

Smart Cities voor Publieke Veiligheid

Geleerde Lessen uit de Praktijk van Crowdmanagement

Managementsamenvatting

Auteurs: Martijn Wessels, Jordi Nahumury, Jip van Stijn



AANLEIDING

Smart city initiatieven met het doel om publieke veiligheid te verbeteren nemen in hoog tempo toe. Veel gemeenten maken steeds vaker gebruik van technologie en (publieke en private) data voor uitvoer van veiligheidstaken en -beleid. Eén van de risico's hierbij is dat er veel lokale initiatieven ontstaan, waardoor het lastig kan zijn voor burgers en publieke organisaties (zoals de Nationale Politie) om overzicht van de initiatieven te krijgen en te behouden, en kan het voor gemeenten uitdagend zijn om van elkaar te leren. Dit leidt ertoe dat het voor publieke en private partijen moeilijk is om kansrijke initiatieven breder of meer in te zetten (opschalen) in de context van een *smart city*.

CONTEXT

Dit onderzoek is onderdeel van een breder onderzoeksprogramma 'Smart Societies' dat in 2021 van start is gegaan. 'Smart Societies' is een gezamenlijk programma van de Impact Coalitie Safety & Security (ICSS) -met in het bijzonder de gemeenten Amsterdam en Den Haag-, de Nationale Politie en TNO voor kennisopbouw rondom *smart societies* voor leefbaarheid en veiligheid. In een *smart society* wordt gericht op de effecten van de inzet van slimme technologie op het maatschappelijk leven (dus de toepassing van technologie). Het doel van het programma is om de capaciteit van gemeenten en de politie te versterken voor het opschalen van kansrijke initiatieven ten behoeve van een *smart city* en daarmee de publieke veiligheid te verhogen. Twee specifieke toepassingsgebieden staan in het programma centraal, namelijk crowdmanagement en gebiedsbeveiliging. Binnen deze toepassingsgebieden ligt de focus van het onderzoek specifiek op de toepassing van mobiliteitsstromen.

DEFINITIES

Smart city initiatief voor publieke veiligheid

Een initiatief dat als doel heeft om via het verzamelen en verwerken van publieke en private data en sensoren de openbare orde en veiligheid binnen stedelijk gebied te verbeteren.

Crowdmanagement

Crowdmanagement kan worden begrepen als voorbereidende maatregelen die worden genomen om het gedrag van (groepen) mensen te beheersen.

DOEL

Het doel van dit onderzoek is om inzicht te geven in de geleerde lessen van Nederlandse *smart city* initiatieven omtrent het implementeren en opschalen door gemeenten binnen het domein van openbare orde en veiligheid. In het bijzonder lag de focus op veiligheidstoepassingen op het gebied van crowdmanagement, waarbij de initiatieven gebruikmaken van mobiliteitsdata. Het overzicht van geleerde lessen kan toekomstige of bestaande *smart city* initiatieven ondersteunen bij het succesvol opschalen van initiatieven.

AANPAK

Voor dit onderzoek is een inventarisatie uitgevoerd van *smart city* initiatieven op het gebied van crowdmanagement bij Nederlandse gemeenten. Onder deze gemeenten waren Amsterdam, Den Haag, Eindhoven, Groningen, Nijmegen, en Rotterdam. Met deze gemeenten zijn vervolgens interviews afgenomen, gericht op wat succes- en risicofactoren zijn bij het ontwikkelen en opschalen van *smart city* initiatieven. Daarna zijn de inzichten die een (in)directe relatie hadden tot de opschaling van initiatieven middels een vooraf opgesteld analysekader op een geaggregeerd niveau per thema uitgewerkt. Vervolgens zijn de succes- en risicofactoren geïdentificeerd door de inzichten uit verschillende gesprekken te combineren. Dit heeft geresulteerd in een overzicht van aandachtspunten waar gemeenten rekening mee kunnen houden bij het opschalen van *smart city* initiatieven, die vervolgens vertaald zijn naar actiegericht geleerde lessen. Een bondig overzicht van deze geleerde lessen is te lezen in het vervolg van deze samenvatting.

