



KENNISCENTRUM
EUROPA
DECENTRAAL

Interviewserie Digitalisering

Decentrale overheden & digitalisering in de praktijk

Samenvatting

Blockchain, big data en de opkomst van artificiële intelligentie laten zien dat digitale technologie volop in ontwikkeling is. Dit kan overheden helpen bij het uitvoeren van hun taken maar het creëert ook bepaalde afhankelijkheden. Kenniscentrum Europa Decentraal ging in gesprek met mensen die beroepsmatig bezig zijn met digitalisering en vroegen naar het gebruik van nieuwe technologie in de publieke sector, de impact van digitalisering op dienstverlening en de uitwerking van Europese regelgeving op dit vlak.

Kernwoorden: digitalisering, Digital Decade, digitale overheid, Artificiële Intelligentie wet, Digitale Markten Wet, NIS2-richtlijn, cyberveiligheid, good governance

Inhoudsopgave

Introductie	3
Verbondenheid & verantwoordelijkheid: Sebastiaan van 't Erve, cyberburgemeester van Lochem, over digitalisering bij de overheid	4
Meer dan alleen een zak geld: Erwin Altena van Oost NL over het stimuleren van digitalisering met EU-project INDUSTRI_14.0	7
Digitale veiligheid als speerpunt: Iris Meerts, cyberburgemeester van Wijk bij Duurstede, over digitaliseringsuitdagingen	12
De menselijke digitale overheid: Prof. Sofia Ranchordás over burgerrechten en digitalisering	14
Dreigingen, urgentie & realisme: Let's Get Digital 3.0 sprekers over cyberveiligheid binnen decentrale overheden	18

Introductie

Digitalisering is zonder enige twijfel het snelst ontwikkelende beleidsterrein in Europa. Blockchain, big data en de opkomst van artificiële intelligentie (AI) laten zien dat technologie volop verandert. Dit biedt niet alleen kansen voor bedrijven maar ook voor overheden en publieke organisaties. Digitalisering kan dienstverlening en contact met burgers namelijk veel efficiënter en effectiever maken.

Deze digitale manier van werken gaat echter ook gepaard met risico's vanwege de toenemende verzameling en snellere verwerking van data. Dit leidt tot privacyvraagstukken en cyberveiligheidskwesties, die door toenemende cybercriminaliteit en geopolitieke veranderingen steeds meer op de voorgrond treden. De wetgevingsinstellingen van de Europese Unie (EU) staan daarom zeker niet stil. Nieuwe wetgeving reguleert deze en andere technologie en verhoogt de cyberveiligheid van de gehele Unie. Hiermee kunnen de lidstaten gewogen stappen nemen om digitaliseringskansen te benutten en -risico's te mijden. Veelbesproken wetten als de AI-verordening, de Digitale Markten Wet en de NIS2-richtlijn komen hierdoor volop in de spotlight.

Ook voor decentrale overheden is dit uitermate belangrijk. Nieuwe digitale technologie kan decentrale overheden helpen met uitvoeren van hun taken. Zo kunnen gemeenten bijvoorbeeld gebruik maken van algoritmes om uitkeringen sneller uit te betalen en kunnen waterschappen *digital twins* inzetten om de effecten van klimaatverandering op het grondwaterpeil te simuleren.

Deze voorbeelden laten de potentie van digitalisering zien, maar illustreren tegelijkertijd de eerdergenoemde uitdagingen op het vlak van gegevensbescherming. Bij beide processen worden er wordt er met gevoelige data gewerkt zoals geolocatie (adressen), namen en rekeningnummers. Het is belangrijk om deze persoonsgegevens te beschermen. Daarnaast kan het gebruik van digitale technologie ook op technisch vlak voor uitdagingen zorgen. Gemeenten zijn immers niet meer in staat om uitkeringen uit te betalen zonder deze technologie, terwijl inwoners dit geld wel nodig hebben. De kansen die digitalisering biedt, brengen dus ook afhankelijkheden met zich mee.

Niemand heeft hier beter zicht op dan de mensen in het veld. Daarom ging Kenniscentrum Europa Decentraal in deze interviewserie in gesprek met mensen die zich beroepsmatig met digitalisering bezighouden. Wij richtten ons hierbij op de maatschappelijke impact van digitalisering en nieuwe technologie, waarbij er specifiek aandacht is voor de balans tussen kansen en risico's.

Verbondenheid & verantwoordelijkheid: Sebastiaan van 't Erve, cyberburgemeester van Lochem, over digitalisering bij de overheid

Sebastiaan van 't Erve is sinds 2014 burgemeester van Lochem en sinds kort is hij ook officieel benoemd als cyberburgemeester. KED sprak Van 't Erve vanwege zijn inzet op het gebied van cyberveiligheid bij Nederlandse gemeenten.

Wat is je klik met digitalisering?

Digitalisering was voor mij altijd al een soort hobby, maar toen de gemeente Lochem werd gehackt in 2019 kwam het ineens heel dichtbij. Dit was een desastreuze hack waarbij we moesten ingrijpen door het hele IT-systeem. We waren genoodzaakt het gehele systeem te laten gaan en opnieuw op te bouwen. Na de hack ben ik mij gaan verdiepen in de onderwerpen digitalisering en cyberveiligheid.

Als burgemeester ben ik verantwoordelijk voor de openbare orde en veiligheid in mijn gemeente. Cyberveiligheid is voor mij hier een belangrijk onderdeel van. Daarnaast ben ik sinds begin 2023 lid van de adviesgroep van ENISA. Hoewel ik werk voor de Nederlandse overheid, vertegenwoordig ik deze niet bij de adviesgroep. Ik zit daar vanuit mijn kennis over de digitaliseringsopgave. Ik draag bij door mijn ervaringen te delen. Zo hoop ik de digitale weerbaarheid van Nederland en de EU te vergroten.

Hiernaast zit ik nog in de Commissie Bestuur en Veiligheid van de VNG, waar ik de portefeuillehouder digitale veiligheid ben. Verder ben ik

bezig met onderzoek als buitenpromovendus. Mijn promotieonderzoek gaat over cybercrisismanagement door Nederlandse gemeentes. Ik maak mij hard voor de principiële politieke keuzes die we moeten maken. Maar ook dat deze daadwerkelijk gemaakt worden. Uiteindelijk

**“Iedereen was betrokken maar
niemand was verantwoordelijk.”**

gaat het om normen en waarden en dat is een klassiek politiek gesprek dat we met elkaar moeten voeren, alleen nu toegepast op digitalisering. Eigenlijk gaat het over het borgen van de rechten van de individuen van mensen zoals jij en ik.

