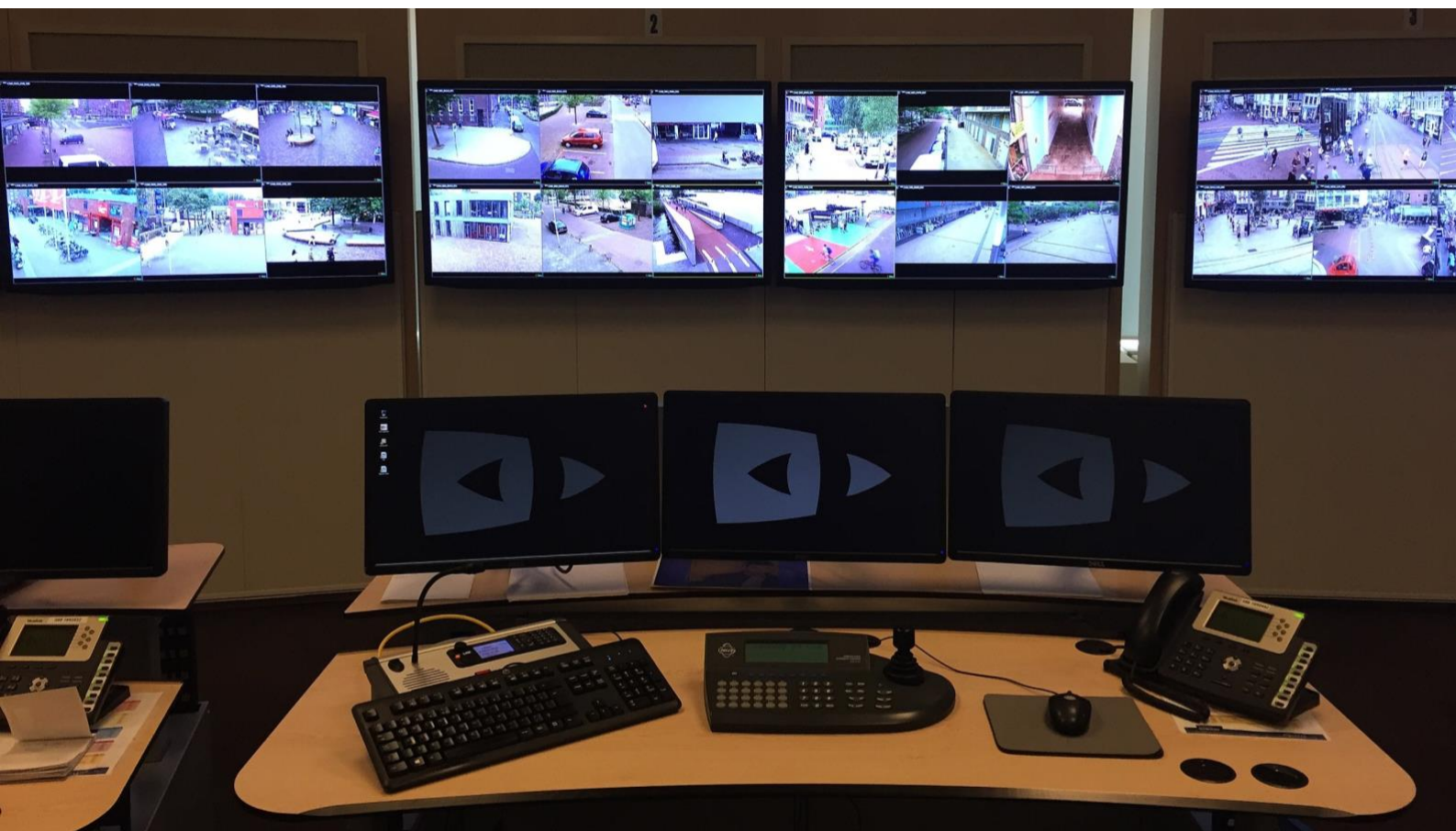


Cameratoezicht op risicolocaties in Nieuwegein

Een inventarisatie van de wetgeving,
techniek, organisatie en kosten



Door

Drs. S. Flight

Opgesteld voor

Gemeente Nieuwegein

Versie

4 maart 2021

Sander Flight

Mail info@sanderflight.nl

Onderzoek & Advies

Web www.sanderflight.nl

Inhoud

1	Inleiding	4
2	Juridisch: wat mag en wat mag niet?	6
2.1	Grondrechten	6
2.2	Persoonsgegevens	12
2.3	Concrete voorbeelden van cameratoezicht	14
2.4	Samenvattend	20
3	Organisatie: wie doet wat?	22
3.1	Preventie	22
3.2	Drie niveaus van rechtstreeks cameratoezicht	23
3.3	Achteraf gebruik beelden	27
3.4	Voorbeelden uit de praktijk	28
3.5	Samenvattend	33
4	Techniek: wat kan er?	34
4.1	Slimme camera's	34
4.2	Artificial Intelligence	35
4.3	Technieken die wel werken	36
4.4	Samenvattend	37
5	Financieel: wat kost het?	38
5.1	Verschillende kostenposten	38
5.2	Gemeentelijk cameratoezicht	38
5.3	Kosten en baten van cameratoezicht	39
5.4	Slimme camera's	40
5.5	Samenvattend	41

1 Inleiding

Motie gemeenteraad

In oktober 2020 heeft de gemeenteraad van Nieuwegein een motie aangenomen over cameratoezicht. De motie verzoekt de burgemeester om:

1. Onderzoek te laten doen naar de noodzaak, proportionaliteit en subsidiariteit van de inzet van cameratoezicht op de door het college benoemde risicolocaties, waarvan in ieder geval de bedrijventerreinen en grote openbare parkeerplaatsen deel uitmaken;
2. De uitkomsten van het onderzoek uiterlijk in Q2 2021 schriftelijk aan de raad terug te koppelen, in welke terugkoppeling tevens staat te lezen op welke wijze het college de resultaten uit dit onderzoek meeneemt in het uitvoeringsplan.

Doel van deze notitie

De gemeente Nieuwegein heeft mij verzocht een notitie op te stellen over de mogelijke inzet van cameratoezicht. De gemeente wil op basis van deze notitie een goed gesprek kunnen voeren met alle stakeholders. Om die discussie van goede input te voorzien ga ik in dit stuk in op de vier “schaakborden” waarop simultaan moet worden gespeeld bij het invoeren van cameratoezicht:

- juridisch: wat mag wel en wat mag niet?
- technisch: wat kunnen camera's?
- organisatorisch: wie doet wat?
- financieel: wat kost het en wat levert het op?

Beperkingen

Deze notitie heeft als belangrijkste doel het bieden van een goede uitgangspositie voor een discussie over de vraag: “Hoe kan de gemeente Nieuwegein het beste omgaan met de mogelijke vormen van cameratoezicht?” Dat is voor een belangrijk deel een politiek-bestuurlijke keuze en geen vraag waar een onderzoek als dit of wetgeving een objectief antwoord op kan geven.

Dat blijkt uit het feit dat vergelijkbare gemeenten in Nederland met vergelijkbare criminaliteitsniveaus zeer uiteenlopende keuzes maken als het op cameratoezicht aankomt. Sommige gemeenten, zoals Amsterdam en Utrecht, hebben relatief weinig gemeentelijke camera's (20 camera's per 100.000 inwoners). Andere grote gemeenten met ongeveer evenveel criminaliteit en overlast, zoals Rotterdam en Den Haag, zetten twee keer zoveel gemeentelijk cameratoezicht in (40 camera's per 100.000 inwoners). En er zijn gemeenten die nog veel meer gemeentelijke camera's hebben, zoals een gemeente in het zuiden van Nederland met 220 camera's per 100.000 inwoners. Die verschillen komen niet door verschillen in criminaliteit: de enige verklaring is een verschil in het politieke draagvlak voor gemeentelijk cameratoezicht.

Dus de vraag of cameratoezicht moet worden ingezet in Nieuwegein is een vraag die alleen in de politieke arena kan worden beantwoord. Met deze notitie hoop ik de ingrediënten voor dat gesprek aan te reiken. Daarom trek ik in dit document geen conclusies en doe ik geen aanbevelingen. De notitie geeft een schets van de verschillende mogelijkheden, zonder een uitspraak over de haalbaarheid of wenselijkheid van een bepaald niveau van cameratoezicht. Dat is een afweging die de gemeente Nieuwegein zelf zal moeten maken.

2 Juridisch: wat mag en wat mag niet?

2.1 Grondrechten

Elke camera is een inbreuk op de privacy van de mensen die in beeld komen. Dat mag niet zonder meer: er moet altijd aan een aantal voorwaarden worden voldaan. Verschillende Nederlandse en internationale wetten stellen grenzen aan de bevoegdheden van de overheid en particulieren om camera's in te zetten. Dat gaat zowel over de inzet van het middel (het plaatsen van de camera's om beelden mee te maken) als over de daadwerkelijke verwerking van die beelden (het bekijken, opslaan, doorsturen, gebruiken en weer verwijderen van de opnames). De waarborgen die gelden voor het plaatsen van camera's volgen vooral uit de Grondwet en het Europees Verdrag voor de Rechten van de Mens. De waarborgen voor het verwerken van de beelden volgen vooral uit de Algemene Verordening Gegevensbescherming.

Grondwet en EVRM

In de Nederlandse Grondwet en het Europees Verdrag voor de Rechten van de Mens is het recht op privacy vastgelegd. Overheden, maar ook bedrijven en burgers onderling, dienen zich terughoudend op te stellen bij het maken van inbreuken op de persoonlijke levenssfeer. Vroeger konden eenvoudig enkele fysieke domeinen worden onderscheiden. Het gebied waar mensen relatief veel recht hadden op privacy was de woning en de inhoud van hun communicatie. Daarbuiten in de openbare ruimte was de verwachting om ongezien over straat te kunnen gaan niet realistisch en mocht de privacy dus meer worden geschonden. Maar dat is een ouderwets onderscheid geworden dankzij nieuwe technologieën. Wat we in huis doen kan vrij eenvoudig van “buitenaf” worden afgelezen, bijvoorbeeld als iemand toegang krijgt tot onze slimme energiemeter of thermostaat of ons wifi-netwerk. En ook wijzelf zorgen voor die grensvervaging: we nemen ons persoonlijke leven mee de straat op. Persoonlijke foto's, dagboeken en administratie staan op onze draagbare smartphone of laptop. De woning is dus niet langer de plaats bij uitstek waar het privéleven zich afspeelt en de openbare ruimte is op een bepaalde manier ook zeer persoonlijk geworden. Onze persoonlijke levenssfeer verdient dus zowel binnen als buiten

bescherming. Een stelsel van wetten, regels en normen beschermt onze persoonlijke levenssfeer.

Wettelijke grondslag

Een van de voorwaarden voor het mogen maken van een inbreuk op het recht op bescherming van de persoonlijke levenssfeer is dat er een wettelijke grondslag voor moet zijn. Die wet moet in een democratisch proces tot stand zijn gekomen en iedereen moet in die wet kunnen lezen in welke situaties en onder welke randvoorwaarden het grondrecht ingeperkt kan worden. Die grondslag kan algemeen zijn of specifiek. Voor een lichte inbreuk op grondrechten is een algemene grondslag voldoende, zoals de Algemene Verordening Gegevensbescherming of de Politiewet. Voor een ingrijpende inbreuk op grondrechten is een specifieke grondslag nodig.