DRIE VORMEN VAN OPSCHALING

- 1. Bestuurlijke en geografische opschaling:** de technologische toepassing die is beproefd in een (deel van de) gemeente wordt ook in andere (delen van) gemeenten toegepast, en dus onder een ander bestuur.
- 2. Uitbreiding van doel:** de beproefde technologie wordt voor een *andere* veiligheidstoepassing gebruikt, met typisch een andersoortige eindgebruikers tot gevolg.
- 3. Uitbreiding van functionaliteit:** de functionele werking van het initiatief wordt uitgebreid, met typisch uitbreiding van middelen (technologie, databronnen) tot gevolg.

ALGEMENE LESSEN

1 **Definieer prestatie-indicatoren**

Dit zorgt voor transparantie over de doelstelling en beoordelingscriteria van het initiatief richting interne en externe stakeholders en daarmee ook voor draagvlak. Maak hierbij onderscheid tussen *output* (een signaal) en *outcome* (het daadwerkelijk maatschappelijke veiligheidseffect na opvolging). Maak prestatie-indicatoren ook specifiek voor het veiligheidsrisico.

2 **Documenteer en standaardiseer ethische processen**

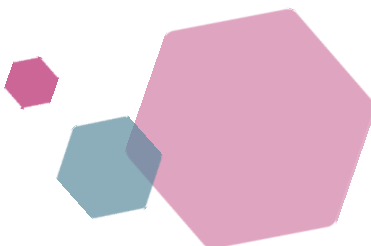
Standaardiseer en documenteer *privacy*- en *ethics-by-design* processen. Dit zorgt ervoor dat de privacy en ethiek van het initiatief op eenduidige wijze wordt beoordeeld. De documentatie kan worden gebruikt voor toekomstige initiatieven, het overdragen naar andere gemeenten, en als verantwoording naar belanghebbenden.

3 **Vermijd persoonsgegevens**

Gebruik zo veel mogelijk adequaat geanonimiseerde gegevens. Dit zorgt ervoor dat het makkelijker is om het initiatief te ontwikkelen en te implementeren. Vermijd informatieverwerking waarbij data van individuen worden verzameld. Het kan hierbij helpen om "situaties", en niet personen, als te herkennen of te voorspellen entiteit te nemen.

4 **Wees transparant**

Maak als initiatief bewuste beslissingen over de inzichtelijkheid in de gebruikte data en informatie om zo transparant mogelijk te zijn. Maak duidelijk onderscheid tussen verschillende soorten informatie om goed te kunnen bepalen welke informatie wel of niet openbaar kan worden gemaakt.



ALGEMENE LESSEN

5

Betrek stakeholders vanaf het begin

Het is raadzaam om belanghebbenden gedurende de gehele ontwikkeling te betrekken. Denk hierbij aan eindgebruikers en burgers, maar ook aan afdelingen die uiteindelijk zorg dragen voor de implementatie en het onderhoud (bijvoorbeeld de IT-dienst, databeheer, of afdeling openbare orde en veiligheid van gemeenten). Op deze manier kunnen eventuele zorgen vroegtijdig worden erkend.

6

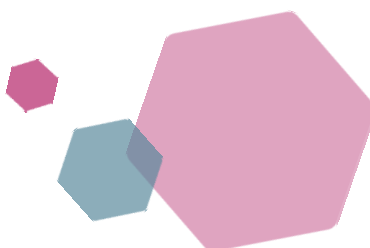
Wees bewust van werken op projectbasis

Op projectbasis werken kan heel nuttig zijn om een probleem op te lossen of technologie te beproeven in gemeenten. Echter kan dit ook nadelige effecten hebben op toekomstige opschaling en doorontwikkeling: na afronding van het project is de opvolging (en de financiering hiervoor) niet altijd vanzelfsprekend. Het implementeren, onderhouden, en opschalen van de smart city toepassing moet namelijk worden georganiseerd in de bestaande organisatie(processen), wat vaak niet onderdeel is van een innovatieproject.

7

Denk vanuit het gewenste maatschappelijke effect

Motiveer de opschaling vanuit de opvolging en de maatschappelijke effecten die er mee verbeterd kunnen worden. Het is raadzaam om niet vanuit het aanbod aan informatie te redeneren, maar vanuit de noodzaak om veiligheidseffecten te verbeteren. Op deze manier wordt informatie als middel en als doel niet verward.