Wat zijn hedendaagse uitdagingen op het gebied van digitalisering?

De bestuurlijke uitdaging van deze tijd op het thema digitalisering is hoe we de beleidspraktijk van gemeenten weten te verbinden met wat er speelt op regionaal, nationaal en Europees niveau. Ik merk in Nederland dat het digitale ecosysteem niet optimaal werkt. De verschillende overheidslagen en de Europese Unie worden niet genoeg met elkaar verbonden en er wordt niet voldoende van elkaar geleerd. Je merkt dat in Nederland verkokering heerst. Wat van de provincies is, is van de provincies; van de waterschappen blijft bij de waterschappen; en de gemeenten houden het bij de gemeenten. Tegelijkertijd zit juist in die samenwerking de meerwaarde.

Het overstijgen van deze verkokering is één van de belangrijkste stappen die Nederland en de EU kunnen zetten om cyberveiliger te worden. Het moet makkelijker worden om van verschillende

overheidslagen te leren, maar ook van verschillende landen. Nederland moet gaan kijken hoe andere landen zijn omgegaan met cyberaanvallen en proberen hier lessen uit te trekken.

Dit is moeilijk omdat voor veel mensen digitale veiligheid een ver-van-mijn-bed-show blijft. Mensen worden pas gemotiveerd als ze zelf zijn geraakt, maar dan is het eigenlijk al te laat. Hier waren wij als gemeente ook geen uitzondering op. Ik wil graag voorkomen dat anderen hetzelfde probleem krijgen dat wij een paar jaar geleden hadden. Hiervoor zullen alle overheden door de gehele EU sneller en slimmer van elkaar moeten leren.



De hack op gemeente Lochem heeft mij laten inzien hoe moeilijk het is om zo'n crisis te managen als burgemeester, maar ook hoe lastig de overheid het nog vindt om met crises om te gaan en correct te handelen. Iedereen was namelijk wel betrokken, maar niemand was verantwoordelijk. Als het systeem plat zou gaan in Nederland is er momenteel niet één iemand eindverantwoordelijk, maar iedereen is nu enkel voor zijn eigen stukje verantwoordelijk. Oftewel, als het een verantwoordelijkheid

is van ons allemaal, is niemand verantwoordelijk. Hierdoor is er geen slagkracht en missen we leiderschap.

Dit is ook een uitdaging in het licht van de hedendaagse geopolitieke verhoudingen. Vanuit Rusland is er momenteel veel criminele activiteit. Er worden pogingen gedaan vanuit het buitenland om Europese systemen binnen te dringen. Dan heb ik het nog niet eens over de aanwezigheid van China in de digitale wereld. Ditzelfde geldt ook voor de Verenigde Staten. Deze steeds dreigendere en ingewikkeldere situatie zou alarmbellen moeten laten rinkelen, want onze digitale soevereiniteit komt mogelijk in het geding. Toch merk ik dat dit gesprek maar beperkt wordt gevoerd.

Wat is hierbij de rol voor gemeentes en Nederland?

De cyberveiligheidsopgave is in mijn opzicht niet iets dat decentrale overheden alleen moeten of kunnen oppakken, maar juist iets wat Nederland en de EU als geheel moeten aanpakken. Nederland heeft nu weinig veerkracht tegen cyberaanvallen dus het is echt heel interessant om te kijken hoe kennis en kunde uit verschillende sectoren met elkaar kan worden verbonden.

Het is daarom ook belangrijk onderzoeksinstituten, bedrijven en alle overheidslagen samen te brengen. De VS en China gaan al op deze manier om met AI, door investeringen en privaat-publieke samenwerking voorop te stellen in het ontwikkelen van deze technologie. De EU moet hiervan leren en kijken hoe zij met nieuwe technologie kan omgaan op een manier die aansluit bij haar principes.

Wat we daarvoor hard nodig hebben is meer digitaal leiderschap. Waar mogelijk probeer ik dit zelf in te zetten binnen gemeentes, maar ik denk dat het belangrijk is om dit centraal op te pakken. Het is cruciaal wat het kabinet gaat doen en of er bijvoorbeeld een minister van digitale zaken komt. Hier moeten wij als overheid zijnde beter over na gaan denken en het anders gaan invullen.

Een verantwoordelijke aanwijzen is hierbij noodzakelijk, zodat er ook daadwerkelijk verantwoordelijkheid genomen kan worden. Het is belangrijk dat er iemand aan het roer staat en beslissingen kan nemen. Dit is in het huidige politieke Nederland alleen niet zo gemakkelijk, want alles lijkt er op gericht te zijn om juist verantwoordelijkheid van zich af te schuiven en elders en lager te benoemen. Ik zie dat op veel plekken de verantwoordelijkheden eerder worden doorgeschoven dan dat ze worden opgenomen en juist op dit digitale thema is het belangrijk dat de verantwoordelijkheid gelijk wordt opgepakt.

“Mensen worden pas gemotiveerd als ze zelf zijn geraakt, maar dan is het eigenlijk al te laat.”

In mijn opzicht is het doel hiervan toe te werken naar digitale soevereiniteit. Ik noemde dit eerder al. Hiermee bedoel ik: in hoeverre zijn wij als Europa in staat onze eigen broek op te houden en is het mogelijk om software en diensten te gebruiken, waarvan we zeker

weten dat andere actoren niet meelesen? Hierbij moeten we dus rekening houden met andere landen, maar ook met grote bedrijven.

Wat is de boodschap die jij graag mee wil geven aan medeburgemeesters, collega's en anderen?

Digitalisering is een wereld die snel ontwikkelt en die nieuwe kansen biedt. Het is nu alleen zo snel gegaan dat we eigenlijk de basisvraag zomaar aan ons voorbij hebben laten gaan: 'Hebben we nou de Rechten van de Mens voldoende beschermd?'. Ik denk dat wij als overheid en bestuur opnieuw deze principiële politieke vraag moeten oppakken door erbij stil te staan en hier de balans in op te maken.