De juridische term die de grens aangeeft tussen lichte en ingrijpende inbreuken op de privacy is stelselmatigheid: een inbreuk op de persoonlijke levenssfeer is stelselmatig als sprake is van een “meer dan geringe inbreuk op de persoonlijke levenssfeer”. Dit is vervolgens ingevuld in de jurisprudentie als een “min of meer compleet beeld van een of meer aspecten van het persoonlijk leven”. Specifieke grondslagen moeten door de wetgever worden ontwikkeld om een legitieme basis te creëren voor ingrijpende inbreuken op de persoonlijke levenssfeer. Het maken van zo’n specifieke grondslag vereist dat verschillende belangen die met elkaar botsen worden afgewogen en er een keuze wordt gemaakt door de wetgever.

Voorbeeld specifieke grondslag: art. 151c Gemeentewet

Een goed voorbeeld van een specifieke grondslag is art. 151c Gemeentewet. Dat wetsartikel geeft burgemeesters de bevoegdheid camera’s te plaatsen voor handhaving van de openbare orde. In 1997 kwamen de ministers van Justitie en van Binnenlandse Zaken nog tot de conclusie dat cameratoezicht in openbare ruimten in beginsel toelaatbaar was op grond van algemene privacywetgeving. Dus was er volgens hen geen aanvullende wettelijke regeling nodig. Maar in 1999 besloten de ministers toch een specifieke wettelijke regeling op te stellen voor systematisch en langdurig cameratoezicht. De aanleiding hiervoor was het feit dat gemeenten ook camera’s wilden gaan invoeren in raamprostitutiegebieden. Die inbreuk op de privacy ging verder dan mogelijk is op een algemene wettelijke grondslag. Er was dus een specifieke wettelijke grondslag nodig, waarmee het cameratoezicht voor de betrokkenen ook op dit soort plekken duidelijk en nauwkeurig en voorspelbaar moest worden. Dat werd art. 151c Gemeentewet.¹

Noot 1 S. Flight (2015), ‘Cameratoezicht’. In: *Hoofdstukken Openbare-Orderecht*, Uitgeverij: Ars Aequi Libri, pp. 125 – 142.

Voorbeeld algemene grondslag: art. 6.1f AVG

Als er geen specifieke wettelijke grondslag is voor cameratoezicht, is het in sommige gevallen mogelijk terug te vallen op een algemene wettelijke grondslag. In die wet staat in het algemeen wat wel of niet mag. Dat is een groot verschil met specifieke wetgeving die vrij precies aangeeft welke spelregels van toepassing zijn. Een voorbeeld van een algemene grondslag voor cameratoezicht is de grondslag “Gerechtvaardigd belang” in de Algemene Verordening Gegevensbescherming.

De AVG in een notendop



Een beroep op die grondslag is mogelijk als de verwerking aan de volgende voorwaarden voldoet:

“Noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.”

Omdat dit een algemene grondslag is, komt het woord “camera” niet voor in dit wetsartikel. Het is aan de verwerkingsverantwoordelijke om aan te tonen dat deze algemene wettelijke grondslag van toepassing is en dat wordt voldaan aan daarin gestelde eisen en randvoorwaarden. De inbreuk op de privacy mag niet groot zijn. Een voorbeeld is een bedrijf dat bewakingscamera’s wil ophangen op de parkeerplaats naast het kantoor. Er is geen specifieke wettelijke grondslag

waar dat bedrijf zich op kan baseren: er is geen sprake van toestemming, vitale belangen, wettelijke verplichting, overeenkomst of algemeen belang. Toch kan dit bedrijf onder bepaalde voorwaarden bewakingscamera's ophangen en een beroep doen op de grondslag "gerechtvaardigd belang". Gerechtvaardigde belangen zijn belangen die door het recht eveneens gerespecteerd en beschermd worden, zoals het nakomen van zorgplichten door een werkgever voor werknemers of het voldoen aan de verplichtingen op basis van het Burgerlijk Wetboek. Het belang moet wel echt, concreet en rechtstreeks zijn, dus niet speculatief, toekomstig of afgeleid. Ook moet de inbreuk op de grondrechten noodzakelijk zijn, dus proportioneel en subsidiair. Die laatste twee eisen komen hieronder aan bod bij bewakingscamera's van particulieren en publiek-private samenwerking.

Noodzakelijkheid

Een inperking van de privacy is voorts alleen legitiem als deze noodzakelijk is.² Of dat het geval is kan niet in het algemeen worden beantwoord: het hangt af van de specifieke situatie en de context. In de jurisprudentie is het noodzakelijkheidscriterium geoperationaliseerd in termen van proportionaliteit en subsidiariteit, oftewel "prop-sub".

Proportioneel

Cameratoezicht is proportioneel als het gerechtvaardigd wordt door het doel en niet verder gaat dan nodig is voor dat doel. Wil men bijvoorbeeld geluidsoverlast van horeca signaleren met behulp van een sensor, dan is het maken van beelden niet proportioneel: een microfoon is dan immers genoeg. Als een ondernemer winkeldieven wil betrappen, is het niet proportioneel als er camera's buiten de winkel worden opgehangen. Binnen in de eigen winkel is genoeg. De proportionaliteit hangt ook af van het aantal camera's dat wordt opgehangen, de grootte van het gebied dat in beeld wordt gebracht en de bewaartermijn van de beelden. Camera's in de pashokjes van een kledingwinkel zijn niet proportioneel, maar camera's tussen de rekken met kleding kunnen dat wel zijn.

Subsidiair

Van subsidiariteit is sprake als het ingezette middel – dus cameratoezicht – het lichtste middel is waarmee het beoogde doel kan worden bereikt. Er mogen geen andere, minder ingrijpende, middelen voorhanden zijn. In veel gevallen wordt de eis van subsidiariteit geïnterpreteerd als een eis om gelijk met de invoering van de camera's ook een paar andere maatregelen te treffen, zoals verbetering van de

Noot 2 De tekst in deze paragraaf is gebaseerd op S. Flight (2013), *Cameratoezicht in Nederland: een schets van het Nederlandse cameralandchap*, Ministerie van Justitie/WODC: Den Haag (<https://repository.wodc.nl/handle/20.500.12832/2065>).

verlichting of meer fysiek toezicht door politie. Dat is echter niet hoe het criterium van subsidiariteit is bedoeld: cameratoezicht is subsidiair als die andere, minder ingrijpende middelen onvoldoende zijn gebleken om het doel te bereiken. Die andere middelen moeten dus eerst zijn uitgetoetst voordat een zwaarder middel mag worden ingezet.

Doelbinding

Het moet voor betrokkenen vooraf duidelijk en voorspelbaar zijn wat er met hun persoonsgegevens zal gebeuren. Daarom is doelbinding een belangrijke voorwaarde voor alle camera-systemen. Een gemeentelijke camera die is opgehangen voor handhaving van de openbare orde mag bijvoorbeeld niet worden gebruikt voor strafrechtelijke handhaving van de rechtsorde of bijvoorbeeld voor stelselmatige observatie. Het verschuiven van doelen van camera's naar andere doelen dan oorspronkelijk afgesproken wordt in de wereld van de privacybescherming ook wel *function creep* of *mission creep* genoemd. Incidentele "bijvangst" voor andere doelen is vaak wel toegestaan. Maar dat moet dan wel gebeuren op basis van een vordering door het bevoegd gezag. De politie kan een opname van een particuliere bewakingscamera vorderen voor haar eigen doelstellingen, dus als het nodig is voor de opsporing van strafbare feiten. Dit is geregeld in artikel 126nda van het Wetboek van Strafvordering:

"In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid (dat zijn misdrijven waar voorlopige hechtenis voor mag worden opgelegd – SF) kan de opsporingsambtenaar in het belang van het onderzoek van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot beelden gemaakt met camera's voor de beveiliging van goederen, gebouwen of personen, vorderen deze gegevens te verstrekken."

Ook de officier van justitie en de rechter-commissaris hebben die mogelijkheid. De politie mag beelden van gemeentelijke camera's die er hangen voor handhaving van de openbare orde ook gebruiken voor opsporing, maar alleen als er een concrete aanleiding is en als de beelden noodzakelijk zijn voor de opsporing van een strafbaar feit (art. 151c Gemeentewet, lid 8). Omdat het niet stelselmatig gebeurt en het primaire doel hetzelfde blijft is het principe van doelbinding hier niet aangetast. Maar opsporing mag nooit het belangrijkste doel worden: dan is een andere grondslag nodig.

Transparantie en informatie

Transparantie is een volgend belangrijk criterium om aan de wetgeving op het gebied van privacybescherming te voldoen. Betrokkenen moeten in bijna alle gevallen actief en transparant worden geïnformeerd over het cameratoezicht en ze moeten weten hoe ze hun rechten kunnen uitoefenen.

Richtlijnen uit Europa

De regels die voor alle verwerkingen van persoonsgegevens gelden staan in de AVG. Voor cameratoezicht zijn deze specifiek uitgewerkt in richtlijnen door de European Data Protection Board (EDPB).³ In het kort komen die voor wat betreft de informatievoorziening aan burgers hierop neer:

- Eerste laag
 - Er moeten informatiebordjes zijn met begrijpelijke en goed leesbare informatie over de beoogde verwerking van de camerabeelden;
 - Een betrokkene moet de informatie kunnen lezen voordat hij of zij in beeld van de camera komt;
 - Het moet duidelijk zijn wie de verwerkingsverantwoordelijke is, het doel van de camera's, de rechten van de betrokkene en bij voorkeur ook de grondslag voor de verwerking en contactgegevens van de verwerkingsverantwoordelijke;
 - Tevens moet duidelijk zijn waar mensen meer informatie kunnen vinden;
- Tweede laag
 - In de "tweede laag" van de informatie – bijvoorbeeld een folder bij de balie of een pagina op een website – moet alle informatie staan die verplicht is gesteld in art. 13 van de AVG;
 - Het gaat dan bijvoorbeeld om de bewaartermijn, het recht op inzage, het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens en of er automatische besluitvorming plaatsvindt op basis van de beelden.

Veel cameraprojecten worden momenteel inderdaad aangekondigd met bordjes of stickers. Maar daarop staat vaak niet alle informatie die volgens de AVG, AP en EDPB nodig zijn.

Verbod op heimelijk cameratoezicht

Heimelijk cameratoezicht is in verreweg de meeste gevallen verboden. Dit is onder andere gereguleerd in het Wetboek van Strafrecht: art. 139f en 441b Sr. Artikel 139f geeft aan dat het in woningen en andere niet voor het publiek toegankelijke plaatsen strafbaar is om met een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en

Noot 3 Zie: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

wederrechtelijk een afbeelding te vervaardigen van een persoon. Artikel 441b zegt bijna hetzelfde, maar gaat over publiek toegankelijke plaatsen en heeft alleen betrekking op “aangebrachte camera’s”. Dat betekent dat draagbare camera’s, zoals smartphones of bodycams op straat mogen worden gebruikt voor het maken van afbeeldingen zonder dat hun aanwezigheid kenbaar is gemaakt. Overigens is het heimelijk inzetten van smartphones en bodycams in de AVG wel verboden, behalve als het gaat om zuiver persoonlijke of huishoudelijke activiteiten zoals een foto maken op vakantie. De reden voor het verschil tussen “binnen” en “buiten” in het Wetboek van Strafrecht is dat mensen op openbaar toegankelijke plekken een andere verwachting hebben van privacy: iedereen weet inmiddels wel dat je op straat kan worden gefilmd, maar in een woning, kantoor of hotelkamer verwacht je dat je niet wordt gefilmd. Er zijn wel degelijk situaties denkbaar waarin heimelijk filmen is toegestaan. Heimelijk cameratoezicht is toegestaan als het niet wederrechtelijk is. Dat wil zeggen: als er een wettelijk fundament voor is gecreëerd. Een voorbeeld is het Wetboek van Strafvordering waarin staat onder welke omstandigheden, voor welke doelen en met welke waarborgen omkleed heimelijke observatie met behulp van technische hulpmiddelen door opsporingsambtenaren is toegestaan.

