



## Veiligheid van online lokale democratie

Waarborgen voor privacy en sociale veiligheid zijn nodig maar te strikte waarborgen kunnen de democratie aantasten

*Roos Hofstra, Ank Michels en Albert Meijer*

*Departement Bestuurs- en Organisationswetenschap, Universiteit Utrecht*

Contact: [a.j.meijer@uu.nl](mailto:a.j.meijer@uu.nl)

6 november 2020

*Dit paper is geschreven in het kader van het onderzoeksprogramma 'Corona als stresstest voor het openbaar bestuur' dat deels wordt gefinancierd door het ministerie van BZK. Binnen dit bredere programma doet de Universiteit Utrecht onderzoek naar de betekenis van de coronacrisis voor democratische innovatie in het lokaal bestuur.<sup>1</sup>*

In de coronacrisis hebben gemeenten en provincies veelvuldig gebruik gemaakt van digitale middelen en communicatiesoftware voor interne en externe communicatie. Politieke processen konden (gedeeltelijk) worden voortgezet, maar het brengt ook nieuwe vraagstukken met zich mee. Een van deze vraagstukken heeft betrekking op privacy en veiligheid. De openheid die digitale middelen biedt creëert ook risico's voor de privacy en de sociale veiligheid. Hoe waarborgen gemeenten en provincies de privacy van deelnemers aan online platforms en hoe zorgen zij ervoor dat er geen ongewenste gasten de vergaderingen binnendringen? En zijn er ook nadelen verbonden aan de gekozen aanpakken? Kan een te grote focus op veiligheid de toegankelijkheid van de democratie beperken? Op basis van een onderzoek bij vier gemeenten en twee provincies presenteren wij lessen voor de omgang met de kwetsbaarheid van een open online democratie.

### Kwetsbaarheid 1: Privacy

Een risico van het gebruik van digitale media is dat gevoelige persoonsgegevens 'weglekken'. Overheden zijn afhankelijk van commerciële softwarepakketten en de vraag is of deze wel voldoende bescherming bieden. Alle gemeenten en provincies gaven aan bij hun keuze voor software goed gekeken te hebben naar privacy en de handhaving van de AVG-wetgeving. Zo heeft bij de gemeente Almere de ICT-afdeling een programma van eisen opgesteld en op basis hiervan allerlei software en applicaties vergeleken, waardoor men een bewuste keuze heeft gemaakt. De gemeente Amersfoort

---

<sup>1</sup> In het kader van het onderzoeksprogramma 'coronabestrijding: stresstest voor het binnenlands bestuur' doet de Utrechtse School voor Bestuurs- en Organisationswetenschap (USBO) onderzoek naar lokale democratische innovatie tijdens de coronacrisis. Het doel is deze processen te begrijpen, te analyseren en hieruit lessen te trekken. Dit onderzoek volgt de ontwikkelingen binnen vier gemeenten (Almere, Amersfoort, Gouda en Woerden) en twee provincies (Overijssel en Zuid-Holland) gedurende acht maanden. De eerste fase van het onderzoek betrof een brede verkenning van democratische innovaties gedurende de coronacrisis. In de tweede fase van dit onderzoek zal op een aantal thema's gedetailleerd gekeken worden naar een aantal 'most informative practices', casuïstiek waar andere overheden lessen uit kunnen trekken.

legt door een datalek van een aantal jaar geleden al veel nadruk op privacy en omgang met gevoelige gegevens, waardoor dat bij de keuze voor een bepaald platform ook een grote rol speelde. De provincie Zuid-Holland heeft bij de selectie van passende videochatdiensten eveneens een risicoafweging gemaakt. Om de privacy van deelnemers te beschermen is rekening gehouden met onder meer de AVG, end-to-end-encryptie en de mogelijkheid tot privacy vriendelijke instellingen.

Over het algemeen is Microsoft Teams de meest gebruikte software onder de gemeenten en provincies. Uit de gesprekken met de vier gemeenten en twee provincies bleek dat zij verschillend denken over het gebruik van het platform Zoom. Op basis van eerder besproken afwegingen hebben onder andere de gemeente Amersfoort en Woerden gekozen om geen gebruik te maken van het platform Zoom. Daarentegen heeft zowel de gemeente Gouda als de provincie Overijssel wel gekozen om Zoom te gebruiken. De ICT-afdeling van de gemeente Gouda heeft Zoom uitgebreid onder de loep genomen en gekozen voor een betaalde versie die privacy en veiligheid volgens hen voldoende waarborgt. Ook zijn er een aantal afspraken gemaakt. Zo is het niet mogelijk om een vergadering of bijeenkomst via Zoom op te nemen. Bovendien heeft de gemeente Gouda de profielen van alle gemeenteraadsleden van een achtergrond voorzien, zodat hun woonkamers en thuissituaties niet in beeld komen. De provincie Overijssel heeft besloten Zoom voor de provinciale staten te gebruiken, met als belangrijke overweging dat bij dit platform veel meer woordvoerders tegelijk in beeld kunnen zijn dan bij bijvoorbeeld Microsoft Teams. De toegangslink is enkel beschikbaar voor deelnemers van de vergadering, om privacy te waarborgen. De gemeente Amersfoort heeft voor medewerkers die niet op een apparaat van de gemeente werken dubbel toegang, vanuit veiligheidsoverwegingen.