Verder wordt de grote opdracht voor de komende tijd wat mij betreft het creëren van digitale soevereiniteit. Er moet een agenda gemaakt worden om samenhang te creëren, bijvoorbeeld om tot een Europees investeringsprogramma te komen of een Europese server op te zetten die aan de Europese principes voldoen. Het wordt nu echt tijd dat deze principes daadwerkelijk geformuleerd en benoemd worden en dat we er ook naar gaan handelen.

Meer dan alleen een zak geld: Erwin Altena van Oost NL over het stimuleren van digitalisering met EU-project INDUSTR_I4.0

Hoe kun je bedrijven stimuleren om de digitale transitie te versnellen? En hoe neem je daarbij de ondernemingen mee die juist geen koploper zijn, maar zich eerder in het peloton bevinden? Het zijn kwesties waar overheden regelmatig mee te maken krijgen. Oost NL, de Regionale Ontwikkelmaatschappij (ROM) voor Oost-Nederland, lanceerde hiervoor het Europese project INDUSTR_I4.0. Het doel is om 200 ondernemers uit het MKB in de grensregio financieel te ondersteunen bij hun haalbaarheidsstudies en innovatieprojecten op het gebied van digitalisering. Het project kwam mede tot stand met financiering van het Europese subsidieprogramma Interreg Deutschland-Nederland. KED wilde er meer van weten en sprak met Erwin Altena, projectmanager tech bij Oost NL en projectleider van INDUSTR_I4.0.

Wat is het idee achter het project INDUSTR_I4.0?

Het project INDUSTR_I4.0 is een fonds dat financiering biedt voor de digitale transitie van de (maak)industrie: industrie 4.0, ook wel Smart Industry genoemd. Zo financiert het haalbaarheidsstudies, innovatieprojecten en verkenningen van grensoverschrijdende samenwerking tussen Duitse en Nederlandse partners. Het project richt zich daarbij juist niet op bedrijven die voorlopers zijn op het gebied van digitalisering, maar juist op de bedrijven die zich 'in het peloton' bevinden, dus die al wel gestart zijn, maar 'in de middenmoot' zitten.

Uit onderzoek tijdens een eerder project van Oost NL bleek namelijk dat het gat tussen de kopgroep en het peloton steeds groter wordt.

Oost NL is de regionale ontwikkelingsmaatschappij voor Oost-Nederland. Het versterkt de regionale economie in de provincies Overijssel en Gelderland door met publiek geld te investeren in Oost-Nederlandse ondernemers, met name in de topsectoren Food, Energy,

Health, Tech en Circular Economy.

Altena: "Vroeger gingen we vaak uit van 'backing the winners', dus vooral inzetten op de koplopers, dan trekt de rest wel bij. Maar in beleidskringen komt steeds meer het besef dat dit niet altijd werkt; dat je een bredere groep



moet stimuleren en wellicht ook op een andere manier. Met dat idee zijn we aan de slag gegaan met INDUSTR_I4.0. In ons project willen we ons echt richten op dat peloton, zodat bedrijven in die groep ook technologie gaan inzetten, gaan gebruiken en gaan adopteren." Dan gaat het bijvoorbeeld niet over het ontwikkelen van een geheel nieuw AI-protocol, maar wel over de toepassing van AI om bedrijfsprocessen verder te vernieuwen.

De focus van INDUSTRI_14.0 ligt op industrie, met de maakindustrie voorop. “Maar digitalisering is bij uitstek een thema dat sector overstijgend is. We zijn een breed en open programma, we sluiten geen sectoren uit van deelname”, aldus Altena. Daarmee is het fonds complementair aan de European Digital Innovation Hubs (EDIH’s). De EDIH’s vormen een netwerk van innovatiehubs in Europa, die digitalisering van het MKB en van de regionale economie moeten versnellen en verbreden. “Aan hun kennis, ondersteuning en netwerk voegen wij een financieringsinstrument toe in de grensregio.” Samenwerking tussen Nederlandse en Duitse partners is een vereiste binnen INDUSTRI_14.0. Het project bedient bedrijven in de hele grensregio, van Groningen tot Limburg en loopt tot 2027.

“In ons project willen we ons richten op het peloton, niet op de voorlopers.”

Financiering van digitalisering en innovatie, dus. Welke concrete mogelijkheden bieden jullie daarvoor aan bedrijven?

Naast haalbaarheidsstudies en innovatieprojecten biedt INDUSTRI_14.0 ondersteuning voor de verkenning van Duits-Nederlandse samenwerking tussen bedrijven. “Dit traject is bedoeld voor bedrijven die nooit eerder iets hebben gedaan met Interreg, die nog geen ervaring hebben met het buurland en die dan met een heel kleine startsubsidie een eerste stap kunnen zetten. Ze worden dan gekoppeld aan een van onze partners”, legt Altena uit. Zo kan een Nederlands bedrijf de haalbaarheid van een samenwerking verkennen met potentiële Duitse bedrijven, krijgt het inzicht in de mogelijkheden

van het buurland en kan het eventueel een beurs bezoeken en visa versa. Daarna wordt er gekeken hoe de volgende stap in de samenwerking gezet kan worden.

Dat zulke verkenningen belangrijk zijn, leerde Oost NL tijdens eerdere projecten waarin de verbinding met Duitse bedrijven werd gezocht. “Daarbij was er vanuit de Duitse kant best wel koudwatervrees. In de Duitse cultuur moet je eerst vertrouwen krijgen, veel koffiedrinken, elkaar beter leren kennen, voordat er echt serieus samengewerkt kan worden aan een innovatieproject. Daarom doen we dit als een eerste stap. Het is ook een stok achter de deur voor die bedrijven om echt wat te gaan doen.”

Altena legt uit dat er voor de kleinere bedragen vereenvoudigde verantwoordingsprocedures gelden en er gewerkt wordt met lumpsums. “Dat was in het begin wel spannend: hoe gaan we daarmee om? We willen zoveel mogelijk een laagdrempelig programma hebben voor het bedrijfsleven, maar hoe controleer je ze dan en hoe zorg je ervoor dat er geen misbruik van het geld wordt gemaakt? Daar hebben we goed over moeten nadenken. We hebben veel geluk dat we collega’s met veel subsidie-ervaring hebben en een aantal juristen die meekijken of we dat goed doen.”

Jullie ontvangen financiering vanuit Interreg, het Europese financieringsinstrument voor grensoverschrijdende samenwerking. Maar INDUSTRI_14.0 is anders dan een gemiddeld Interreg-project. Kun je daar iets meer over vertellen?