2.2 Persoonsgegevens

Als een camera eenmaal is geplaatst, worden er bijna altijd ook opnames mee gemaakt. Die opnames bevatten bijna altijd informatie over personen. Dan is dus ook de Europese privacywetgeving voor de verwerking van persoonsgegevens van toepassing op die camerabeelden. De Algemene Verordening Gegevensbescherming (AVG) is het belangrijkste kader voor de verwerking van persoonsgegevens. In de AVG staat onder andere aan welke eisen moet worden voldaan om persoonsgegevens te mogen verwerken. Twee zaken zijn van groot belang in de AVG in vergelijking met de voorganger van de AVG, de Wet bescherming persoonsgegevens (Wbp).

Verwerkingsverantwoordelijke

Ten eerste is het begrip verwerkingsverantwoordelijke geïntroduceerd. Dat is de (rechts)persoon die doel en middelen van de verwerking bepaalt. Belangrijk in de AVG is dat die verantwoordelijkheid niet kan worden overgeheveld naar een partij die in opdracht van de verantwoordelijke de camerabeelden bekijkt of bewaart. De verantwoordelijke moet ervoor zorgen dat ook een alarmcentrale of een beveiligingsbedrijf dat de beelden verwerkt zich aan de AVG houdt. Dit kan worden geregeld in een verwerkersovereenkomst. Bij bewakingscamera’s van particulieren is dat eenvoudig: de eigenaar van het camerasysteem stelt zo’n overeenkomst op met de verwerker, zoals een alarmcentrale. Maar bij

gemeentelijk cameratoezicht ligt dit een stuk ingewikkelder, zoals hieronder zal blijken. De burgemeester is namelijk de verwerkingsverantwoordelijke voor de inzet van de camera's, maar de politie is de verwerkingsverantwoordelijke voor de verwerking van de camerabeelden. Daar ligt intensieve samenwerking en afstemming dus voor de hand, maar dat is nog lang niet overal in Nederland het geval.

Data Protection Impact Assessment

Een tweede verschil tussen de Wbp en de AVG is de Data Protection Impact Assessment. In het Nederlands heet dat een gegevensbeschermingseffectbeoordeling, maar de Autoriteit Persoonsgegevens hanteert de Engelse afkorting: DPIA. Dit is een document waarin de verwerkingsverantwoordelijke beschrijft welke persoonsgegevens worden verwerkt, op grond van welke onderbouwing dat gebeurt, welke privacyrisico's er aan de verwerking vastzitten en hoe die risico's tot een acceptabel niveau worden verlaagd. De DPIA moet worden voorgelegd voor advies aan de Functionaris voor de Gegevensbescherming. Een DPIA is verplicht voor alle verwerkingen die een hoog privacyrisico opleveren. Cameratoezicht op publiek toegankelijke plaatsen is zo'n "hoog risico" verwerking en dus is een DPIA in bijna alle gevallen verplicht.

Politiegegevens

De AVG reguleert de verwerking van persoonsgegevens in Nederland en in alle andere EU-lidstaten. Maar de AVG geldt niet voor de verwerking van persoonsgegevens die voor opsporing worden gebruikt. In de AVG staat het als volgt: de AVG is niet van toepassing op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. De bevoegde autoriteiten zijn bijvoorbeeld politie en andere opsporingsambtenaren, maar ook het openbaar ministerie en rechtbanken. De verwerking van dergelijke gegevens is gereguleerd in een richtlijn in plaats van een verordening: Richtlijn 2016/680/EU. Een verordening geldt direct als "wet" in elke lidstaat, maar een richtlijn moet door het land zelf worden uitgewerkt in nationale wetgeving. In Nederland is de "Richtlijn opsporing" zoals deze ook wel wordt genoemd, uitgewerkt in een nieuwe versie van de Wet politiegegevens (Wpg). Veel van de principes uit de AVG op het gebied van bescherming van de rechten van de personen waarvan gegevens worden verwerkt zijn hetzelfde. Maar er zijn ook grote verschillen. Zo is de bewaartermijn van een camerabeeld onder de AVG meestal drie dagen of vier weken, terwijl politiegegevens meestal tien jaar worden bewaard. Ook de

toegankelijkheid, het inzage-recht voor betrokkenen en de uitwisselbaarheid van gegevens is totaal anders.

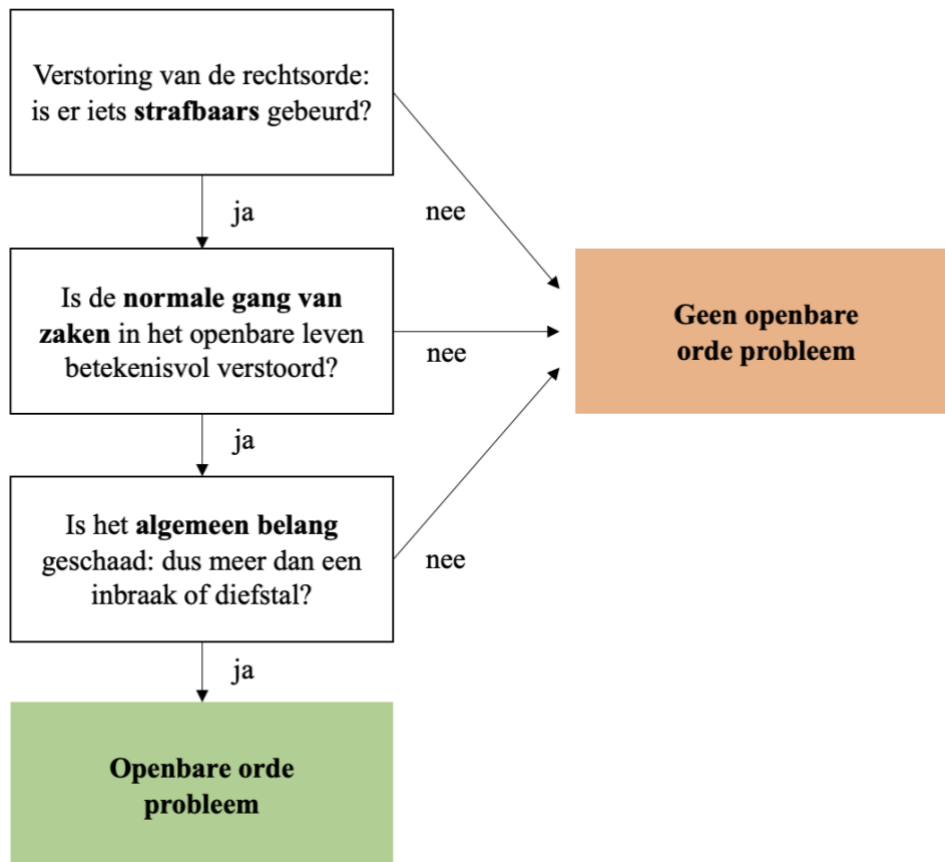
De Wet politiegegevens is ook van toepassing op opsporingswerk dat (gemeentelijke) buitengewoon opsporingsambtenaren (boa's) doen: dit staat in het Besluit Politiegegevens voor buitengewoon opsporingsambtenaren.

2.3 Concrete voorbeelden van cameratoezicht

Gemeentelijk cameratoezicht voor handhaving openbare orde

In de motie van de gemeenteraad die tot deze notitie heeft geleid wordt voorgesteld vaker gebruik te maken van de burgemeestersbevoegdheid om gemeentelijk cameratoezicht in te voeren. Met gemeentelijk cameratoezicht wordt bedoeld op het type cameratoezicht op grond van art. 151c Gemeentewet. Dat wetsartikel biedt burgemeesters de mogelijkheid cameratoezicht in te stellen op openbare plaatsen voor handhaving van de openbare orde. Het is een bijzonder type cameratoezicht, omdat er een specifieke juridische grondslag voor is gecreëerd die beschrijft onder welke voorwaarden dit cameratoezicht mag worden ingezet. Twee zaken zijn van belang: het moet gaan om camera's op openbare plaatsen en om handhaving van de openbare orde. Wanneer is er sprake van een (dreigende) verstoring van de openbare orde? De jurisprudentie maakt duidelijk dat de definitie kan verschillen naar plaats en tijd. Maar *grosso modo* moet het gaan om i) strafbare feiten, ii) een (dreigende) verstoring van het normale leven en iii) een algemeen belang dat wordt geschaad.

Wat is openbare orde?



Voorbeelden van openbare orde probleem

- Uitgaansgeweld
- Structurele jeugdoverlast en intimidaties in een woonwijk
- Protestdemonstraties met dreiging van geweld

Voorbeelden van geen openbare orde probleem

- Fietsendiefstal uit een stalling bij een tramhalte
- Inbraken in kantoren of diefstal uit opslagloodsen op een bedrijventerrein
- Graffiti op een buurthuis of gymzaal

Wie is verwerkingsverantwoordelijke voor gemeentelijke camerabeelden?

De verwerking van camerabeelden van gemeentelijk cameratoezicht is bijzonder. Want er is een specifieke wettelijke grondslag voor gecreëerd waarin afwijkende regels zijn gesteld. Een bijzondere keuze is dat de verwerking van de beelden niet onder de AVG valt, maar onder de Wpg. Dat roept in veel gemeenten allerlei vragen op. Wie moet de beelden opslaan? Wie moet de

beelden bekijken? De Autoriteit Persoonsgegevens heeft op de website⁴ een uitleg gegeven:

- De burgemeester is verwerkingsverantwoordelijke voor de *inzet* van cameratoezicht. De gemeenteraad kan de burgemeester de bevoegdheid geven in de APV. Daarna kan de burgemeester bepalen of er daadwerkelijk cameratoezicht komt. Voor de uitvoering van het cameratoezicht maakt de burgemeester gebruik van de politie;
- De politie is verwerkingsverantwoordelijke voor de *verwerking* van de beelden. De politie bekijkt en gebruikt de camerabeelden – voor rechtstreeks toezicht ter handhaving van de openbare orde, maar ook voor de opsporing van strafbare feiten.

De burgemeester en de landelijke korpschef van politie zijn elk verwerkingsverantwoordelijke voor een verschillend deel van het cameratoezicht: de gemeente voor de inzet van cameratoezicht en de politie voor de verwerking van de beelden. Omdat beiden verwerkingsverantwoordelijke zijn moeten ze ook beiden een Data Protection Impact Assessment (DPIA) uitvoeren voor hun deel van het verwerkingsproces. Zij zullen deze DPIA's uiteraard moeten afstemmen met elkaar. Ze kunnen er ook voor kiezen om gezamenlijk een DPIA uit te voeren. De bewaartermijn van de politiegegevens is in de Gemeentewet overigens op 28 dagen gezet in afwijking van de jarenlange bewaartermijnen die gelden voor de meeste politiegegevens.

Bewakingscamera's van particulieren

Het cameratoezicht door gemeenten dat hierboven is beschreven is bijzonder om verschillende redenen. Ten eerste omdat er een specifieke wettelijke grondslag voor is. Gemeentelijk cameratoezicht is ook bijzonder omdat het vrij zeldzaam is. Naar schatting waren er in 2013 ongeveer 3.300 gemeentelijke camera's in Nederland. Tegelijkertijd werden er voor verkeerstoezicht en openbaar vervoer ongeveer 50.000 camera's op openbare plaatsen gebruikt: de meeste van deze verkeerscamera's waren niet van de overheid (zoals bijvoorbeeld Douane, Rijkswaterstaat of ProRail), maar van bedrijven (zoals NS, RET of GVB). Daarnaast waren er naar schatting nog eens 1.500.000 bewakingscamera's van particulieren. Daarvan waren er naar schatting 640.000 op straat gericht, zoals bijvoorbeeld de camera's rondom tankstations, op openbare parkeerterreinen, in geldautomaten, aan de gevel van horecagelegenheden en dergelijke. Als deze schattingen juist zijn, betekent dit dat slechts één op de tweehonderd camera's op straat van de overheid is; de rest (199 van de 200) zijn in particuliere handen.

