Digitale informatieuitwisseling is sleutel tot succes bij toezicht en handhaving

Op welke wijze biedt digitale dienstverlening ondersteuning in de verschuiving van toezicht- en handhavingstaken binnen het veiligheidsdomein?

Digitale dienstverlening is de trigger voor betere samenwerking tussen toezichthoudende partijen in het publieke domein.

Highlights

- De politie is niet meer de enige handhaver in het publieke domein.
- De (nieuwe) handhaver moet beter worden ondersteund.
- De handhavende partij heeft de benodigde informatie altijd en overal beschikbaar.
- Digitale dienstverlening maakt informatiedeling toegankelijker.

Toezicht in het publieke domein

Traditioneel gezien is het waarborgen van veiligheid in de openbare ruimte een taak die aan de politie toebehoort. Dit is echter aan het verschuiven. De burger wordt steeds vaker geconfronteerd met verschillende handhavers die niet in dienst zijn van de politieorganisatie. Denk hierbij aan BOA's in dienst van de gemeente, in de rol van parkeercontroleurs, toezicht- en handhavingsteams en service- en veiligheidteams. Daarnaast zijn particuliere beveiligingsbedrijven meer aanwezig om het publieke domein veiliger te maken en te houden. Een goed voorbeeld hiervan is de horecaportier die van een rol als poortwachter (de deur bewaken van een horecagelegenheid) meer naar een rol als toezichthouder (niet alleen bij de horecagelegenheid zelf maar ook op straat) beweegt.

Het besef dat de particuliere en publieke ordehandhavers elkaar versterken, neemt toe. Daarmee neemt ook het belang van informatieverstrekking tussen deze partijen toe. Op dit gebied ontstaan moeilijkheden omdat niet alle informatie mag worden gedeeld. Zo worden in het geld en waardetransport, waar publieke en private partijen samenwerken, alleen signalementen gedeeld met het beveiligingsbedrijf om bijvoorbeeld overvallen te voorkomen. Enkel in bijzondere gevallen kan, na toestemming van het OM, ook informatie zoals persoonsgegevens of foto's gedeeld worden. Omdat de politie gebonden is aan de Wet politiegegevens wordt bij publiek-private samenwerking in het convenant vaak een geheimhoudingsplicht opgenomen.

De collectieve horecaontzegging

De particuliere beveiliger wordt in toenemende mate en in verschillende projecten betrokken bij gemeentelijk beleid. Vooral in het veiliger maken van de uitgaansgebieden zijn steeds meer samenwerkingsverbanden tussen publieke en private partijen zichtbaar. Een voorbeeld hiervan is de collectieve horecaontzegging (CHO[1]). Meerdere gemeenten (Utrecht, Amersfoort, Apeldoorn, Enschede en anderen) in Nederland hebben hier een convenant voor opgesteld in samenwerking met de politie en particuliere beveiligingsbedrijven. Zoals het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) aangeeft, is het beoogde effect van de CHO dat notoire geweldplegers worden geweerd uit de aangesloten horecagelegenheden, dat de kennis over notoire geweldplegers wordt vergroot en dat van de maatregel een afschrikwekkende werking uitgaat.

Een ander voorbeeld is het portiersoverleg, een structureel overleg dat door de gemeente Utrecht georganiseerd wordt. Hierin nemen gemeente, politie en horecaportiers plaats, en wordt de uitvoering van beleidsmaatregelen zoals de CHO en de samenwerking tussen de partners besproken.

Eén van de middelen die gebruikt wordt bij deze publiek-private samenwerking is de 'UIT-telefoon', een telefoonnummer waarop de portier rechtstreeks contact kan zoeken met de dienstdoende politieagent van het Uitgaans-Interventie-Team in het uitgaansgebied. Uit het Trends in Veiligheid onderzoek 2015 van Capgemini, uitgevoerd door TNS NIPO, blijkt dat de telefoon het meest gebruikte medium is om in contact te komen met de politie.

Anywhere, anyplace, anytime

In toenemende mate moeten horecaportiers niet alleen de veiligheid binnen de horecagelegenheid handhaven, maar ook de publieke ruimte in de gaten houden, bekende 'probleemgevallen' herkennen (mensen met een ontzegging) en contact onderhouden met collega-portiers en politie. Hiernaast moeten de horecaportiers steeds meer kennis hebben van EHBO, ontruimingsprocedures en het herkennen van verschillende soorten drugs. Ook moeten de horecaportiers zich constant bewust zijn van hun rechten in de uitoefening van hun vak. Bij een eventuele aanhouding heeft een horecaportier bijvoorbeeld niet dezelfde rechten als een politieagent bij een staande houding. De horecaportiers weten vaak niet precies meer wat ze mogen doen, wat ze moeten doen en hoe ze dat moeten doen. Om de juiste beslissingen te kunnen, nemen ontstaat er de drang om op elk moment en op elke plek over de gewenste informatie te beschikken. Daarnaast bestaat ook de behoefte om ondersteund te worden in de dagelijkse werkzaamheden door informatie op te kunnen vragen over hun rechten en plichten.