“We hebben de cascadefinanciering opgezet binnen Interreg volgens best een unieke formule, namelijk een kleinprojectenfonds”, zegt Altena. Zo’n kleinprojectenfonds (KPF) is een constructie binnen Inter-



(Ko-)financierd von
der Europäischen Union
(Mede) gefinancierd
door de Europese Unie

Deutschland – Nederland

KPF INDUSTRI_14.0

wijze verdeelt. Minimaal 80% van het budget moet rechtstreeks naar het bedrijfsleven gaan. Altena: “Een kleinprojectenfonds is eigenlijk bedoeld om een instapticket te bieden voor organisaties. Dus het moet een versimpelde versie zijn van het programma.”

“Een kleinprojectenfonds is bedoeld om een instapticket te bieden voor organisaties.”

De constructie van een kleinprojectenfonds leent zich volgens Altena bij uitstek voor het experimenteren met alternatieve vormen van financiering, omdat het een gecontroleerde setting biedt. “Als je concept niet werkt dan heb je binnen dat project wel wat schade, maar heb je veel kennis opgedaan die je weer kunt inzetten bij het Interreg-programma of in de volgende programmaperiode.”

Oost NL heeft ruime ervaring met het helpen en financieren van bedrijven. Waar letten jullie op bij het opzetten van zo'n programma?

Altena komt terug op het belang van laagdrempeligheid: “Hoe zorgen we ervoor dat we een stimuleringsprogramma bieden en niet een zwaar ‘blok aan je been programma’ met heel veel regels waar uiteindelijk het mkb-bedrijf en het bedrijfsleven niet mee gediend zijn. Om een brede groep aan te spreken, moet je het aantrekkelijk genoeg maken. En dat is meer dan alleen maar een zak geld. Een zak geld aanbieden kan iedereen. Je moet goed nadenken over wat je de bedrijven wilt aanbieden, hoe wil je hen helpen om de volgende stap te zetten.”

Altena vertelt vervolgens over de aanpak die bij een eerder Europees project is ontwikkeld. “Daarin hebben we veel bedrijven geholpen, maar wel op een manier waarbij het voor ondernemers zo simpel mogelijk was. Dat hebben we de SOFA Approach genoemd: een Service Oriented Funding Approach.” Bij deze aanpak ga je na waar de kracht en zwakte van de bedrijven ligt en beperk je de administratielast. Dat is belangrijk voor het mkb, zeker als de focus ligt op een doelgroep die niet dagelijks met subsidies bezig is. Daar komt volgens Altena ook steeds meer besef voor.

Bij INDUSTR_I4.0 gaat ook het beheer van het project met de tijd mee. Zo kunnen partijen een filmpje uploaden als toevoeging op een projectplan en mogen ze ChatGPT en andere producten inzetten voor het projectplan.”

Zijn er obstakels geweest bij het opzetten van het project?

Altena legt uit dat een kleinprojectenfonds, volgens de regels van Interreg, maar door één partij kan worden aangevraagd. Maar het project INDUSTR_I4.0 bedient het bedrijfsleven in het hele programmagebied van Interreg Deutschland-Nederland, veel groter dan de regio van Oost NL.

“Dat was best een struikelblok. Als Oost NL zouden we dat niet alleen kunnen dragen, want we hebben geen kennis over de ontwikkelingen in Groningen, laat staan dat we weten wat er in bijvoorbeeld Nedersaksen gebeurt.” Daarom deed Oost NL de aanvraag alleen, maar bereidde het een Europese aanbesteding voor om toch andere partijen te betrekken. In Nederland waren de partners snel gevonden via het landelijk dekkend netwerk van ROM's. In Duitsland, waar zo'n netwerk niet bestaat, lag dat anders. “Daardoor was het een zoektocht.

Er zijn bijvoorbeeld Duitse kennisinstellingen aangesloten die veel samenwerken met het bedrijfsleven, iets wat in Duitsland veel voorkomt.”

Tijdens het aanbestedingstraject is ervoor gekozen om een publiek samenwerkingsverband op te zetten met de deelnemende partijen. Het publieke samenwerkingsverband is de enige begunstigde van het fonds. Altena: “Dat was gunstig omdat we zo al voordat de regels (van het subsidieprogramma) bekend waren, toch met een soort van consortium aan de start stonden.” De partners hebben allemaal ervaring met Interreg. Dat laatste was een bewuste keuze, om zo optimaal te kunnen schakelen met bedrijven. Altena: “Eén van de doelstellingen van het project is om ook nieuwkomers in de industrie een kans te geven. Je moet enige ervaring hebben, wil je zo'n nieuwkomer over de streep kunnen trekken.”

De constructie van een publiek samenwerkingsverband had nog een voordeel, namelijk een transparante en niet-discriminerende begeleiding van voorstellen geborgd kon worden. Altena: “Het regionale belang moet voorop staan, niet een eventueel commercieel belang van een op winst gericht adviesbureau. Dat allerlei commerciële bedrijven een aanvraag doen, prima. Dat er allerlei adviseurs zijn die daarmee helpen, dat is ook prima. Alleen voor het kernconsortium gaan deze belangen niet samen. Waar het gaat om een transparante selectie van voorstellen, zoals de regeling ook voorschrijft, zou het algemene belang altijd boven het commerciële belang moeten gaan, iets wat we met een publieke samenwerking kunnen borgen.”

Eind april is INDUSTR_I4.0 opengegaan voor aanmeldingen. Hoe kijk je terug op het aanlooptraject en wat is jullie verwachting voor de toekomst?

Altena is trots op het neerzetten van een kleinprojectenfonds: “Niet elke organisatie zal geschikt zijn een dergelijk fonds op te zetten, maar hopelijk hebben we een weg gebaad voor andere organisaties die een soortgelijke rol hebben als wij. Aan de achterkant is het best een complexe puzzel geweest, je moet er wel voor zorgen dat de ervaring er is om dat te doen. Wij hebben nu een programma neergezet dat in de ontwikkeling veel tijd heeft gekost. Nu het eenmaal staat wordt het hopelijk een heel plezierig programma voor het bedrijfsleven, dat zich ook makkelijk laat uitleggen aan hen.”