Noot 4 Bron: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/cameratoezicht-op-openbare-plaatsen>.

Het juridische regime voor bewakingscamera's van particulieren is niet specifiek, maar algemeen: er is geen equivalent van art. 151c Gemeentewet voor ondernemers die een camera op straat willen ophangen. Dat betekent dat particulieren die een camera willen inzetten zich aan algemene wetgeving moeten houden. Ten eerste betekent dit dat camera's alleen mogen worden ingezet als dit een gerechtvaardigd belang van de particulier dient. Het beveiligen van de eigen woning tegen inbrekers levert al snel een gerechtvaardigd belang op; het ophangen van camera's in een winkelstraat om te zien naar welke etalages het winkelende publiek het meest kijkt is dat waarschijnlijk niet. Ten tweede moet het noodzakelijk zijn om een camera in te zetten: dat wil zeggen proportioneel en subsidiair. Het probleem dat de camera moet helpen oplossen moet dus in verhouding staan tot de inbreuk op de privacy. En lichtere maatregelen moeten hebben gegaald. Ten derde moet de inbreuk op de privacy van de gefilmde personen beperkt zijn. Algemene wetgeving biedt hooguit ruimte voor een beperkte inbreuk op grondrechten en dus niet voor ingrijpende inbreuken (in juridische termen: stelselmatige observatie). Het gaat te ver als met een camera een min of meer volledig beeld van een of meer aspecten van iemands persoonlijke leven kan worden verkregen. Als het de bedoeling is camera's in te zetten op plekken waar mensen normaal gesproken niet worden gefilmd door ondernemers, zoals in woningen, in kleedkamers of op de meeste publiek toegankelijke plaatsen, zoals uitgaansgebieden – dan is daar dus een specifieke wet voor nodig en is algemene wetgeving niet stevig genoeg om de camera's op te baseren.

Publiek-private samenwerking

Publiek-privaat cameratoezicht is een samenwerking tussen publieke en private partijen vanuit een gedeeld belang. De overheid wil vaak cameratoezicht stimuleren op bedrijventerreinen waar het verenigd bedrijfsleven een collectief beveiligingsconcept heeft ontwikkeld. Dat is goed voor het economische klimaat. Maar op die bedrijventerreinen is meestal geen sprake van een verstoring van de openbare orde en dus is gemeentelijk cameratoezicht op grond van art. 151c Gemeentewet niet mogelijk. Toch kan de gemeente dan meewerken aan publiek-privaat cameratoezicht.

In dat geval moet aan een aantal juridische voorwaarden worden voldaan. Ten eerste moet de gemeente expliciet besluiten dat er geen gemeentelijk cameratoezicht zal worden ingesteld. Ten tweede moet de private partij die camera's wil plaatsen verantwoordelijkheid hebben (of krijgen) voor het gebied dat in beeld wordt gebracht. Dat is meestal niet het geval voor afzonderlijke ondernemers, maar kan wel mogelijk zijn voor een stichting of vereniging voor collectieve beveiliging. Uit de statuten van die stichting moet dan blijken dat het

doel van de stichting is het beveiligen van ondernemers op een bedrijventerrein of winkelgebied, inclusief de tussenliggende straten.

De gemeente kan zich overigens nooit onttrekken aan haar verantwoordelijkheid voor de openbare ruimte, aldus de Autoriteit Persoonsgegevens in een onderzoek op een bedrijventerrein in Vianen in 2008. Dus is het wenselijk als de gemeente in het bestuur van de stichting gaat zitten om te controleren of de stichting zich aan de wet- en regelgeving houdt en niet te ver gaat in het inperken van de fundamentele rechten van voorbijgangers. De samenwerking tussen gemeente en stichting (en in voorkomend geval: de politie) kan in een convenant schriftelijk worden vastgelegd. De gezamenlijke ambities en de intentie om samen te werken vanuit gedeeld belang is dan ook op papier geborgd. Hierin zou dan ook moeten staan dat de gemeente geen gemeentelijke camera's zal plaatsen, maar wel steunt dat particulieren dat doen als zij dat binnen de wet- en regelgeving doen. Vervolgens kan de stichting in een cameraprotocol met privacyreglement aantonen dat dit het geval is. In periodiek overleg, bijvoorbeeld in het kader van een Keurmerk Veilig Ondernemen kunnen de afspraken worden bewaakt.

Tijdelijk cameratoezicht door de politie

In de wettelijke taakstelling van de politie ligt besloten dat de politie alle handelingen mag verrichten die nodig zijn om haar taak naar behoren te vervullen. De begrenzing ligt in de verplichting te handelen in ondergeschiktheid aan het bevoegde gezag: de burgemeester voor handhaving van de openbare orde en de officier van justitie voor handhaving van de rechtsorde. Ook moet worden gewerkt in overeenstemming met de geldende rechtsregels.

Bij de inzet van cameratoezicht door de politie wordt inbreuk gemaakt op de persoonlijke levenssfeer: een inperking van een grondrecht. Een dergelijke inbreuk is alleen toegestaan als daar een wettelijke grondslag voor bestaat. De politie beschikt over zo'n grondslag: de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die dat behoeven: art. 3 Politiewet 2012. Camera's mogen door de politie worden ingezet ter ondersteuning van de deeltaken:

- a. handhaving openbare orde
- b. strafrechtelijke handhaving rechtsorde
- c. hulpverlening aan hen die deze behoeven
- d. taken ten dienste van justitie
- e. waken over de veiligheid van personen

De opnames worden verwerkt conform de Wet politiegegevens. In overeenstemming met de juridische kaders kunnen bodycamopnames gedeeld

worden binnen het politiedomein met politie, Koninklijke Marechaussee en Bijzondere Opsporings Diensten en verstrekt worden aan andere personen en instanties. Ook kunnen ze – conform wettelijke kaders, geldend beleid en de gebruikelijke afspraken daaromtrent – gebruikt worden bij de afhandeling van klachten, interne- en strafrechtelijke onderzoeken naar politieambtenaren. Omdat artikel 3 Politiewet geen specifieke, maar een algemene grondslag biedt voor cameratoezicht mag het cameratoezicht niet tot stelselmatige observatie leiden. Dat is een inbreuk op de privacy die een min of meer volledig beeld geeft van een wezenlijk deel van iemands privéleven. Dat betekent in de praktijk dat politiecamera's meestal kortstondig worden ingezet, zoals bij een demonstratie, evenement of acute gevaarzetting. Direct daarna worden ze weer verwijderd.

Als dit niet voldoende is om het doel te bereiken, mag de politie niet op eigen houtje besluiten camera's in te zetten. Als het nodig is een grotere inbreuk op de privacy te maken, moet het bevoegde gezag de politie daar op grond van een specifieke wettelijke grondslag opdracht voor geven. Als het doel de handhaving van de openbare orde is, is het de burgemeester die dit doet op grond van art. 151c Gemeentewet. Als het doel de strafrechtelijke handhaving van de rechtsorde is, is het de officier van justitie of de rechter-commissaris die daartoe de opdracht moet geven op grond van het Wetboek van Strafvordering. Daarover gaat de volgende paragraaf.

Opsporing door politie en het openbaar ministerie

De politie heeft in feite twee “opdrachtgevers”: de burgemeester voor de handhaving van de openbare orde en het openbaar ministerie voor de handhaving van de rechtsorde. In sterk vereenvoudigde vorm komt dit neer op het verschil tussen het voorkomen van criminaliteit (burgemeester) en “boeven vangen” (openbaar ministerie). De politie mag op gezag van het openbaar ministerie camerabeelden gebruiken voor de opsporing van strafbare feiten. Die camerabeelden kunnen op verschillende manieren bij de politie terechtkomen.

Gemeentelijke camerabeelden zijn politiegegevens

Gemeentelijke camerabeelden mogen worden gebruikt voor opsporing (art. 151c, lid 9 Gemeentewet) als er concrete aanleiding is om te vermoeden dat die opname noodzakelijk is voor de opsporing van een strafbaar feit. De camerabeelden zijn politiegegevens en de politie is zoals gezegd verantwoordelijk voor de verwerking van de beelden, aldus de Autoriteit Persoonsgegevens. De burgemeester en gemeenteraad hebben geen toegang tot de camerabeelden: als de gemeente de beelden wil verkrijgen, kan de gemeente dat aan de politie vragen. De politie beslist dan, net als bij andere verzoeken, over die gevraagde verstrekking. De juridische verantwoordelijkheid voor

camerabeelden van gemeentelijke camera's ligt al bij de politie en binnen de Wet politiegegevens, dus daar is geen vordering voor nodig.

Vrijwillige verstrekking camerabeelden aan de politie

Een particuliere eigenaar van een camera – dat kan een bewakingscamera zijn, maar net zo goed een smartphone, drone, webcam of deurbelcamera – mag opnames te allen tijde aan de politie geven, bijvoorbeeld na een inbraak. Als de camerabeelden maar vrijwillig en ongevraagd door de eigenaar van de camera aan de politie zijn gegeven mogen die beelden zonder vordering worden gebruikt door de politie. De politie verwerkt de opname volgens de Wet politiegegevens en mag de opname gebruiken voor waarheidsvinding, opsporingsonderzoek en als bewijsmateriaal.

Vordering door politie, officier van justitie of rechter-commissaris

Als de politie in het kader van een onderzoek zelf bepaalt dat er informatie uit camera's nodig is, kunnen beelden worden gevorderd. Opsporingsambtenaren van de politie mogen zelf op grond van art. 126nda Sv camerabeelden van bewakingscamera's vorderen. Voor vorderingen met een ingrijpend karakter is een vordering van een officier van justitie nodig, op grond van art. 126nd Sv. Voor zeer ingrijpende gegevens is zelfs een machtiging van de rechter-commissaris nodig.⁵ Bekende voorbeelden zijn “gevoelige” of bijzondere persoonsgegevens, zoals gezondheid, seksuele voorkeuren, religieuze of politieke overtuigingen of etnische identiteit.

2.4 Samenvattend

- Camera's perken het grondrecht op privacy in; dat is alleen onder bepaalde voorwaarden toegestaan;
- Er zijn algemene wettelijke grondslagen, zoals de AVG, waarop een lichte inbreuk op privacy kan worden gebaseerd. Voor een ingrijpende inbreuk op de privacy is een specifieke wettelijke grondslag nodig, zoals art. 151c Gemeentewet of het Wetboek van Strafvordering;
- Cameratoezicht moet niet alleen een grondslag hebben in een wet; het is ook alleen maar toegestaan als het noodzakelijk is: dat wil zeggen proportioneel en subsidiair;
- Heimelijk cameratoezicht is in vrijwel alle gevallen verboden;
- Camerabeelden zijn persoonsgegevens of politiegegevens en dus is de

Noot 5 Er is een modernisering op komst van het Wetboek van Strafvordering conform de aanbevelingen van de “Commissie Koops”. In de tekst van deze notitie is alvast rekening gehouden met die voorstellen. Zie: Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018.

