verschillende ketenpartners zoals gemeenten, waterschappen en politie zien we dat ook zij aandacht besteden aan digitale ethiek. Ketenpartners die direct contact hebben met de burger richten vaak een ethische commissie in waar burgers ethische dilemma's neer kunnen leggen. Bij andere ketenpartners zien we juist meer ontwikkeling richting het ethisch begeleiden van data en technologische trajecten en het opstellen van waardenkaders om zo gericht keuzes te maken. Zo zien we dat veel gemeenten een ethiek coördinator hebben aangesteld (vaak binnen de CIO office), en hebben de waterschappen een bestuurlijk waardenkader voor AI ontwikkeld.^[2]

“ Waarden helpen om verantwoorde keuzes te maken bij nieuwe technologieën ”

^[1] De Interbestuurlijke Datastrategie (IBDS) is databeleid voor de hele overheid dat interbestuurlijk tot stand kwam. Het is op 18 november 2021 aan de Tweede Kamer aangeboden:

[Interbestuurlijke Datastrategie Interbestuurlijke datastrategie - Digitale Overheid](#)

^[2] [AI-kompas-unie-van-waterschappen.pdf](#)

Waarden als kompas

Binnen de overheid zijn waarden al bekend via de algemene beginselen van behoorlijk bestuur (ABBB), waarin waarden zoals zorgvuldigheid, gelijkheid, transparantie, rechtszekerheid en evenredigheid een belangrijke rol spelen. Sinds 2025 is er bovendien het landelijke waardenkader voor goed digitaal bestuur, het CODIO [3]. Dit waardenkader is gebaseerd op de fundamentele democratie, rechtsstaat en bestuurskracht, uitgewerkt in 32 waarden zoals non-discriminatie, uitlegbaarheid, privacy en inclusie. Sommige waarden zijn zo fundamenteel dat ze wettelijk worden beschermd. De Europese AI-verordening (AI Act) is daar een goed voorbeeld van. Deze wet stelt strikte eisen aan het gebruik van AI in hoog-risico toepassingen, juist om kernwaarden te waarborgen zoals non-discriminatie, transparantie, veiligheid en gezondheid, privacy en menselijke autonomie. Er is een handreiking ontwikkeld dat veiligheidsregio's helpt om deze wetgeving goed in de praktijk toe te passen. [4]

Ook de veiligheidsregio's werken vanuit waarden. Uit een analyse van de websites en regionale risicoprofielen van de 25 veiligheidsregio's blijkt dat de volgende waarden vaak specifiek benoemd worden (in volgorde van hoe vaak ze genoemd worden):

- *Veiligheid en gezondheid*: een bijdrage leveren aan de veiligheid en gezondheid van de bewoners en bezoekers in hun regio
- *Samenwerking*: intensief samenwerken met andere regio's en partners in de keten
- *Solidariteit*: verbonden zijn met de samenleving en vraagstukken samen met burgers en maatschappelijke groepen oppakken
- *Betrouwbaarheid*: burgers en medewerkers moeten erop kunnen vertrouwen dat hulpverlening goed en zorgvuldig wordt uitgevoerd
- *Slagvaardigheid*: snel, doeltreffend en met overtuiging handelen wanneer dat nodig is



De veiligheidsregio's benoemen dus al waarden in hun strategische communicatie uitingen, en deze zijn ook zeer geschikt als sturing bij het gebruik van nieuwe technologieën.

[3] [Het CODIO-instrument | Rapport | Rijksoverheid.nl](#)

[4] (35) [Post | LinkedIn](#)

Waarden zijn een moreel kompas: idealen waar organisaties naar streven. Soms botsen waarden met elkaar en ontstaan er ethische dilemma's, ook wel waardenspanningen genoemd. Een voorbeeld is het gebruik van drones die brandhaarden detecteren en beelden doorsturen naar de meldkamer: die bieden snel overzicht bij branden (innovatie), maar kunnen door storingen of verkeerde detecties tot risico's leiden (zorgvuldigheid). Een andere bekende waardenspanning is snelheid versus samenwerking: "alleen gaan we sneller", maar "samen doen we het beter". Ook kunnen waardenspanningen ontstaan door nieuwe ontwikkelingen: door de huidige geopolitieke situatie zien we steeds meer de spanning tussen het afhankelijk zijn van Microsoft producten (autonomie) versus het gebruik van opensource producten (transparantie). **Digitale ethiek helpt om zulke spanningen bij nieuwe data of digitale ontwikkelingen zichtbaar te maken en af te wegen.**



Waardenspanning

Digitale ethiek bij innovatietrajecten

Hieronder volgen twee voorbeelden die laten zien hoe ethische aspecten een rol spelen tijdens innovatietrajecten bij de veiligheidsregio's.

AI beslishulpen

Veiligheidsregio's experimenteren met verschillende op AI gebaseerde tools om besluitvorming bij incidenten in crisisbeheersing en brandweer te ondersteunen. Dit zijn AI-toepassingen die bijvoorbeeld taalmodellen gebruiken om patronen te ontdekken in informatie rondom een incident, of om relevante (preparatieve) informatie op te zoeken. Op basis daarvan geven ze een waarschuwing of advies aan de verantwoordelijke besluitvormer.

