

GOVERNANCE, TOEZICHT EN I OVERHEID

Twee recente boeken en een wat ouder boek, Ze behandelen interessante sturingsvragen in het publieke domein. Hans Hoek neemt ons mee in de geheimen van de governance in de gezondheidszorg, Ferdinand Mertens in (zijn grote ervaring op het vlak van) het toezicht en de WRR in de zich snel ontwikkelende wereld van de iOverheid. Voor de vakbroeders niet te missen literatuur.



Hans Hoek (2007). *Governance & Gezondheidszorg – private, publieke en professionele invloeden op zorgaanbieders in Nederland*. Assen: van Gorcum.

In dit proefschrift neemt Hans Hoek ons mee in vijf delen en zestien hoofdstukken mee in de wereld van de governance van de gezondheidszorg zoals hij deze heeft waargenomen. In deel één een verkenning van het veld, gevolgd door deel twee waarin het begrip governance uiteen wordt gezet, de methodologische verantwoording en de theorie wordt geformuleerd. Dat levert drie overlappende governance-werelden en daarmee moraliteiten op, namelijk de publieke, de private en de professionele werelden. In deel drie worden drie cases besproken, terwijl in deel vier de theorie en praktijk bij elkaar komen. In deel vijf komen we bij de conclusies. De governance zou ertoe moeten dienen maatschappelijke problemen te voorkomen. De praktijk leert dat dit door de strijdigheid van de governance-werelden niet zondermeer vanzelfsprekend is. Terwijl de keuze voor één ook de oplossing niet zal brengen. Het gaat erom de juiste balans te vinden bij de inzet van de governance-werelden. De promovendus eindigt met adviezen over hoe die balans gevonden kan worden. Voor iedere manager en controller in de gezondheidszorg een proefschrift dat goed te lezen is en handige en praktische adviezen geeft over te maken keuzes in de governance rond zijn organisatie.



Ferdinand Mertens (2011). *Inspecteren, toezicht door inspecties*. Den Haag: Sdu.

Het boek is geschreven tegen de achtergrond van wat de auteur de crisis in het toezicht noemt. Maatschappelijk lijkt het beeld te bestaan dat de overheid haar burgers en bedrijven zo veel mogelijk ruimte moet geven en zo weinig mogelijk lastig moet vallen met regels en het toezicht op de handhaving ervan. Tegelijkertijd wordt die zelfde overheid erop aangekeken dat ze te weinig toezicht heeft gehouden als zich kleine of grote rampen voordoen.

Het boek bestaat uit twee delen. In het eerste deel worden de functies van toezicht, de ontwikkeling en samenhang, de systematiek en modellen, de organisatie en structuur en de methode en werkwijze uiteengezet. In het tweede deel wordt de praktijk van het toezicht heel levendig beschreven aan de hand van de Bijlmerramp, het onderwijs, de scheepvaart, veetransporten, de zorg en de delfstoffenwinning.

Ferdinand Mertens is zeer gezaghebbend in het domein van het toezicht door de vele functies die hij er in de loop der jaren succesvol vervulde zowel praktisch als wetenschappelijk. Voor iedereen die zich met toezicht bezig houdt is het een leerzaam en zeer toegankelijk boek.

Duidelijk wordt in ieder geval dat er de afgelopen decennia veel beweging is in de manier waarop toezicht wordt uitgeoefend, terwijl de wetenschap eigenlijk pas sinds ruim veertig jaar hard werkt aan het inzicht in de verschillende perspectieven op toezicht. Dat er een meervoudige relatie is tussen vertrouwen en toezicht wordt goed uiteengezet en praktisch hanteerbaar gemaakt. De risicobenadering die de samenleving de afgelopen jaren domineert en zich ook vertaalt in wetgeving kent ook zijn beperkingen, zo wordt de lezer duidelijk gemaakt. Hoe dan ook is toezicht een functie die in sociale systemen vervuld (moet) word(en)t. De toezichthouder is een intelligente organisatie. Kennis is de driver en dus ook kennisverwerving. Systemen kennen hun beperkingen, zowel in wat ze zijn als wat ze beschrijven. De essentiële kenmerken van de toezichthouder zijn: transparantie (met gevoel voor de werking van het systeem), materiaal leveren voor een geïnformeerd gesprek in het systeem, een goed samenspel met de media en de politiek. Prachtig, goed leesbaar boek voor de geïnteresseerde lezer.