LESSEN VOOR BESTUURLIJKE EN GEOGRAFISCHE OPSCHALING VAN DE TOEPASSING

8 **Maak het ontwikkelproces overdraagbaar**

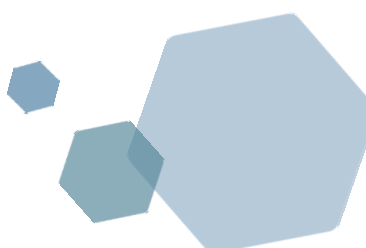
Om een toepassing eenvoudiger in een ander gebied of gemeente in te zetten, is het van belang dat alle ontwikkelstappen goed gedocumenteerd zijn, en gemakkelijk over te dragen aan andere bestuurders. Denk hierbij bijvoorbeeld aan de documentatie voor de *Data Protection Impact Assessment* (DPIA) en de prestatie-indicatoren (zie ook les #1 en #2).

9 **Synchroniseer de ontwikkelstappen**

Als smart city initiatieven op eenduidige wijze worden ontwikkeld, is het eenvoudiger om inzichten over te dragen binnen en tussen gemeenten. Door deze standaardisatie kunnen gemeenten die ervaring hebben op het gebied van smart city initiatieven ook kennis overdragen naar gemeenten met minder ervaring.

10 **Onderscheid generieke en specifieke aspecten van de architectuur**

Maak duidelijk wat in de architectuur (bijvoorbeeld definities van indicatoren en grenswaarden) generiek is, en dus te kopiëren is op een andere locatie of gemeente, en wat specifiek is, en dus aangepast dient te worden aan de context. Het vermogen om het initiatief over te dragen is groter als databronnen, indicatoren en wegingsfactoren zo generiek mogelijk beschreven zijn.



LESSEN VOOR OPSCHALING VAN HET DOEL VAN DE TECHNOLOGIE

11

Waak voor function creep

Als technologie wordt ingezet voor andere veiligheidstoepassingen, moet worden gewaakt voor *function creep*: het onrechtmatig gebruik van data voor andere toepassingen dan waar het initieel voor is bedoeld. Dit kan worden vermeden door delen van het gestandaardiseerde privacy-by-design proces opnieuw uit te voeren.

12

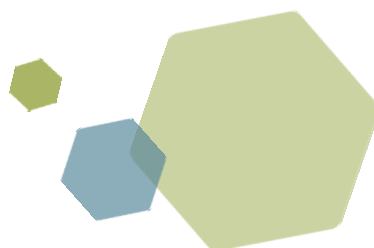
Neem toekomstige use-cases mee

Om efficiënt van middelen gebruik te kunnen maken, kan het nuttig zijn om ook use-cases voor de technologie te bedenken voor andere toepassingen op de langere termijn. Dataminimalisatie kan het ontwikkelproces van het eerste initiatief versnellen, maar opschaling voor andere veiligheidstoepassingen bemoeilijken. Het is dus raadzaam om hierin te zoeken naar de juiste balans.

13

Standaardiseer dataset-structuren

Door het format van typen datasets te standaardiseren is het makkelijker om deze te gebruiken voor andere smart city initiatieven. Bij de standaardisatie kan ook duidelijk worden aangegeven welke kwaliteitseisen zijn gehanteerd, zodat er een goede inschatting kan worden gemaakt van hoe de dataset kan worden hergebruikt.



LESSEN VOOR UITBREIDING VAN DE FUNCTIONELE WERKING VAN HET INITIATIEF

14

Investeer in een schaalbaar IT-platform

Door te werken met een schaalbaar platform waar makkelijk nieuwe technologie aan kan worden toegevoegd, is het eenvoudiger om de technologie voor andere veiligheidstoepassingen te gebruiken. Hierdoor kunnen meerdere (commerciële) partijen worden betrokken bij (toekomstige) initiatieven en voorkomt dit te sterke afhankelijkheid van derde partijen. Zorg er voor dat de samenstelling van een IT-platform past bij de verantwoordelijkheden van de deelnemers, zoals een afdeling openbare orde en veiligheid.

15

Documenteer hoe data leidt tot indicatoren van veiligheidsrisico's

Documenteer eenduidig hoe data wordt gebruikt om indicatoren van veiligheidsrisico's te herkennen. Dit is nodig om daar de juiste verantwoordelijkheid voor te kunnen beleggen en (laten) nemen. Daardoor wordt het eenvoudiger om de functionele werking van het initiatief op te schalen.