Het voordeel is dat beschikbare informatie, zowel binnen als buiten de organisatie, beter benut kan worden, wat kan leiden tot betere beslissingen. Tegelijkertijd roept dit ethische vragen op:

- Welke datasets worden gebruikt en hoe zijn die samengesteld? Is de data ethisch verkregen, zitten er onbedoeld vooroordelen in de datasets?
- Zijn er aannames (bias) ingebouwd in de algoritmen die tot vertekening kunnen leiden?
- Hoe transparant is de weging van gegevens en de totstandkoming van adviezen?
- Wat betekent dit voor de autonomie van de besluitvormer, blijft er voldoende ruimte om eigen ervaring en expertise mee te laten wegen?

Deze vragen raken waarden als doelmatigheid, betrouwbaarheid, transparantie en autonomie. Door hier al vroeg aandacht aan te besteden, kunnen maatregelen worden genomen om risico's te beperken. Denk aan technische eisen voor transparantie en traceerbaarheid van de tool, maar ook aan extra training voor de gebruikers.

Gebruik van camerabeelden

Daarnaast experimenteren Veiligheidsregio's ook steeds vaker met camerabeelden voor vroege branddetectie en tijdens inzetten. Soms wordt hierbij ook AI-beeldherkenning gebruikt. De voordelen zijn duidelijk: brand kan sneller worden ontdekt, de schade kan worden beperkt en het situatiebeeld tijdens een inzet wordt beter. Dat leidt niet alleen tot een effectievere inzet, maar ook tot meer veiligheid voor het eigen personeel.

Tegelijkertijd zijn er belangrijke ethische vragen:

- Leggen de camera's per ongeluk ook beelden vast van mensen in de omgeving?
- Wat gebeurt er met deze beelden, en wie krijgt er toegang toe?
- Mogen andere partijen, zoals verzekeraars, de beelden ook gebruiken?

Deze vragen raken vooral de waarden privacy en rechtszekerheid. Door deze dilemma's al in een vroeg stadium te signaleren, kunnen passende maatregelen worden genomen, zoals het maken van duidelijke afspraken over opslag en toegang tot beelden. Ook kan er communicatie richting de burgers opgestart worden waarin wordt uitgelegd waarom en hoe de technologie wordt gebruikt.



Naar een digitaal ethische VR

Digitale ethiek is niet alleen van belang bij innovaties, maar ook in het dagelijkse werk van alle medewerkers die met data en technologie omgaan. Vaak beloven medewerkers van de veiligheidsregio in hun ambtseed om te werken voor het algemeen belang. Daarom is het essentieel dat zij de juiste kennis en hulpmiddelen hebben om te herkennen wanneer het gebruik van data of technologie (onvoorzien) negatieve effecten kan hebben op publieke waarden. Medewerkers moeten digitaal vaardig én bewust zijn van ethische kwesties.

Omdat digitale ethiek nog relatief nieuw is en zich continu ontwikkelt, is sprake van een groeipad. In de volgende tabel schetsen we de verschillende volwassenheidsfases van een digitaal ethische organisatie, met bijbehorende kenmerken en acties. Daarna geven we een aantal concrete stappen die veiligheidsregio's kunnen nemen op het gebied van digitale fitheid, het gebruik van hulpmiddelen en borging in de organisatie.

Volwassenheidsfase	Kenmerken	Acties
Bewustwording	Ethiek komt ad hoc ter sprake. In de organisatie worden vragen gesteld of iets "de bedoeling is". Mensen weten niet waar ze naar toe moeten met vragen	Houden van trainingen, workshops of communicatiecampagnes ter bevordering van bewustwording
Toepassing	Ethische instrumenten (DEDA, Begeleidingsethiek, opleidingen) worden projectmatig en in de lijn gebruikt	Verplichte ethische toets bij (innovatie)projecten
Borging	Digitale ethiek is structureel ingebed in governance en cultuur van de afzonderlijke veiligheidsregio's en de gezamenlijke voorzieningen	Instellen van een coördinator ethiek, maturity monitoring, instellen ethische commissies

Bewustwording (fase 1): Medewerkers digitaal vaardig en bewust

Net zoals brandweerpersoneel eerst leert hoe een brandweerslang werkt voordat zij een inzet doen, moeten medewerkers van de veiligheidsregio's leren verantwoord om te gaan met data en digitale technologie. Dit is geen eenmalige actie, maar vraagt om voortdurende aandacht. Belangrijke onderdelen kunnen zijn:

- Basistraining: een (verplichte) e-learning over ethiek bij onboarding.
- Opleidingsaanbod: een vaste ethiekmodule in het opleidingsprogramma, bijvoorbeeld via de Nationale AI-cursus. [\[5\]](#)
- Technologie specifieke risico's: bewustwording van thema's zoals betrouwbaarheid, transparantie en bias bij AI.

- Kennisnetwerken: werkgroepen rond specifieke technologieën (zoals Copilot) om gezamenlijk af te wegen of het gebruik past bij publieke waarden.
- Data-ethiek versterken: extra aandacht binnen BI- en datateams.
- Regelmatige communicatie: blijvende aandacht voor ethiek in interne kanalen.