WRR (2011). *iOverheid*. Amsterdam: Amsterdamse University Press.

De WRR heeft een zeer lezenswaardig advies geschreven. Natuurlijk kennen we de risico's van de digitalisering op het technische vlak, hoewel de Diginotar-affaire dat in twijfel doet trekken. Dit keer adviseert de WRR over de iOverheid in de iSamenleving. Het advies bestaat uit drie delen, negen hoofdstukken en een epiloog. Het eerste deel biedt de inleiding en het onderzoekskader. De gehanteerde beginselen worden geordend in stuwende (veiligheid, effectiviteit en efficiency), verankerende (privacy en keuzevrijheid) en procesmatige beginselen (accountability en transparantie), waarbij de afweging troef is. Elke situatie stelt andere eisen. Het tweede deel betreft de empirische analyse waarin de aansturing van de eOverheid, het beleid en de eRealiteit worden besproken. Wanneer ben je deze markt meester? Wie zijn en wat is de rol van de controleurs (Raad van State, College Bescherming Persoonsgegevens, Nationale Ombudsman, Algemene rekenkamer, en rechterlijke macht)? Het derde deel bevat de analyse en de aanbevelingen. Geadviseerd wordt tot een paradigmawisseling van de eOverheid naar de iOverheid.

De Wikileaks-affaire laat zien welke risico's we ook als individuele burgers lopen als ongecontroleerd informatie op straat komt te liggen. Burgers lopen steeds vaker tegen systemen en informatie op waar ze zich niet adequaat tegen heeft kunnen wapenen. Terwijl de bewijslast wel bij hen neer gelegd lijkt te worden.

Een op informatieniveau verknoopte overheid heeft zich ook in organisatorisch opzicht aan te passen. Het verlangt een verantwoordelijkheidsstructuur die past bij de nieuwe realiteit. Hiervoor is vereist dat ze is voorzien van de benodigde slagkracht in strategisch (perspectief en systeemverantwoordelijkheid), maatschappelijk (transparantie en accountability) en operationeel opzicht. De nieuwe technologie maakt meer handhaving en controle mogelijk, maar ook meer criminaliteit. Het debat over de nieuwe technologie laat zien dat er meer mogelijk wordt maar ook dat de risico's toenemen. Risico's op het

vlak van privacy, miljoenen verslindende projecten, nieuwe kwetsbaarheden als identiteitsfraude en onvoldoende aandacht voor beveiliging.

De focus van de analyse ligt op de relatie tussen burgers, instituties en applicaties. Het is dit samenspel dat uiteindelijk bepaalt hoe de dynamiek tussen informatie en technologie er uit komt te zien. Gaan we van een *street level bureaucrat* naar een *screen level bureaucrat*? Is de iOverheid is zich voldoende bewust van de informatiestromen en de processen die daarmee verband houden? Dat blijkt door de feitelijke opeenstapeling van initiatieven erg ingewikkeld, zodat reële gevolgen nog nauwelijks op onze radar verschijnen. Dit gebrekkige bewustzijn wordt krachtig aan de kaak gesteld. Een alles omvattende strategie lijkt hierbij zinloos. Een evenwichtige ontwikkeling van de iOverheid vereist een doordachte afweging van de stuwende, verankerende en procesmatige beginselen die geëxpliciteerd, toetsbaar en publiekelijk te verantwoorden is. Aan drie, onderling gerelateerde, processen worden waarschuwingsvlaggen mee gegeven; met name het vernetwerken van informatie, het samenstellen en verrijken van informatie, en het preventief en proactief beleid op basis van informatie, i.e. het actief beoordelen van en ingrijpen in de samenleving op basis van informatiegestuurde risicoanalyse. De kwaliteit van informatie moet voortdurend kritisch worden bekeken. 'Vergeten' moet blijvend worden verankerd; verouderde gegevens moeten worden verwijderd. De iOverheid dient werk te maken van goed opdrachtgeverschap, waarbij investeren in eigen kennis op het snijpunt van beleid, uitvoering en techniek prioriteit heeft boven het in huis hebben van technische kennis en ontwikkelcapaciteit (die overigens ook bij vele overheden al een serieus probleem vormt). Jaarlijks zou zij ook moeten rapporteren over hoe het staat met de iOverheid. Iedere controller en manager zou dit advies moeten lezen en er voor zijn organisatie consequenties aan moeten verbinden.