AVG of de Wet politiegegevens van toepassing;

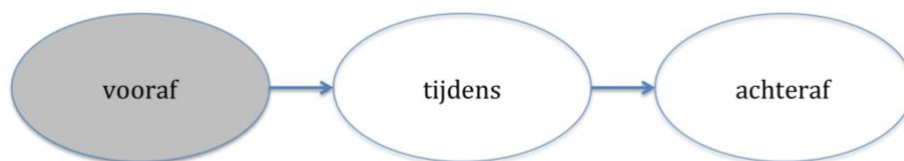
- Gemeentelijk cameratoezicht is er voor een specifiek doel: handhaving van de openbare orde. De burgemeester is verwerkingsverantwoordelijke voor de inzet; de politie voor de verwerking van de camerabeelden;
- Bewakingscamera's van particulieren moeten voldoen aan de AVG;
- Publiek-private samenwerking is mogelijk als gemeente en ondernemers hier goede afspraken over maken en schriftelijk vastleggen;
- De politie kan zelf kortdurend cameratoezicht inzetten voor het "dagelijkse politiewerk" mits de inbreuk op de privacy beperkt blijft;
- Ingrijpende vormen van cameratoezicht door politie en het openbaar ministerie zijn mogelijk maar dan alleen binnen de kaders van het Wetboek van Strafvordering.

3 Organisatie: wie doet wat?

In dit hoofdstuk gaat het over de samenwerking die nodig is om van cameratoezicht een succes te maken. Er zijn drie “mechanismen” die door een camera kunnen worden geactiveerd: preventie vooraf, reactie tijdens incidenten of opsporing achteraf. Die drie mechanismen komen in dit hoofdstuk aan bod.

3.1 Preventie

Het plaatsen van een camera is soms al voldoende om het doel te bereiken: preventie van criminaliteit en overlast. Dat is het eerste van de drie mechanismes die door camera's kunnen worden geactiveerd: *deterrence* of afschrikking. Dit wordt ook wel het *civilizing effect* of beschavende effect van camera's genoemd. In het dagelijkse spraakgebruik horen we vaak: ‘Criminelen zullen zich wel twee keer bedenken voordat ze onder het oog van een camera hun slag slaan’ of ‘Vreemde ogen dwingen’. Het mechanisme is bekend uit de sociologie en wordt geactiveerd als we ons bekeken voelen. De meesten van ons passen dan ons gedrag in positieve zin aan.



Dit corrigerende effect treedt echter niet altijd en overal op: de context maakt veel uit, evenals het probleem dat de camera moet aanpakken. Criminaliteit die wordt gepleegd door rationele daders, zoals een deel van de woninginbraken, neemt sneller af door camera's dan impulsieve criminaliteit, zoals geweldsdelicten. Maar *grosso modo* is bewezen dat een camera preventief kan werken als hij goed wordt ingezet. Een belangrijke voorwaarde is in elk geval dat mensen de camera kunnen zien. De zichtbaarheid van de camera is dus zeer belangrijk. Maar ook andere vormen van informatie kunnen het preventieve effect vergroten: informatieborden, stickers, confrontatiemonitors (waarop

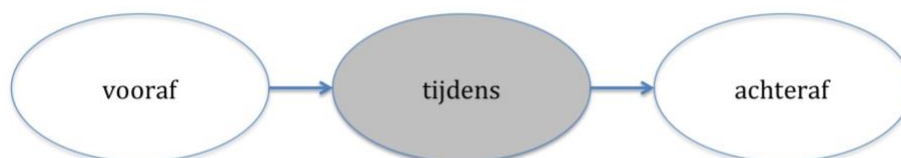
mensen zichzelf zien) en dergelijke. Voor een preventief effect is het van belang ervoor te zorgen dat communicatie geen sluitpost wordt, maar juist alle aandacht krijgt.

Verplaatsing van criminaliteit en overlast

Als ergens camera's worden opgehangen is er altijd de angst dat de criminaliteit en overlast zich simpelweg zullen verplaatsen "om de hoek" waar de camera niets kan zien. Dit wordt ook wel eens het "waterbedeffect" genoemd. Uit onderzoek blijkt echter dat het nettoresultaat van cameratoezicht eigenlijk altijd positief is.⁶ Zelfs als criminelen hun werkgebied verplaatsen is dat eigenlijk nooit volledig. En vaak is er zelfs sprake van het tegenovergestelde: een positieve uitstraling die verder reikt dan alleen het gebied dat in beeld is van de camera's. De verklaring hiervoor is dat criminelen en overlastgevers zich door de camera's realiseren dat de overheid de aanpak van criminaliteit en overlast blijkbaar intensiveert. Dat gebeurt op de ene plek met een camera, op de andere plek met meer fysiek toezicht door politie en op een derde plek met meer fysieke beveiligingsmaatregelen. Dat kan er dus ook op die andere plekken zonder camera's toe leiden dat criminaliteit en overlast worden voorkomen. De gedachte dat cameratoezicht bijna automatisch zal leiden tot volledige verplaatsing van de problemen "om de hoek" wordt dus zeker niet ondersteund door ervaringen in de praktijk.

3.2 Drie niveaus van rechtstreeks cameratoezicht

In sommige gevallen is het plaatsen van een camera al genoeg om ervoor te zorgen dat mensen zich aan de wet houden. Maar vaak is het louter neerzetten van een camera niet genoeg en moet er ook iets met de beelden worden gedaan. Dat kan op twee manieren: via rechtstreeks toezicht of achteraf op basis van de gemaakte beelden.



Noot 6 Flight, S., Y. van Heerwaarden en P. van Soomeren (2003) 'Does CCTV Displace Crime? An Evaluation of the Evidence and a Case Study from Amsterdam', in M Gill (ed.) *CCTV*, pp. 93-8. Leicester: Perpetuity Press.
Waples, S., Gill, M., & Fisher, P. (2009). Does CCTV displace crime? *Criminology & Criminal Justice*, 9(2), 207-224.
Cerezo, A. (2013). CCTV and crime displacement: A quasi-experimental evaluation. *European Journal of Criminology*, 10(2), 222-236.

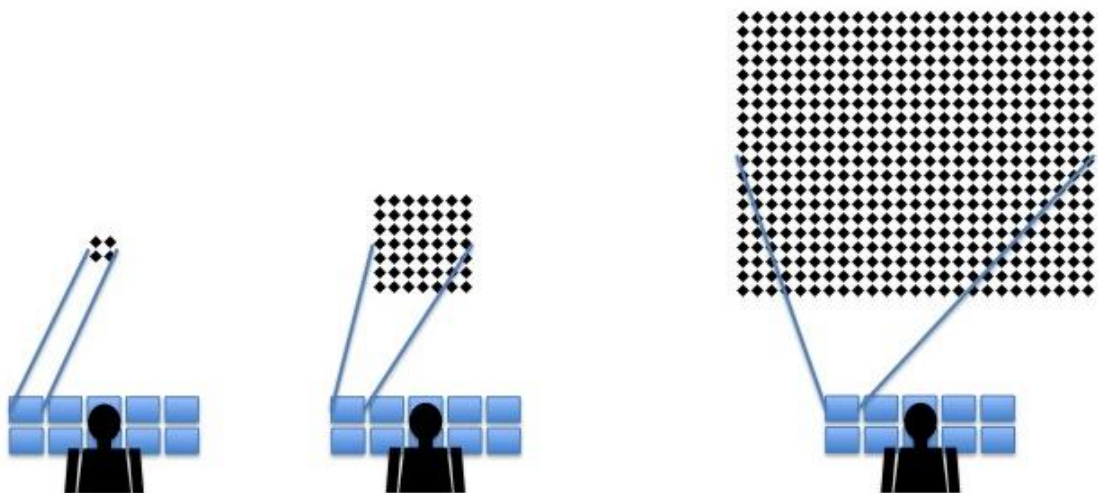
Voor gemeentelijk cameratoezicht is het verplicht om – in elk geval een deel van de tijd – rechtstreeks toezicht te houden. In art. 151c Gemeentewet (lid 3) staat dat de burgemeester de periode vaststelt waarin de beelden in elk geval rechtstreeks worden bekeken.

Rechtstreeks toezicht vergt veel organisatie en is relatief kostbaar. Maar het maakt het wel mogelijk incidenten in de kiem te smoren en het vergroot ook de kans op een aanhouding op heterdaad.

Verschillende soorten van rechtstreeks cameratoezicht

Er is een groot verschil tussen cameratoezicht en alarmafhandeling. Met cameratoezicht wordt hier bedoeld dat er ook naar de camerabeelden wordt gekeken als er nog helemaal niets aan de hand is. Zodra er dan iets in beeld gebeurt, wordt het rechtstreeks waargenomen in de centrale en kan er een reactie op straat worden gegeven. Dit zien we in gemeentelijke toezichtcentrales.

Cameratoezicht is een totaal ander concept dan alarmafhandeling, zoals dat gebeurt in particuliere alarmcentrales. Bij alarmafhandeling staan alle beeldschermen standaard “op zwart”. Het beeldscherm met camerabeelden springt pas aan als er een alarm afgaat, zoals een inbraakalarm, brandalarm of overvalalarm. Het aantal camera's dat kan worden aangesloten op een toezichtcentrale is dus veel groter dan in een gemeentelijke centrale. Dat blijkt uit onderstaande figuur met drie voorbeelden uit de praktijk.



- Links: cameratoezicht in een gemeentelijke centrale;
- Midden: cameratoezicht en alarmafhandeling bij een OV-bedrijf;
- Rechts: alarmafhandeling in een particuliere alarmcentrale.

Het idee van gemeentelijk cameratoezicht is dat alle camera's continu in de gaten worden gehouden. Een mens kan natuurlijk maar een beperkt aantal beelden bekijken. In de meeste gemeentelijke centrales worden per beeldscherm vier camera's weergegeven. Dit zijn de vierkante blokjes in bovenstaande figuur. Er staan meestal tien beeldschermen per werkplek. Elke centralist kan dus veertig camera's tegelijk bekijken. In een stad als Rotterdam hangen circa vierhonderd gemeentelijke camera's en dus zijn er in de toezichtcentrale tien werkplekken nodig (10 werkplekken X 40 camera's = 400 camera's).

Aan het andere uiterste staat een particuliere alarmcentrale die alleen alarmen afhandelt. Daar is de werkplek van elke centralist hetzelfde: ook hier staan tien beeldschermen. Maar al die beeldschermen staan standaard "op zwart" totdat er een alarm afgaat. Dan springt het beeld aan en kan de centralist de politie bellen of de melding als een vals alarm afboeken. In een alarmcentrale kunnen wel 15.000 tot 50.000 camera's per werkplek worden verwerkt – afhankelijk van het soort klant en de frequentie van alarmen. Als het aantal alarmen groter wordt dan het aantal beschikbare beeldschermen en centralisten, dan worden de alarmen in een wachtrij geplaatst en op volgorde van binnenkomst en prioriteit afgehandeld.

Een OV-bedrijf bevindt zich meestal tussen deze twee uitersten. Een deel van de camera's moet continu worden bekeken: dat is bijvoorbeeld de camera in de stationshal of op een druk perron. De meeste camera's worden alleen maar bekeken als er een alarm afgaat, zoals bij liften, roltrappen of informatiezuilen. In zo'n toezichtcentrale kunnen dus circa vijfhonderd camera's per werkplek worden bekeken. Maar veel van dit soort grotere organisaties kiezen voor een scheiding van cameratoezicht en alarmafhandeling. De werkzaamheden zijn gewoon té verschillend. Als er een alarm binnenkomt verslapt automatisch de aandacht voor het reguliere cameratoezicht. Daarom hebben organisaties als ProRail, Rijkswaterstaat, NS en Schiphol aparte centrales gebouwd voor cameratoezicht en voor alarmafhandeling.

Politie en rechtstreeks cameratoezicht

De politie kijkt niet rechtstreeks naar alle camerabeelden van particulieren: dat zou een veel te grote tijdsinvestering vergen. Maar camerabeelden kunnen we degelijk relevant zijn. Daarom is er een andere werkwijze ontwikkeld: Live View.