Dat blijkt wel uit de vliegende start die het project heeft gemaakt: binnen een week was de eerste aanmelding al binnen, de reacties, bijvoorbeeld op social media, zijn positief en de agenda staat vol met gesprekken. Dankzij de ondersteuning door INDUSTR_I4.0 kunnen bedrijven in het digitaliseringspeloton nu de demarrage inzetten en het gat met de kopgroep dichtrijden.

Digitale veiligheid als speerpunt: Iris Meerts, cyberburgemeester van Wijk bij Duurstede, over digitaliseringsuitdagingen

Als cyberburgemeester heeft Iris Meerts (burgemeester Wijk bij Duurstede) een sterk speerpunt: de digitale veiligheid van Nederlandse decentrale overheid moet verhogen. Dagelijks verneemt ze in haar gemeente van DDos-aanvallen en pinpasfraudes, maar ziet ze dat het voor gemeenten een lastige opgave is om hun organisatie te digitaliseren. KED sprak haar over haar rol als cyberburgemeester, de uitdagingen van digitalisering, en vroeg haar om tips voor decentrale overheden.

Als voormalig medewerker van de afdeling European Affairs in Rotterdam staat Europees recht en beleid hoog bij u in het vaandel. Is dat bij andere gemeenten ook het geval?



“Voor zover ik weet leeft Europa niet echt bij de middelgrote en kleine gemeenten. Dat heeft voornamelijk twee redenen. Ten eerste heeft ‘Brussel’ weinig aandacht voor de uitvoerbaarheid van Europees beleid op lokaal niveau. Lang

leve het werk dat het Comité van de Regio’s voor ons verricht, maar

we zijn er nog lang niet. Ten tweede, gemeenten hebben vaak andere prioriteiten dan het in de gaten houden van Europese ontwikkelingen. Ze zijn bezig met overleven, zo simpel is het. Het is ook lastig hoor, vooral het onderwerp cyberveiligheid. Als burgemeester krijg ik bijvoorbeeld wel gegevens over woningbraken en fietsendiefstallen, maar niets over de cybercrime. De gemeente Wijk bij Duurstede geeft digitale veiligheid wel prioriteit in het veiligheidsbeleid, maar als we er niets over weten, kunnen we er onvoldoende mee.”

Hoort bij uw rol als cyberburgemeester de agendasetting van cyberveiligheid bij gemeenten?

“Ja, dat is nodig. Ik werd cyberburgemeester omdat ik me vanuit mijn vorige rol flink verbaasde over uitspraken als “het komt wel”, “dat ligt niet bij mij” en “ik heb al zoveel op mijn bordje”. Veel collega’s vonden daarnaast dat cyberveiligheid de verantwoordelijkheid is van het Rijk. Dat is begrijpelijk: het is technisch en complex en voor velen een reden om het voor zich uit te schuiven. Voor mij staat wel urgentie voorop. Sinds de oorlog in Oekraïne krijgen wij namelijk in de gemeente vier keer per dag te maken met DDOS-aanvallen op onze vluchtelingengroep, hacks dus. Ik voel daardoor sterk de verantwoordelijkheid om digitale veiligheid hoog op de agenda te zetten. Ik heb er alle vertrouwen in dat dat – misschien soms op termijn – zijn vruchten af gaat werpen. Stoppen is dan ook geen optie, want het wordt alleen maar meer.”

Hoe zorgt u ervoor dat medewerkers inzien dat cyberveiligheid een taak voor elke ambtenaar is?

“De kwaliteit van onze dienstverlening vraagt dat we 24/7 up and running en veilig zijn. Wanneer je het over de kwaliteit van de dienstverlening hebt, snapt iedereen het. Dan gaat het namelijk over

beleidsvoering: dat is van ons allemaal, daar zijn we voor aangenomen. In feite draait het daar ook om. Het gaat niet zozeer om welke technische tools je gebruikt; het gaat erom dat die dienstverlening veilig en betrouwbaar moet zijn.”

Ziet u in de begroting prioritering van cyberveiligheid of digitalisering terug?

“Nee, we hebben en krijgen te weinig geld hiervoor, terwijl je op gemeentelijk niveau veel kunt regelen. Er kan basisinfrastructuur aangelegd worden die veilig is en privacy respecteert. Dan hoef je de hele discussie over autonomie van gemeenten echt niet te voeren. De kleinere gemeentes kunnen het gewoon echt niet alleen. Dat vervolgens aangrijpen om maar te zeggen dat ‘die kleintjes’ dan te klein zijn voor hun wettelijke taak en maar moeten fuseren, vind ik een beetje flauw.”

Hoe zorgt u ervoor dat die decentrale overheden alsnog met hun digitale veiligheid aan de slag gaan?

“Een leuk initiatief hiervoor zijn de ‘peer-to-peergesprekken’ waar de VNG een tijdje geleden mee begonnen is. Dat zijn gesprekken met twee willekeurige gemeenten en een cyberburgemeester als gespreksleider. Per gemeente zitten een burgemeester, gemeentesecretaris, openbare orde- en veiligheidsadviseur, een Chief Information Security Officer (CISO), en nog wat anderen bij elkaar. In die gesprekken gebeurt vaak iets bijzonders. Iedereen ziet er een beetje tegenop, want het is lastige materie, maar je moet het er met elkaar over hebben. Dan merk je dat je in je eigen kamer eerst ongemakkelijk met de CISO praat, omdat die technische taal gebruikt en bestuurders vaak dingen zeggen waar de CISO weer weinig van begrijpt. Bij de andere gemeente gaat het vervolgens precies hetzelfde. Zo wordt het

uiteindelijk een erg leuk gesprek. Er komen altijd leuke dingen uit die ze van elkaar leren en er worden altijd vervolgspraken gemaakt. Die olievlek proberen we uit te spreiden.”

“Peer-to-peergesprekken tussen gemeenten beginnen vaak een beetje ongemakkelijk, maar blijken achteraf altijd nuttig te zijn.”

“Daarnaast werkt in Wijk bij Duurstede de inzet van een digitale wijkagent. Hij heeft bevoegdheden om op sociale media opsporingen te doen; ik mag dat bijvoorbeeld niet. Hij kijkt vooral naar strafbare feiten die bijvoorbeeld via smartphone of websites worden gepleegd. De reguliere wijkagenten komen daar niet aan toe. De digitale wijkagent komt bij iedereen die gehackt is even langs om te kijken en te praten. Daar zijn we hartstikke blij mee.