[1] Convenant III Veilig uitgaan binnenstad Utrecht 2011-2015

Mobiele applicaties

Om invulling te geven aan dit groeiende takenpakket en de communicatie met andere horecaportiers in de binnenstad (politie, collega's) mogelijk te maken, worden verschillende mobiele applicaties geïntroduceerd. Deze digitale dienstverlening staat echter nog in de kinderschoenen. In het centrum van Utrecht wordt geëxperimenteerd met de veiligheidsapp. Deze applicatie moet horecaportiers extra handvatten bieden in het uitvoeren van hun steeds complexer wordende takenpakket. Wanneer zij bijvoorbeeld onbekende drugs aantreffen bij het uitgaanspubliek kunnen zij terugvallen op de applicatie om op te zoeken welk soort drugs het betreft en wat de eventuele bijwerkingen zijn. Naast de naslagfunctie van de applicatie biedt deze ook de mogelijkheid om informatie te delen met het UIT-team. Want waar de particuliere beveiliging steeds vaker taken van de politie overneemt, creëert deze particuliere branche veel eigen data. Voorbeelden van werkgebieden waarin de particuliere beveiliging haar eigen gegevens verzamelt zijn uitgaansgebieden, bedrijventerreinen, de aanpak van jeugdoverlast in probleemwijken en gegevensuitwisseling met betrekking tot overvallen op professionele geld –en waardetransporten. In al deze voorbeelden zijn successen behaald doordat de samenwerking tussen particuliere beveiligingsbedrijven en politie is vergroot en er in toenemende mate informatieuitwisseling plaatsvindt.

Privacy

In grote lijnen zijn de verschillende veiligheidapps bedoeld om de gebruiker van informatie te voorzien (EHBO, soorten drugs), en informatieuitwisseling tussen gebruikers mogelijk te maken (foto's van verdachten, kentekenplaten). Zoals eerder in dit artikel aangegeven mag lang niet alle informatie zomaar worden uitgewisseld. In het geval van de collectieve horecaontzegging worden de horecabezoekers met een verbod met naam en foto op een beveiligde website geplaatst. In de eerste twee jaren (2009-2011) van het CHO-beleid betrof dit in totaal 29 personen. De website mag door de horecaondernemer worden geraadpleegd, maar niet door de horecaportiers. Terwijl zij juist de personen zijn die het beleid moeten handhaven. Om dit soort beleid toch werkbaar te maken, worden in verschillende convenanten afspraken gemaakt met betrekking tot de uitwisseling van informatie en het borgen van privacyvoorwaarden. Wat betreft de collectieve horecaontzegging mogen de horecaportiers bijvoorbeeld alleen in het bijzijn van de horecaondernemer op de website met probleemgevallen kijken. Ze krijgen geen persoonlijke toegang of een eigen account.

Het is erg belangrijk dat persoonsgegevens beschermd worden en dat onbevoegden geen toegang tot persoonlijke gegevens hebben. Maar waar in de verschillende publiek-private samenwerkingsverbanden de plank wordt misgeslagen, is op het selectief toegankelijk maken van bepaalde gegevens en het reguleren van de informatieuitwisseling. In verschillende projecten blijkt dat er geen duidelijkheid is over welke informatie wel, en welke informatie niet gedeeld mag worden. Dit zorgt ervoor dat er helemaal geen informatie gedeeld wordt of dat juist informatie wordt gedeeld die niet gedeeld mag worden, ook wel 'function creep' genoemd. De partijen (politie en particuliere beveiliging) weten van elkaar niet op welke gegevens ze zitten te wachten en vaak is er ook geen duidelijkheid over de manier van communiceren en het vastleggen van de gegevens.

Om informatie beter te structureren, vast te leggen en te borgen dat de informatie niet voor iedereen raadpleegbaar is, zou gewerkt kunnen worden met een gezamenlijke portal, gebaseerd op het principe van privacy by design[2]. Door middel van een goed doordachte autorisatiestructuur kan namelijk worden bepaald welke gebruiker toegang heeft tot bepaalde gegevens. Een gezamenlijke portal kan gemeente, politie, horecaondernemers en portiers faciliteren om gegevens (zoals verslagen van het portiersoverleg of gegevens van nieuwe ontzeggingen) met elkaar uit te wisselen.

Hoe nu verder?

Samenwerking tussen politie en particuliere beveiligingsbedrijven vindt momenteel grotendeels plaats op basis van losse projecten. Elk project lijkt zijn eigen spelregels te hebben wat betreft de informatiedeling[3]. Er zijn nog geen duidelijke richtlijnen voor informatie uitwisseling bij publiek-private samenwerkingsverbanden in het openbare veiligheidsdomein. Dit moet beter worden ingeregeld; de verschillende partijen moeten weten waar zij aan toe zijn en op welke informatie zij wel of geen recht hebben. Wanneer hier duidelijkheid in ontstaat wordt het ook beter mogelijk om, door middel van digitale dienstverlening, meer gegevens uit te wisselen en elkaar op de hoogte te houden. De politie kan haar rol als dienstverlener pakken en via verschillende kanalen deze dienstverlening aanbieden. Niet alleen richting de burgers, maar ook naar haar partners in de handhaving van publieke veiligheid. Er wordt constant data gegenereerd, maar deze data komt nog niet altijd op de juiste plek terecht. Het intensiveren van de samenwerking tussen de verschillende handhavingspartners door middel van efficiëntere informatieuitwisseling, kan een belangrijke stap zijn in een betere handhaving van de veiligheid in de publieke ruimte, voor nu en in de toekomst.

[2] Zie Innovatieagenda 2015 min. Van Veiligheid en Justitie

[3] Nederlandse veiligheidsbranche, Informatie-uitwisseling Politie en Particuliere beveiliging.

Over de auteurs

Sjoerd van Veen MSc en Gijs Daalmijer MSc zijn beide consultant en bestuurskundigen bij Capgemini en als zodanig actief op het gebied van openbare orde en veiligheid.

Voor meer informatie kunt u contact met de auteurs opnemen via sjoerd.van.veen@capgemini.com of gijs.daalmijer@capgemini.com