Live View

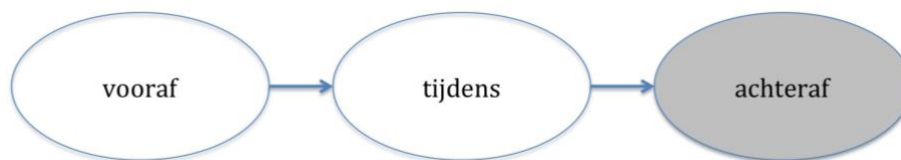
Dankzij *Live View* kunnen centralisten in de 112-meldkamers rechtstreeks meekijken met camerabeelden van particulieren of van de overheid. De camerabeelden worden pas doorgestuurd nadat ze zijn beoordeeld door een alarmcentrale of een gemeentelijke toezichtcentrale. Die andere centrales worden de “poortwachters” genoemd. In 2013 waren er veertig poortwachters op *Live View* aangesloten: particuliere alarmcentrales, regionale toezichtruimtes en gemeentelijke toezichtcentrales. Samen ontsloten die poortwachters circa 50.000 camera’s voor de politie. Dat aantal kon snel groeien, want van de particuliere bewakingscamera’s was slechts een heel klein deel via een videoverbinding een alarmcentrale gekoppeld. Volgens de Vereniging van Beveiligings-Ondernemers in Nederland (VEBON) ging het in 2013 om 1% van alle particuliere bewakingscamera’s. Dat betekende dus dat er ongeveer 15.000 van de 1.500.000 bewakingscamera’s in Nederland waren gekoppeld. Als het percentage zou stijgen naar 5% gaat het al om 75.000 camera’s. De opbrengst van *Live View* hangt niet alleen af van het aantal camera’s, maar ook van de kwaliteit van de alarmbeoordeling door de poortwachters. De samenwerking tussen de meldkamers en de poortwachters is cruciaal om te voorkomen dat de 112-meldkamers overbelast raken.



Zie: <https://www.politie.nl/themas/live-view.html>

3.3 Achteraf gebruik beelden

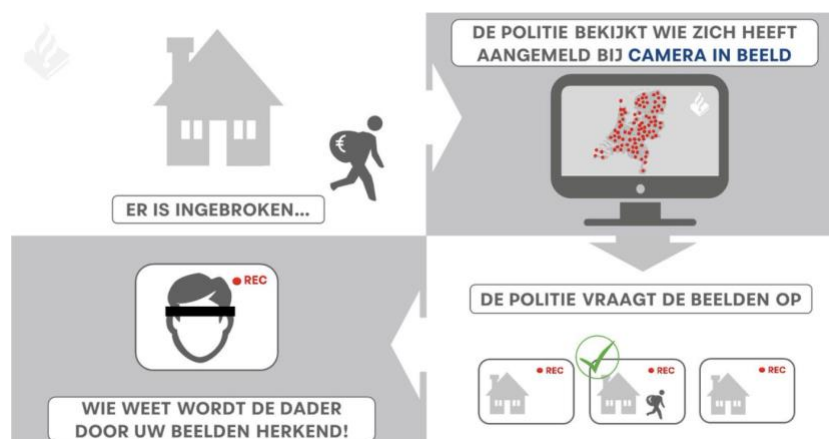
Achteraf gebruik van opnames is waar de meeste mensen als eerste aan denken bij cameratoezicht: “Gelukkig hebben we de beelden nog”. Dat zijn de beelden zoals die langskomen in het programma *Opsporing Verzocht*.



Deze vorm van cameratoezicht is goedkoper dan rechtstreeks toezicht. Het is ook eenvoudiger te organiseren. Maar ook dit derde mechanisme vergt een goede samenwerking tussen de eigenaar van de camera en de politie. Soms weet de politie niet dat er een camera hangt, soms zijn de beelden al gewist, soms kan de politie de beelden niet afspelen en soms zijn de camera's niet goed genoeg of niet op de goede plek gericht. De politie heeft een werkwijze bedacht om dit mechanisme beter te laten werken: Camera in Beeld.

Camera in Beeld

Ondernemers en particulieren met bewakingscamera's kunnen aan de politie doorgeven waar de camera's zijn geïnstalleerd. De politie kan dan na een aangifte snel zien of er een camera in de buurt is die wellicht iets heeft opgenomen en contact opnemen met de eigenaar. Volgens *Trouw* stonden er begin 2019 200.000 beveiligingscamera's in het systeem.



Zie <https://www.politie.nl/themas/camera-in-beeld.html>.

3.4 Voorbeelden uit de praktijk

Gemeentelijk cameratoezicht voor handhaving openbare orde

Bij gemeentelijk cameratoezicht neemt de burgemeester het besluit om camera's in te zetten. Daarna bedient de burgemeester zich van de politie voor de uitvoering van dat besluit, aldus de Gemeentewet. In de praktijk wordt dit deel van de Gemeentewet echter zeer verschillend uitgelegd in verschillende gemeenten.

- In sommige gemeenten, bijvoorbeeld Den Haag, heeft de politie een cameratoezichtruime gebouwd in een politiepand waar politiemensen het rechtstreekse cameratoezicht uitvoeren. De politie neemt hier de volledige verantwoordelijkheid voor de camerabeelden en voert ook alle werkzaamheden zelf uit: uitkijken, opslaan, verstrekken en verwijderen.
- Er zijn daarnaast ook gemeenten (onder andere Utrecht en Amsterdam) waar de politie wel de toezichtruimte heeft gebouwd in een politiepand, maar waar het daadwerkelijk bekijken van de camerabeelden door gemeentelijke toezichthouders wordt gedaan (Amsterdam) of door studenten van de opleiding Integrale Veiligheid (Utrecht). De politie is wel aanwezig als regisseur en om bij incidenten politiecollega's aan te kunnen sturen, maar het meeste werk wordt dus door anderen dan politiemensen gedaan.
- Daarnaast zijn er gemeenten (zoals Rotterdam) waar de gemeente de toezichtcentrale heeft ingericht in een gemeentelijk gebouw waar toezichthouders onder regie van de politie het rechtstreekse toezicht doen.
- Er zijn ook gemeenten, vooral de middelgrote en kleinere gemeenten, waar geen politiemensen aanwezig zijn in de toezichtruimte.
- Er zijn zelfs gemeenten waar de politie in het geheel niet is betrokken bij het opslaan, bekijken, gebruiken of verwijderen van de camerabeelden. Dat is bijzonder aangezien de beelden politiegegevens zijn en de politie verantwoordelijk is voor de verwerking van gemeentelijke camerabeelden.
- Er zijn ook gemeenten waar de camerabeelden niet rechtstreeks worden bekeken, maar alleen opgeslagen voor gebruik achteraf. Dat is ook weer bijzonder omdat in de Gemeentewet staat dat er in elk geval op bepaalde uren/dagen rechtstreeks naar de beelden moet worden gekeken.

In elk geval is de conclusie dat gemeentelijk cameratoezicht in Nederland op zeer verschillende manieren wordt uitgevoerd. Juridisch is het helder: de burgemeester is verantwoordelijk voor het besluit tot inzet van de camera's en

de politie is verantwoordelijk voor de verwerking van de camerabeelden. Maar in de praktijk is dat meestal niet conform de wet georganiseerd.

Bewakingscamera's van particulieren

Grote organisaties, zoals OV-bedrijven, banken of supermarktketens hebben zoveel bewakingscamera's dat ze een eigen toezichtcentrale inrichten voor rechtstreeks toezicht en het verwerken van de opnames. Kleinere organisaties en particulieren kunnen een contract sluiten met een Particuliere Alarm Centrale of een Video Alarm Centrale. Als er dan een alarm afgaat, zoals een brandalarm of inbraakalarm, kan de alarmcentrale op basis van de beelden het alarm verifiëren en de politie bellen.

Maar zoals gezegd hebben verreweg de meeste bewakingscamera's geen videoverbinding met een centrale. Daar worden de beelden alleen maar opgeslagen. De politie kan veel baat hebben bij beelden van bewakingscamera's van particulieren. Als er iets bruikbaars op de beelden staat, kunnen deze aan de politie worden verstrekt en worden gebruikt voor opsporing. Maar hoe krijgt de politie die beelden? Meestal gaat de politie na een aangifte zelf op onderzoek uit en als dan blijkt dat er in de buurt van het incident bewakingscamera's hangen, kunnen die beelden worden opgevraagd bij de eigenaar. Vaak zijn de beelden dan al gewist. Daarom zijn er de afgelopen jaren pogingen gedaan tot een meer structurele samenwerking te komen tussen politie en particulieren. Live View is er voor de rechtstreekse doorzending van beelden naar de 112-meldkamer. Camera in Beeld is er voor de opgenomen beelden. Beide concepten zijn hierboven al besproken.

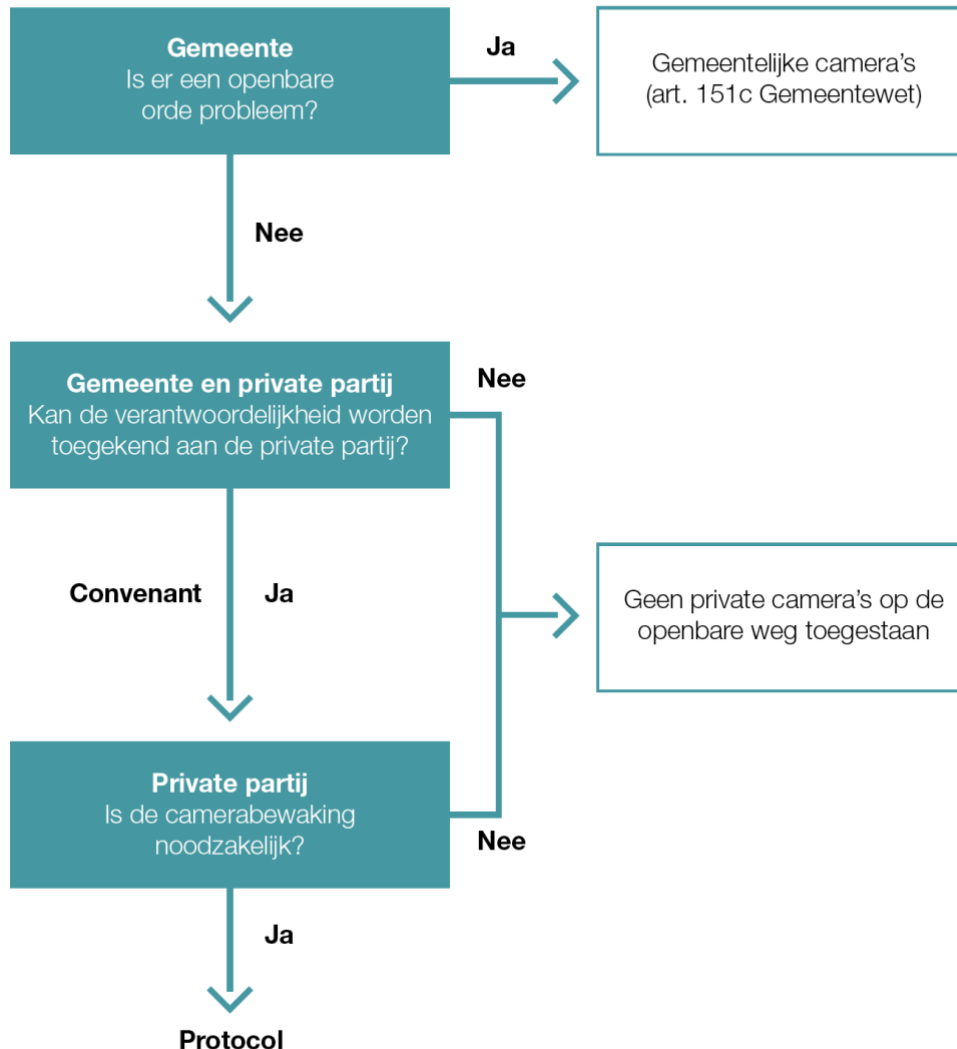
Publiek-private samenwerking

Bij publiek-private samenwerking is de uitdaging om de samenwerking tussen publieke en private partijen goed te regelen en langdurig vast te houden. Op veel bedrijventerreinen en in winkelgebieden wordt gewerkt met het Keurmerk Veilig Ondernemen. Dat is een prima organisatievorm waar camerabewaking een onderdeel van kan worden gemaakt. De belangrijkste partners zitten in het KVO om tafel en daar profiteert het cameratoezicht ook van.