Als laatste tip aan gemeenten: praat met je CISO. Bestuurders en CISO's zijn volgens mij nog niet overal goed in gesprek. Dat praten met die CISO kan bijvoorbeeld ook tijdens oefeningen van cyberdreigingen. Dat is trouwens ook een goede tip: oefeningen doen. Zo ben je beter voorbereid als het een keer echt gebeurt. En als het dan een keer wel fout gaat, vertel het verhaal dan. Je schaamt je er misschien voor, maar gooi het toch open, want je moet het van elkaar weten. Dan zien bestuurders in dat dit echt gebeurt en dus ook bij hen kan gebeuren. Werk aan de winkel dus!”

De menselijke digitale overheid: Prof. Sofia Ranchordás over burgerrechten en digitalisering

Professor Sofia Ranchordás is hoogleraar bestuursrecht bij Tilburg University. Ze benadert digitalisering vanuit het perspectief van inclusie en kwetsbaarheid. Zo komen de rechten van burgers die in aanraking komen met de digitaliserende overheid op haar pad. KED sprak haar en vroeg naar haar bevindingen over decentrale overheden en digitalisering.

Hoe bestudeer je digitalisering? Is alle ingezette digitale technologie door decentrale overheden bijvoorbeeld artificiële intelligentie (AI)?

Ik kijk naar digitalisering vanuit de positie van de burger, waarbij ik focus op digitale inclusie en uitsluiting. Ik ben geïnteresseerd in hoe digitale technologie bestaand ongelijkheden vergroot.

Informatie stond vroeger 'op papier', maar dat hebben we nu gedigitaliseerd. We gaan er veelal vanuit dat deze informatie hetzelfde is en op dezelfde manier overkomt, maar dat is niet zo. Zo is het online aanvragen van toeslagen anders dan het aanvragen met pen en papier. Burgers hebben bepaalde digitale vaardigheden nodig om de juiste stappen te doorlopen.

De meeste overheden gebruiken momenteel redelijk eenvoudige vormen van automatisering, met geringe inzet van AI. Soms gebruikt de overheid niet meer dan een algoritme in een Excel Sheet. Dit begint nu echter te veranderen. In de toekomst zullen decentrale overheden steeds meer AI om processen zoals het uitbetalen van toeslagen te automatiseren. Ik bestudeer de inzet van digitale technologie in de

publieke sector in de brede zin, zodat ik ook deze nieuwe vormen van digitalisering en automatisering kan meenemen.

Waar een decentrale overheid kan opschalen, kom je meer toepassingen van AI of *machine learning* tegen. Daarin probeer ik voornamelijk vast te stellen welke impact dit heeft op de verhouding tussen burger en overheid. De beginselen van algemeen behoorlijk bestuur geven uiteraard richtlijnen voor hoe besluiten vormgegeven moeten worden, maar deze moeten opnieuw geïnterpreteerd worden in het kader van nieuwe uitdagingen door digitalisering en ontwikkeling. Ik onderzoek hoe we de verhouding overheid-burger in lijn kunnen brengen met die beginselen.

Op welke manieren beïnvloedt de EU dit proces?

Het recht van de Europese Unie geeft kaders voor automatisering en digitalisering. Het eerste belangrijke kader hiervoor werd vastgelegd in de Algemene Verordening Gegevensbescherming (AVG), die grenzen stelde aan de automatisering van persoonsgegevensverwerking in besluitvorming. Deze verordening beperkte de mogelijkheden tot automatisering voor overheden en bedrijven.

De AI-verordening geeft hier een soort tegenreactie op. Deze verordening geeft ons nu namelijk een belangrijk kader om te begrijpen hoe we de besluitvorming kunnen automatiseren en AI kunnen inzetten op allerlei gebieden zonder daarmee mensen en burgerrechten te schaden.

In de eerste versie van de AI-verordening waren heel veel overheden uitgesloten, vrijgesteld van toepassing. Na bekendmaking van de toeslagenaffaire is dat op internationaal niveau veranderd. Ineens

werd de verordening ook van toepassing op decentrale overheden, bijvoorbeeld op gemeenten, wanneer zij algoritmen inzetten voor opsporing.

Deze twee voorbeelden laten zien hoe de EU actief bezig is met kaders uitzetten waarop technologie ingezet kan worden. Uiteraard zijn andere verordening en jurisprudentie van het Hof van Justitie van de Europese Unie ook van belang voor de regulering van digitale technologie.

Je recente inaugurele rede ging over de overheid empathischer maken door middel van digitalisering. Hoe kan de overheid dit bewerkstelligen?

Empathisch besturen betekent in de eerste plaats vereenvoudigen. Dit houdt in dat je de omgang met de burger vereenvoudigt door op een andere, meer empathische manier te communiceren. Momenteel maakt empathie nog niet echt onderdeel uit van het Europees recht als zodanig. Dit zou in mijn ogen juist wel zo moeten zijn. We moeten het meer over empathie hebben.

Empathie werkt namelijk vanuit twee kanten. Enerzijds is het belangrijk dat burgers begrijpen dat gemeenten geen oneindige middelen hebben. Anderzijds moet de gemeente zich in de burger kunnen verplaatsen. Het is belangrijk om te kunnen begrijpen wat het met mensen doet wanneer ze langdurig kampen met problemen, zoals ziekte en armoede. Mensen die met schaarse middelen te maken hebben, zullen namelijk niet altijd de beste oplossingen en beslissingen kunnen nemen en gaan hierdoor ook niet altijd even rationeel om met bureaucratie.

Waar gaat het mis tussen de burger en de overheid?

Het jeugdrecht is een van de voorbeelden waar het heel vaak misgaat. Er is hier namelijk sprake van zogenaamde beschikkingsarmoede, waarbij de gemeente te weinig middelen en capaciteiten tot haar beschikking heeft om alle aanvragen te beantwoorden en vervolgens vaak helemaal niet reageert. Deze beschikkingsarmoede heeft dus tot gevolg dat burgers zich niet gezien voelen door het bestuursorgaan. Burgers wachten heel lang, krijgen niks, maar weten vervolgens vaak te weinig om hier verder op te reageren. Dit leidt weer tot frictie.

“We moeten het meer over empathie hebben.”

Zit er verschil in de mate van empathie tussen de rijksoverheid en decentrale overheden?