[5] [De Nationale AI-Cursus - AI voor iedereen! Gratis online leren.](#)

Toepassing (fase 2)

Bij data- en technologie trajecten wordt al vanaf het begin rekening gehouden met ethische aspecten, dit heet ook wel ethics by design. Er zijn verschillende hulpmiddelen beschikbaar, zoals:

- Begeleidingsethiek (ECP): helpt om tijdens een project of toepassing systematisch waarden en dilemma's te bespreken met alle betrokkenen.^[6]
- DEDA, de Ethische Data Assistent (Universiteit Utrecht): een vragenlijst en werkvorm om de ethische kanten van dataprojecten te verkennen en vast te leggen.^[7]
- Toolbox ethisch verantwoorde innovatie (Digitale Overheid): biedt praktische handvatten, stappenplannen en voorbeelden om ethiek in innovaties te borgen.^[8]
- Value Sensitive Design: een ontwerpbenadering waarbij waarden van gebruikers en stakeholders vanaf het begin worden meegenomen in de technologie-ontwikkeling.^[9]
- Moreel Beraad: een gestructureerd gesprek waarin medewerkers samen een ethisch dilemma onderzoeken en handelingsopties verkennen.^[10]

Borging (fase 3)

Borging op regionaal en landelijk niveau is nodig om digitale ethiek duurzaam te verankeren. Regionaal betekent dit dat digitale ethiek een vast onderdeel wordt van beleid, besluitvorming en opleidingen binnen de veiligheidsregio's. Landelijk vraagt het om afstemming, kennisdeling en gezamenlijke werkwijzen. De volgende activiteiten horen bij borging, deze kunnen zowel regionaal als landelijk relevant zijn:

- Het onderwerp ethiek opnemen in de beleidsplannen
- Het aanstellen van een coördinator ethiek
- Ingerichte processen om ethiek te borgen
- Ethische commissies

[6] [Home - Begeleidingsethiek](#)

[7] [De Ethische Data Assistent \(DEDA\) | De Ethische Data Assistent \(DEDA\)](#)

[8] [Toolbox Ethisch Verantwoorde Innovatie Toolbox Ethisch Verantwoorde Innovatie - Digitale Overheid](#)

[9] [7.1 Introduction to Value Sensitive Design - TU Delft OCW](#)

[10] [moreel-beraad-DEF.pdf](#)



Het is nú het moment
om te starten met digitale ethiek



Aanbevelingen

Digitale ethiek staat nog in de kinderschoenen bij de veiligheidsregio's. Toch is nú het moment om te starten, zodat nieuwe technologieën en datatoepassingen vanaf het begin passen bij onze maatschappelijke opdracht en publieke waarden. Digitale ethiek hoeft geen rem te zijn, maar kan ook kansen bieden: het stelt ons in staat de best passende keuzes te maken over hoe we technologie en data willen toepassen bij de veiligheidsregio.

Hierbij geven we een aantal aanbevelingen waarmee we samen kunnen werken aan een digitaal ethische veiligheidsregio:

- **Vergroot ethisch bewustzijn over data en nieuwe technologieën:** via leermodules digitale ethiek en door het gesprek over ethiek standaard onderdeel te maken van nieuwe projecten. Deze activiteiten passen goed in het kader van de “digitaal fitte organisatie”
- **Veranker digitale ethiek in beleid:** neem ethiek op in landelijke en regionale (informatie)beleidsplannen.
- **Werk met ethics by design:** integreer ethiek vanaf de start van technologie- en dataprojecten. Dit geldt voor zowel landelijke als regionale projecten.
- **Investeer in expertise:** leid medewerkers binnen de veiligheidsregio's op tot begeleiders van ethische workshops. Vanuit de ervaringen vanuit het project “Ethiek bij de veiligheidsregio's” wordt voorgesteld om te starten met Begeleidingsethiek en DEDA.
- **Bouw een community of practice:** verbind deze begeleiders bovenregionaal voor kennisdeling en versterking.
- **Borg op strategisch niveau:** de huidige ontwikkelingen rondom het inrichten van een landelijke CIO-office voor de veiligheidsregio's, maar ook daarop aansluitende regionale CIO offices bieden een kans voor de borging van digitale ethiek. Benut deze (landelijke en regionale) CIO-offices als spil voor de coördinatie, bewaking van waarden en het verbinden van digitale ethiek met leiderschap
- **Borg ethiek binnen het Masterprogramma IV 2025 - 2030:** ethische vraagstukken zijn relevant binnen de meeste programmalijnen van het masterprogramma IV 2025 – 2030, omdat hier veel innovaties plaats vinden met nieuwe technologieën. Zorg ervoor dat er goede ethische afwegingen plaats vinden bij deze ontwikkelingen.

Opgesteld door project “Ethiek bij de Veiligheidsregio's” van het programma IV 2020 - 2025,
in samenwerking met iNowit, november 2025.

Generatieve AI is gebruikt ter ondersteuning van de leesbaarheid van deze tekst.