De gemeente is vaak betrokken als deelnemer aan het bestuur van de stichting of vereniging die de collectieve beveiliging regelt. De burgemeester is soms ook bereid het bedrijventerrein aan te wijzen als cameratoezichtgebied conform de Gemeentewet, hoewel de vraag legitiem is of hier wel echt sprake is van een verstoring van de openbare orde. Meestal is de gemeente betrokken omdat velen denken dat private partijen geen openbare plaatsen mogen filmen. Dat is niet het geval, zoals in het juridische hoofdstuk is besproken. Maar het heeft in veel gemeenten wel de situatie opgeleverd dat de burgemeester het bedrijventerrein

of winkelgebied aanwijst als gemeentelijk cameragebied. De camera's worden vervolgens door de ondernemers geplaatst en in een particuliere alarmcentrale of andere particuliere toezichtcentrale bekeken. De politie is echter ook in dit geval de verwerkingsverantwoordelijke voor de camerabeelden omdat de Gemeentewet de basis is. Dat levert in een aantal gemeenten momenteel discussies op over de vraag of het niet anders moet worden geregeld. Een mogelijkheid is dat de politie de beelden gaat verwerken. Maar een alternatief is ook een publiek-private samenwerking waarbij de gemeente niet verantwoordelijk is, maar wel betrokken blijft. Dat kan bijvoorbeeld via de wethouder Economische Zaken in het kader van het werken aan een aantrekkelijk vestigingsklimaat door veilig ondernemen. Maar het is dan niet meer de burgemeester als handhaver van de openbare orde die hierbij betrokken is als verwerkingsverantwoordelijke.

Stappenplan voor private bewakingscamera's op de openbare weg op bedrijventerreinen



Dit is een verrassende insteek voor veel gemeenten die al publieke camera's inzetten voor handhaving van de openbare orde. De regels die daarvoor gelden worden vaak automatisch van toepassing verklaard op ondernemers die met een plan naar de gemeente komen om bewakingscamera's op de openbare weg te richten. Maar het doet er in juridische zin niet zoveel toe waar een camera precies op is gericht: veel belangrijker is het doel van die camera. Is dat handhaving van de openbare orde of bewaking van particuliere eigendommen? Er zijn heel veel camera's van particulieren die gericht staan op publiek toegankelijke plaatsen (dat zijn de openbare weg en alle andere plekken waar mensen kunnen komen en gaan zonder een toegangsbewijs of kaartje). De plek waar een camera staat is dus niet het onderscheidende criterium. Veel

belangrijker is het doel: art. 151c Gemeentewet gaat alleen over handhaving van de openbare orde. Is dat niet aan de orde? Dan kan een ondernemer – onder de voorwaarden die in de wet staan – bewakingscamera's op publiek toegankelijke plaatsen neerzetten.

De ondernemers mogen publiek toegankelijke plaatsen (waaronder de openbare weg) alleen filmen als ze verantwoordelijk zijn voor het gebied dat ze in beeld willen brengen. Die verantwoordelijkheid kan in bijzondere gevallen worden toegekend aan een vereniging of stichting voor collectieve beveiliging mits de gemeente ook zitting neemt in het bestuur. De ondernemers moeten uiteraard aan alle wet- en regelgeving voldoen en dit kunnen aantonen. Daarom verdient het aanbeveling in dit soort projecten een cameraprotocol (of een ander document) op te stellen waaruit blijkt dat het cameratoezicht gerechtvaardigd is. De belangrijkste eisen volgens de Autoriteit Persoonsgegevens zijn:

- De camera's moeten proportioneel en subsidiair zijn;
- Het doel van de camera's moet worden beperkt tot beveiliging; het handhaven van de openbare orde of het strafrechtelijk handhaven van de rechtsorde mag geen doel zijn;
- Er moet een veiligheidsanalyse zijn uitgevoerd waaruit blijkt dat de problemen ernstig genoeg zijn om het relatief zware middel camerabewaking in te zetten;
- De camera's moeten worden verwijderd als ze niet meer noodzakelijk zijn;
- Bewoners en voorbijgangers in het gebied moeten worden betrokken omdat zij recht hebben in principe onbespied over straat te gaan;
- Betrokkenen hebben rechten, zoals het recht op inzage of het recht op verwijdering van onterecht verzamelde gegevens;
- Het aantal camera's moet zo klein mogelijk zijn, evenals het gebied dat in beeld wordt gebracht;
- Beelden moeten zo min mogelijk rechtstreeks worden bekeken, dus alleen op tijdstippen dat dit aantoonbaar noodzakelijk is;
- De opgenomen beelden moeten goed worden beveiligd om onbevoegd gebruik te voorkomen en personen die de beelden gebruiken moeten aan een aantal eisen voldoen (gescreend, geheimhoudingsverklaring, e.d.);
- De bewaartermijn moet zo kort mogelijk zijn.

Deze eisen zijn afgeleid uit het onderzoek dat de Autoriteit Persoonsgegevens deed op een bedrijventerrein in Vianen.⁷

Noot 7 <https://autoriteitpersoonsgegevens.nl/nl/nieuws/onderzoek-cameratoezicht-bedrijventerrein-vianen>.

In veel gemeenten is de discussie hierover ingewikkeld door organisatorische, financiële en soms ook ideologische discussies over de rol van de overheid versus de rol van het bedrijfsleven. Het vergt bestuurlijke moed, juridische kennis en ook wat gezond verstand om publiek-private samenwerking te laten slagen. Vooral als de gemeente bereid is subsidie te geven aan private bewakingscamera's op bedrijventerreinen leidt dat vaak tot de begrijpelijke neiging ook juridisch de verantwoordelijkheid te willen dragen. Dat is niet nodig en ook niet verstandig: gemeenten kunnen een organisatie een subsidie geven zonder dat ze daardoor meteen verantwoordelijk zijn voor alles wat er met dat geld wordt gedaan.

Rol van de politie

Bij publiek-private samenwerking is de politie vaak niet zo actief betrokken als bij gemeentelijk cameratoezicht. Meestal is de politie wel een van de ondertekenaars van een convenant, maar worden de opgenomen camerabeelden uitsluitend na incidenten aan de politie geleverd. Wel kan de politie vaak ondersteunen bij het uitkiezen van de meest geschikte locaties om de camera's te plaatsen.

3.5 Samenvattend

- Camera's kunnen op drie manieren werken: preventief (vooraf), door *live* meekijken (tijdens) of door opsporing (achteraf);
- Voor preventie is communicatie het belangrijkste: mensen moeten weten dat er camera's zijn en daar hun gedrag op aanpassen;
- Bij rechtstreeks cameratoezicht is er een groot verschil tussen continu cameratoezicht en alarmafhandeling. De kosten verschillen ook sterk: cameratoezicht is veel kostbaarder dan alarmafhandeling;
- Live View is een manier om private camerabeelden via poortwachter zoals Particuliere Alarm Centrales, rechtstreeks in de 112-meldkamer te kunnen bekijken;
- Achteraf gebruik van camerabeelden voor opsporing wordt ondersteund door het project Camera in Beeld: een landelijke database waar particulieren hun bewakingscamera's kunnen aanmelden;
- De betrokkenheid van de politie bij gemeentelijk cameratoezicht is in Nederlandse gemeenten zeer verschillend georganiseerd;
- Voor publiek-private samenwerking is het van belang de rollen tussen gemeente, politie en ondernemers duidelijk te verdelen en schriftelijk vast te leggen, bijvoorbeeld in een convenant.

4 Techniek: wat kan er?

4.1 Slimme camera's

Er zijn grote verschillen tussen camera's in beeldkwaliteit, robuustheid, weersbestendigheid en storingsgevoeligheid. Ook de technologie in de camera zelf is zeer divers. Sommige camera's kunnen dankzij infrarood ook in het donker of bij slecht weer een redelijk beeld opleveren. Andere camera's hebben twee lenzen naast elkaar – net als de menselijke ogen – waardoor het mogelijk is afstand te schatten. Daar zit dan uiteraard wel een ander prijskaartje aan vast. Dat is het onderwerp van het volgende hoofdstuk.

Ook de functionaliteit verschilt enorm. Sommige camera's filmen altijd dezelfde plek: de vaste camera's. Maar er zijn ook camera's die kunnen draaien en inzoomen. Dat is heel handig voor live toezicht, maar minder geschikt voor een situatie waarin er behoefte is aan een continu overzicht. Een oplossing die momenteel erg populair is, is de gecombineerde 360° camera – hieronder rechts weergegeven.



De gecombineerde 360° camera lost een probleem op waar alle andere camera's mee te kampen hebben. Als de camera naar links wordt gericht, is het onzichtbaar wat er rechts gebeurt. Zo kan het gebeuren dat incidenten die bij wijze van spreken recht onder de camera gebeuren soms toch niet in beeld zijn. Dankzij de gecombineerde camera is dat geen probleem meer. Die bestaat namelijk uit vier camera's die in een cirkel zijn gemonteerd voor een continu overzichtsbeeld, gecombineerd met een bedienbare camera daaronder die een

bepaalde kant op kan worden gericht. Bijkomend voordeel is dat geautomatiseerde analyse van camerabeelden, zoals kentekenherkenning of gedragsherkenning, veel beter werkt met vaste camera's dan draaibare camera's.

4.2 Artificial Intelligence

Naarmate het aantal camera's groeit, neemt ook de behoefte toe aan “slimme camera's”. Daarmee wordt gedoeld op hardware of software die een deel van het menselijke werk kan automatiseren. Bijvoorbeeld door kentekens automatisch te lezen en te vergelijken met een referentiebestand. Of door gedrag te herkennen en automatisch alarm te slaan bij de politie als er geweld wordt gepleegd.

Een OV-bedrijf heeft onderzoek laten uitvoeren naar slimme camera's. De vraag was of het mogelijk was om een deel van het werk dat de toezichthouders in de cameracentrale doen te automatiseren. Er is onderzoek gedaan in vier landelijke toezichtcentrales en er zijn interviews gevoerd met een groot aantal experts. De conclusie was heel duidelijk: slimme cameratoepassingen zijn in theorie heel veelbelovend, maar in de praktijk vallen de resultaten eigenlijk altijd tegen. Leveranciers beloven vaak meer dan ze kunnen waarmaken én opdrachtgevers en eindgebruikers hebben vaak veel te hoge verwachtingen van de techniek. Slimme camera's denken niet zelf na, dus ze moeten worden getraind door mensen en optimaal ingeregeld voor de situatie ter plaatse. Veel organisaties die slimme camera's willen hebben zijn niet bereid de investeringen te doen die daarvoor nodig zijn.