Een goed voorbeeld van empathie en reacties op het gebrek eraan, is de begintijd van de aardbevingenproblematiek in Groningen. Groningers gingen gebukt onder de neveneffecten van de aardbevingen zoals beschadigde huizen en emotioneel lijdende families. Hierbinnen moesten de provincie en gemeente Groningen druk uitoefenen op de Rijksoverheid om de situatie te veranderen en laten zien dat ze aan de kant van de burger stonden. Zo zou het ook moeten zijn. Het lijkt logisch of aannemelijk dat gemeentes in principe meer empathie hebben voor burgers dan de rijksoverheid: ze staan

tenslotte dichterbij. In het algemeen zie ik dit alleen nog te weinig. Als decentrale overheid sta je het dichtst bij de burger, en de vertegenwoordigers van de gemeente worden gekozen door hun eigen inwoners. Dit betekent dat de burger ook empathie van de gemeente verwacht. Aangezien Den Haag ver van de meeste burgers afstaat, zou je een duidelijk verschil met de nationale overheid verwachten. Momenteel is dit verschil echter nog heel minimaal.

“De grootste uitdaging wordt gevormd door het systeem dat mensen het gevoel hebben er niet bij te horen.”

Is empathie de grootste uitdaging op digitaliseringsvlak voor Nederland of zijn er ook andere uitdagingen?

Volgens mij is de grootste uitdaging dat Nederland een systeem heeft gecreëerd waar mensen het gevoel hebben dat ze er niet bij horen. Nederland is informeel digital by default [digitaal als standaard, zonder wettelijke verplichting, red.]. Als je een dienst probeert te bereiken met telefoon, moet je lang in de wacht staan en word je niet altijd even goed geholpen. AI worden deze middelen officieel nog steeds aangeboden, je krijgt er als burger weinig voor terug. De offline dienstverlening is dus niet gelijkwaardig aan online. Vanuit lopend juridisch onderzoek is gebleken dat burgers niet altijd goed behandeld worden door deze alternatieve offline diensten.

Als Nederland *digital by default* is, betekent dit dat veel mensen niet mee kunnen doen. Een vierde van de Nederlanders heeft moeite met digitalisering en het uitoefenen van hun rechten, om allerlei redenen. 20% van de Nederlandse bevolking kan bijvoorbeeld niet goed lezen en schrijven. Het gaat niet alleen om nieuwkomers, maar ook om mensen die in Nederland zijn geboren en getogen, maar een beperking hebben of op leeftijd zijn. Nederland moet ervoor zorgen dat het begrijpt wie er mee kan doen en wat te doen met de mensen die het dreigt buiten te sluiten. Je kunt mensen niet uitsluiten van uitoefening van hun rechten.

Voor de meerderheid regelt Nederland alles goed, maar met 20/25% van de Nederlandse bevolking gaat het niet goed. Deze mensen hebben het gevoel niet gezien te worden. Ze hebben niet alleen maatwerk nodig, maar moeten ook worden gezien als individuen met hun eigen kenmerken, niet als groep. Het probleem is dat we denken dat het goed gaat met de meerderheid, en we dus op dezelfde voet verder kunnen. Deze denkwijze sluit te veel mensen uit en verklaart ook het dalen van het vertrouwen van de Nederlandse burger in de overheid.

Gaat artificiële Intelligentie de menselijk besluitvorming in overheden overnemen?

De overheid zou zeker AI kunnen inzetten om besluitvorming te ondersteunen. De discussie over de inzet van AI om mensen te helpen leeft. Bij grootschalige besluiten heeft AI een deel van de besluitvorming dan ook al overgenomen. Deze inzet zal waarschijnlijk uitbreiden. Echter zal AI de discretionaire bevoegdheden door de overheid nog niet volledig invullen. Artificiële intelligentie zal

ongetwijfeld veel meer processen creëren en dat is maar goed ook, vanwege onze menselijke biases [vooroordelen, red.].

Wat kunnen decentrale overheden doen?

Decentrale overheden zouden meer met burgers moeten spreken. Op zijn minst zouden zij het gesprek moeten blijven voeren met organisaties die burgers in kwetsbare posities helpen. Iedereen kan immers in een kwetsbare positie terecht komen. Verder moet de AI-geletterdheid van ambtenaren ontwikkelen. De AI-verordening verplicht hier ook toe. Manieren vinden om dit te bereiken zou op de agenda's van decentrale overheden moeten staan. De digitale geletterdheid is in het algemeen al laag; de AI-geletterdheid is nog lager. Daarom zouden decentrale overheden meer trainingen voor hun ambtenaren moeten verzorgen en daarvoor middelen reserveren. Op zijn minst moeten alle medewerkers die AI gebruiken een cursus AI-geletterdheid krijgen.

Kortom, meer begrip en meer opleiding over digitalisering en automatisering is nodig om burgers en bestuursrechtelijke besluitvorming gericht op elkaar aan te laten sluiten. Zo sluiten we niemand buiten.

Dreigingen, urgentie & realisme: Let's Get Digital 3.0 sprekers over cyberveiligheid binnen decentrale overheden

Digitalisering is inmiddels onmisbaar in het dagelijkse leven van Europeanen, maar cyberveiligheid is net zo belangrijk voor een betrouwbaar digitaal Europa. Hoe kunnen de decentrale overheden hieraan bijdragen?

Tijdens het Let's Get Digital evenement over cyberveiligheid ging KED in gesprek met Frank Heijligers (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties), Vincent Lokin (Unie van Waterschappen), Gemma Jansen (Provincie Noord-Holland), Patrick Spigt (Gemeente Katwijk) en Folkwin Poelman (NEXIS) om te weten te komen hoe zij naar dit onderwerp kijken.

Hoe groot is de urgentie van cyberveiligheid binnen uw werkveld?

Volgens Patrick Spigt, Directeur Dienstverlening en Bedrijfsvoering Gemeente Katwijk, is de urgentie van cyberveiligheid binnen de overheid groot. "Je ziet dat er de afgelopen jaren een toename is van aanvallen, ook richting gemeentes, en dat dit tot problemen leidt. Dat geeft een zekere urgentie. Ik denk dat we de afgelopen 5 jaar al behoorlijk geïnvesteerd hebben als je kijkt naar alle gemeentes bij elkaar, maar de risico's veranderen exponentieel waardoor je ook veel meer moet gaan investeren om dat bij te kunnen houden. De urgentie is dus groot en wordt de komende jaren alleen maar groter."