We concluderen dat, om privacy te waarborgen, een aantal elementen van belang zijn. Allereerst vraagt het om preventief de juiste keuze te maken en gedetailleerd kijken naar geschikte software. Door hier bij voorbaat veel aandacht aan te schenken, wordt de kans op privacy schending verlaagd. Daarnaast moet men tijdens het gebruik alert blijven en bepaalde keuzes maken omtrent wat wel en niet mogelijk is voor gebruikers van de software.

## **Kwetsbaarheid 2: Ongewenste gasten**

Een tweede gevoeligheid bij de inzet van digitale media waarbij videodiensten worden gebruikt is dat ongewenste gasten invloed kunnen uitoefenen op de bijeenkomst. Zoals bij sommigen bekend zal zijn werd begin mei een gemeenteraadsvergadering van West-Betuwe verstoord door ongepaste beelden en geluiden. Dit kon gebeuren doordat de link naar de Zoom-vergadering openbaar was, zodat inwoners actief konden deelnemen aan het gesprek. Om dergelijke situaties te voorkomen hebben een aantal gemeenten besloten om in eerste instantie geen mogelijkheid tot inspraak door externen te faciliteren. De gemeenten Almere en Woerden hadden de eerste maanden geen mogelijkheid voor inwoners om digitaal in te spreken bij een vergadering. Bij de gemeente Almere konden inwoners schriftelijk hun inbreng aanleveren, maar was er geen mondelinge toelichting mogelijk. Volgens de gemeente Woerden kon het gebrek aan inspraak verklaard worden door de twijfels rondom de veiligheid van de digitale tools bij deze mogelijkheid. Bij beide gemeenten is het wel mogelijk om de bijeenkomsten live te volgen.

Andere gemeenten en provincies vlogen dit anders aan. Bij de gemeente Gouda, Amersfoort en de provincie Overijssel was het wel mogelijk om in te spreken bij een gemeenteraads- of commissievergadering. Bij de gemeente Gouda ontvingen inwoners vlak voor een bijeenkomst een code, als zij zich vooraf geregistreerd hadden als inspreker. Zij konden dan enkel bij het onderwerp van hun inspraak het woord voeren. Ook bij de provincie Overijssel en de gemeente Amersfoort moesten

inwoners zich aanmelden en hun contactgegevens overleggen om in te kunnen spreken. Bij de provincie Overijssel was dit voor het coronatijdperk echter ook al de norm. De link naar de bijeenkomsten werd niet publiekelijk gedeeld. Allen hebben door deze inspraakmogelijkheid geen hinder ondervonden. Bij zowel de gemeenten als de provincie kunnen inwoners ook live de bijeenkomsten volgen. Bij raadsvergaderingen van de gemeente Amersfoort kijken de raadsleden zelf verder ook scherp mee of er onbekenden in de vergadering zitten. Door dit scherp in de gaten te houden voorkom je ook dat outsiders kunnen meepraten.

Samenvattend is een spanning tussen veiligheid en inspraak zichtbaar. Hoewel het niet faciliteren van de mogelijkheid tot digitaal inspreken zorgt voor een waarborging van sociale veiligheid, staat dit wel op gespannen voet met de democratische waarden van inwoners. Inspraakmogelijkheden voor inwoners zijn van groot belang voor het waarborgen van de democratie, wat maakt dat het voor gemeenten en provincies van belang is om dit wanneer mogelijk altijd te faciliteren met inachtneming van de nodige veiligheidsmaatregelen.

## **Conclusie**

Ons onderzoek laat zien dat het waarborgen van de kwetsbaarheden van een online democratie aandacht vraagt maar zeker niet onmogelijk is. De risico's zijn zeker niet zo onbeheersbaar dat dit een reden kan zijn om geen online democratie te organiseren. Wel zien we in de praktijk dat sommige lokale besturen beperkingen opleggen aan democratische interactie omdat zij denken de privacy en veiligheid niet voldoende te kunnen waarborgen. Deze redenering is begrijpelijk maar ook gevaarlijk. Een te grote nadruk op online veiligheid kan de democratie bedreigen. Lokale besturen moet oppassen dat een focus op bescherming van privacy en sociale veiligheid barrières opwerpt die de toegankelijkheid van de democratie aantasten.