Dit wordt beaamd door Folkwin Poelman, programma-coördinator bij NEXIS, het Nationaal Coördinatiecentrum voor Cyberveiligheids-innovatie. "Je ziet steeds meer cyberaanvallen en cybercriminaliteit. Aanvallers worden steeds inventiever, daarom moet je zelf ook inventiever worden om cyberaanvallen enerzijds tegen te houden en anderzijds, als je bent aangevallen, te zorgen dat je gegevens veiliggesteld worden en de risico's beperkt worden."



Ook Vincent Lokin, bestuurslid van Waterschap De Dommel en de Unie van Waterschappen, deelt de mening dat de urgentie zeer hoog is. "De dreigingen zijn er namelijk al. Bepaalde ontwikkelingen zijn voor iedereen onontkoombaar, daar moeten we als overheid in mee en ook wat mee willen. Die ontwikkelingen brengen risico's met zich mee. Het is volgens mij zaak om voortdurend in de gaten te houden wat er gebeurt en er iets van te leren om die risico's voortdurend op orde te hebben."

Frank Heijligers, van Ministerie van BZK, Directoraat-Generaal Digitalisering en Overheidsorganisatie Directie Digitale Samenleving, ziet ook in zijn werk dat veel partijen urgentie ervaren. “Deels zie ik binnen cyberveiligheid met name de urgentie in eenduidigheid. Iedereen ziet het belang van cyberveiligheid als zodanig, maar wil tegelijkertijd te veel eigen keuzes maken. Dat pakt soms minder handig uit. Daarnaast vind ik dat we meer om ons heen moeten kijken. De wereld verandert, de dreigingen veranderen mee, en dat is zorgwekkend.”

Wat zou de rol van decentrale overheden moeten zijn binnen cyberveiligheid?

Gemma Jansen, Chief Information Security Officer (CISO) bij de Provincie Noord-Holland, vindt dat de provincies een grote rol hebben binnen het gebied van cyberveiligheid. “Provincies hebben een belangrijke rol op een aantal maatschappelijke onderwerpen, zoals wonen en milieu, maar wij beheren ook daadwerkelijk operationele technologie. Dus ik denk dat het heel belangrijk is dat wij de centrale overheid daarin goed ondersteunen en versterken. Samenwerking is daarvoor belangrijk.”

Naast de provincies is Patrick Spigt van mening dat ook de gemeenten een grote rol spelen binnen cyberveiligheid. “Een gemeente heeft ontzettend veel taken, is ook het dichtst bij de burger en dus ook het meest zichtbaar als er bijvoorbeeld iets misgaat. Desondanks wordt de gemeente vaak ook het meest vertrouwd door diezelfde burger. Dat maakt het cruciaal dat we als gemeenten met elkaar ervoor zorgen dat we die burger ook zo goed mogelijk beschermen, als het gaat om data, maar ook om processen en alle andere dingen die gebeuren in gemeenten.”

Frank Heijligers beaamt dat decentrale overheden een relevante rol spelen. “Decentrale overheden beheren een deel van de gegevens in hun context. Daar geldt net zoals voor de centrale overheid voor dat je daar zorgvuldig mee om moet gaan. Ik zou het als burger oncomfortabel vinden als mijn gemeente minder zorgvuldig zou omspringen met mijn gegevens dan een andere gemeente. Dat is aan geen enkele burger uit te leggen.”

“Iedereen ziet het belang van cyberveiligheid, maar wil tegelijkertijd te veel eigen keuzes maken.”

Vincent Lokin vindt dat de rol van decentrale overheden niet anders is dan elke andere organisatie. “Ze moeten in de gaten houden wat er gebeurt, de kansen daarvan in proberen te zien en niet te naïef zijn in de risico’s die daarbij horen. Ik zie nu meer dat mensen denken van ‘goh, dit is niet helemaal duidelijk, straks doe ik iets verkeerd dus dan doe ik maar helemaal niets.’ Dat kan niet.”

Gemma Jansen deelt die mening. “Als organisatie moet je die vooruitgang faciliteren en organiseren - we gaan dat niet tegenhouden. Als je zegt ‘we doen er niet aan mee’ dan sta je direct met 10-0 achter. Dan gaat het sowieso niet vliegen.”

Nieuwe technologieën zoals artificiële intelligentie: risico of kans voor cyberveiligheid?

Patrick Spigt ziet nieuwe technologieën als kans maar ook als risico voor cyberveiligheid. “Het is een kans om zaken versneld beter te beveiligen maar aan de andere kant, de kant van de boeven, zitten natuurlijk ook mensen die dat gebruiken en die dus makkelijker aanvallen kunnen uitvoeren op gemeentes. Je moet er mee gaan oefenen, je moet er echt dingen mee gaan doen zodat je weet wat er kan komen. Het is dus zoeken naar een balans waarbij AI kan helpen, om bijvoorbeeld de nieuwe software, applicaties, en systemen ook goed te beveiligen.”

“100% veiligheid bestaat niet.”

Gemma Jansen pleit voor realisme, maar roept vooral op om aan de slag te gaan. “Nieuwe technologieën zoals AI bieden zeker kansen, maar 100% veiligheid bestaat niet. Dat is een gegeven. Het is niet stom dat je als organisatie nog niet zoveel gedaan hebt met nieuwe technologieën. Met digitalisering zijn we pas een jaar of 30, 40 bezig. Het is dus helemaal niet gek dat we op het gebied van digitalisering staan waar we staan. Het is misschien ingewikkeld, het is veel en in detail, maar begin er wel aan. En ga stap voor stap, dat is het recept voor succes.”



KENNISCENTRUM
EUROPA
DECENTRAAL

Contact met Europa Decentraal

info@europadecentraal.nl

www.europadecentraal.nl

De dienstverlening van Kenniscentrum Europa Decentraal beperkt zich tot het verlenen van eerstelijns advies. Wij kunnen geen bindende en gedetailleerde uitspraak doen. Wel kunnen we proberen u aan de hand van relevante informatie verder op weg te helpen. Als u toch behoefte heeft aan een volledig juridisch advies om meer zekerheid en duiding te verkrijgen voor uw specifieke situatie kunt u overwegen een juridisch adviesbureau in te schakelen.