Deze sombere conclusie geldt overigens niet voor alle soorten “slim cameratoezicht”: er zijn twee uitzonderingen op. Automatische kentekenherkenning (ANPR) werkt namelijk heel goed, net als bewegingsdetectie. Maar ingewikkelder analyses zijn onmogelijk aan een camera over te laten. Camera's “zien” namelijk niet zoals mensen kunnen zien. Camera's zijn nog net zo blind voor de betekenis van objecten, personen en bewegingen als ze vijftig jaar geleden waren. Waar wij als mens direct zien dat een duif niet zal gaan inbreken in een woning, kan een slimme camera toch alarm slaan. Ook het vergelijken van gezichten levert soms “matches” op waar mensen niets van begrijpen omdat het totaal verschillende personen zijn. De verhouding tussen het aantal vals positieven (wel alarm, maar geen incident) en het aantal vals negatieven (wel een incident, maar geen alarm) is moeilijk optimaal te krijgen. Daarom zijn er vaak forse investeringen nodig in camera's, verbindingen, servers, verlichting, beheer, onderhoud en personeel om Video Content Analyse optimaal in te richten. De kosten daarvan zijn vaak zo hoog dat er niet voor wordt gekozen. Er zijn veel succesvolle experimenten die niet kunnen worden opgeschaald, terwijl de techniek soms precies doet wat vooraf

was afgesproken. De eindgebruikers klagen vaak over al die valse alarmen, terwijl de leverancier heel trots is op de prestaties van de software. Maar alles overziend staat Video Content Analyse bij veel ervaringsdeskundigen nog altijd bekend als: ‘Unable to do what it says on the box’.

4.3 Technieken die wel werken

Domme, maar oplettende camera's

Zoals gezegd zijn computers dan wellicht niet zo slim als we zouden willen, maar ze zijn wel veel sneller, betrouwbaarder en daardoor veel beter dan mensen in het uitvoeren van “domme” en repeterende werkzaamheden. Mensen vallen na acht uur in slaap, maar een computer kan dag en nacht doorgaan met eenvoudige algoritmes. In veel digitale camera's is dat soort intelligentie gratis ingebouwd.

Dan gaat het bijvoorbeeld om bewegingsdetectie: er gaat dan een alarm af in de centrale als er iets in beeld beweegt. Dat kan heel nuttig zijn op een rangeerterrein van een spoorbedrijf waar 's nachts niemand mag komen.

Bewegingsdetectie kan ook slim worden ingezet door het tegenovergestelde: een alarm als er te lang *niets* in beeld beweegt. Dan is de camera stuk of heeft iemand er wellicht iets overheen gegooid om de camera onbruikbaar te maken. Een andere slimme analyse op basis van bewegingsdetectie is *virtual fencing*: een alarm als er op een specifieke plek in beeld iets beweegt, zoals achter een hek of slagboom. Ook het algoritme voor *left luggage* werkt goed: dit soort camera's geeft een melding als ergens iets wordt neergezet en bijvoorbeeld langer dan vijf minuten blijft staan. Wel werken dit soort analyses alleen maar bij vaste camera's die altijd dezelfde plek in beeld brengen.

Multi-sensor

Wat ook goede resultaten oplevert is de combinatie van een camera met een andere sensor om de betrouwbaarheid van de analyse te vergroten. Net zoals mensen beeld, geluid, geur en temperatuur combineren als ze zeker willen weten of er ergens brand is, kunnen camera's veel betere beoordelingen maken als er informatie uit een ander “zintuig” of een andere sensor wordt gekoppeld. De beste sensor die camera's kan helpen is de mens: als iemand een alarmknop of informatiekноп indrukt kan de dichtstbijzijnde camera in de alarmcentrale worden geactiveerd en automatisch worden gericht op de plek waar die knop of dat alarm is ingedrukt (lift, roltrap, SOS- of informatiezuil). Daarna kan het alarm door de centralist worden afgehandeld op de normale wijze, maar dan aangevuld met beeldmateriaal voor een beter omgevingsbeeld.

Automatische triggers zoals bewegingsdetectie werken goed, maar leveren pas echt interessante informatie op als op meer dan alleen camerabeelden zijn gebaseerd. Andere sensoren die de camera ondersteunen helpen dan veel. Een rookmelder of thermometer kan bepalen of er brand is of mist. Een inductielus in het asfalt kan bevestigen of er een vrachtwagen langsrijdt of dat er een wolk een schaduw over de weg trekt. Dergelijke technieken zijn echter vrij kostbaar en worden dus alleen ingezet in kritieke infrastructuur of situaties waarin het de moeite loont hierin te investeren.

Een goed uitgangspunt bij het overwegen van slimme camera's is om alleen samen te werken met ervaren en verantwoordelijke leveranciers. Veel onervaren leveranciers beweren dat technisch alles kan, maar dat is zeker niet het geval. Niet de beschikbare techniek zou leidend moeten zijn (aanbodgestuurd), maar de behoefte van de opdrachtgever (vraaggestuurd).

4.4 Samenvattend

- Camera's zijn er in alle soorten en maten;
- Slimme camera's zijn er nog niet echt: er zit een groot gat tussen de beloftes van leveranciers en de wensen van de klanten;
- Wat wel goed werkt is automatische kentekenherkenning en bewegingsdetectie;
- Camera's kunnen eenvoudige analyses veel sneller, betrouwbaarder en grootschaliger uitvoeren dan mensen;
- Het aantal valse alarmen (vals positief) is vaak zo groot dat slimme camera's minder gevoelig worden afgesteld; maar daardoor wordt de kans dat een boef ongezien zijn slag kan slaan (vals negatief) vaak onacceptabel groot;
- Om slimme camera's optimaal in te regelen is vaak onvoldoende tijd en geld beschikbaar;
- De combinatie van camera's (beeld) met andere sensoren (geluid, temperatuur, radar, inductielussen) vergroot de betrouwbaarheid van sensorsystemen aanzienlijk.

5 Financieel: wat kost het?

5.1 Verschillende kostenposten

De kosten van cameratoezicht kunnen moeilijk in algemene termen worden besproken. De kosten hangen af van de camera's die worden aangeschaft, maar ook van de bijbehorende software en hardware. Die kosten vallen vaak veel hoger dan de kosten van de camera's zelf: verbindingen, opslagserver, toezichtcentrales, personeelskosten voor *live* toezicht, softwarelicenties, onderhoud, verzekeringen en dergelijke. Een deel van die kosten is niet eenmalig zoals de aanschaf van de camera's, maar een jaarlijks terugkerende kostenpost.

Een goedkope bewakingscamera van Ring is te koop vanaf circa vijftig euro. Een professionele camera zoals die door de overheid wordt gebruikt kost al snel het tienvoudige. Camera's met extra's zoals infrarood of radar zijn nog duurder. De multi-camera die in het vorige hoofdstuk werd besproken met vier vaste camera's en een bedienbare camera daaronder kost circa € 4.500. Een enkele dome-camera van dezelfde leverancier kost € 2.500 (prijspeil 2018).

Een belangrijke kostenpost is de infrastructuur: als een bestaand glasvezelnetwerk kan worden gebruikt voor het datatransport zijn er geen extra verbindingen nodig en zijn de kosten voor beheer van het netwerk meestal elders al gedekt. Maar als er een nieuwe breedbandaansluiting moet worden aangelegd lopen de kosten daarvan al zeer snel op.

5.2 Gemeentelijk cameratoezicht

Ondernemers maken de kosten van camerabewaking meestal niet openbaar bekend. Daar valt dus weinig over te zeggen. De kosten van gemeentelijke cameraprojecten worden iets vaker openbaar gemaakt dan van private camerabewaking.

Uit twee inventarisaties van tien respectievelijk vijf jaar geleden, blijkt dat de gemiddelde kosten voor realisatie van een gemeentelijk cameraproject in 2010

circa €300.000 bedroegen en in 2014 circa €500.000. Dit tweede bedrag was gebaseerd op relatief grote gemeenten met veel camera's. Het goedkoopste cameraproject kostte €90.000 en het duurste project kostte €1,5 miljoen. Per camera waren de aanschafkosten gemiddeld €17.000, dus dat is inclusief verbindingen, opslag en toezichtcentrale. Die kosten per camera worden niet lager als er meer camera's worden aangeschaft, omdat er dan vaak relatief veel geld nodig is voor lange verbindingen over grotere afstanden.

De kosten voor beheer, onderhoud en vervanging bedroegen in 2010 gemiddeld € 70.000 per camerasysteem per jaar; in 2014 was dat – voor een aantal relatief grote gemeenten – gemiddeld € 100.000 per jaar.⁸ Dat is inclusief het rechtstreekse toezicht. In gemeenten waar de beelden niet rechtstreeks worden bekeken zijn de jaarlijkse kosten laag (ca. € 1.000,- per camera per jaar); in gemeenten met veel rechtstreeks toezicht zijn de jaarlijkse kosten hoog (circa € 10.000,- per camera per jaar).

Deze bedragen zijn nog redelijk actueel, blijkt uit informatie uit twee gemeenten. In een gemeente met tachtig camera's werd in de negen jaar van 2013 tot en met 2021 in totaal €1,6 miljoen aan het cameratoezicht gespendeerd: de aanschafkosten waren €300.000 en jaarlijks werd €150.000 uitgegeven aan verbindingen, opslag, *live* toezicht en onderhoud.

In de gemeente Utrecht bedragen de kosten van het gemeentelijke camerasysteem circa €800.000 per jaar. Daarvan is ongeveer de helft voor beheer en onderhoud van de camera's, verbindingen en toezichtcentrale. De andere helft is voor het *live* uitkijken van de camera's.

5.3 Kosten en baten van cameratoezicht

De kosten van cameratoezicht zijn hoog. Maar dat wil niet zeggen dat het geld ten onrechte is uitgegeven. Cameratoezicht levert immers als het goed is ook baten op: criminaliteit kost de samenleving geld en als camera's criminaliteit voorkomen verdienen ze zichzelf als het ware terug.

Voor de gemeente Utrecht is uitgerekend of de gemeentelijke camera's meer opleveren dan ze kosten of andersom.⁹ Zo'n berekening is niet eenvoudig te maken, omdat er allerlei aannames moeten worden gedaan. Ook is een deel van de kosten en baten niet goed te meten, zoals veiligheidsgevoel of immateriële

Noot 8 Zie: A. Schreijenberg en G. Homburg (2010), *Steeds meer beeld; Evaluatie vijf jaar cameratoezicht op openbare plaatsen*, Regioplan, Amsterdam.

Zie ook: S. Flight (2013), *Cameratoezicht in Nederland: een schets van het Nederlandse cameralandschap*, Ministerie van Justitie/WODC: Den Haag (<https://repository.wodc.nl/handle/20.500.12832/2065>).

Noot 9 Zie: DSP-groep (2018), *Evaluatie cameratoezicht Utrecht 2018*, Amsterdam.

kosten zoals leed en emotionele schade voor slachtoffers. Op basis van een Brits model voor de kosten van criminaliteit kunnen de kosten van verschillende soorten criminaliteit worden geschat. Een vernieling kost de samenleving circa €2.000, terwijl een mishandeling circa €21.000 aan materiële en immateriële kosten met zich meebrengt.

Dat betekent dat cameratoezicht zichzelf relatief snel terugverdient als er mishandelingen mee worden voorkomen. In het concrete rekenvoorbeeld voor de gemeente Utrecht was de conclusie dat de camera's zichzelf zouden terugverdienen in het centrum van de stad als ze circa 40 mishandelingen zou kunnen voorkomen (van de naar schatting 500 geweldsdelicten die jaarlijks binnen het blikveld van de camera's worden gepleegd).

Maar als gemeentelijke camera's worden opgehangen in gebieden waar vernielingen worden gepleegd, moeten er ruim vierhonderd vernielingen per jaar mee worden voorkomen om een positieve balans te bereiken.

Ten tweede laat de analyse zien dat preventie van incidenten veel meer baten oplevert dan opsporing achteraf. Want in het laatste geval is de criminaliteit wel degelijk gepleegd (met de bijbehorende schade en andere kosten) en moet de politie een opsporingsonderzoek uitvoeren (met de kosten daarvan). Voorkomen is dus beter dan genezen vanuit het perspectief van de slachtoffers van criminaliteit, maar het is dus ook nog eens veel beter voor de kosten-baten balans van cameratoezicht.

5.4 Slimme camera's

De reden om slimme camera's te willen invoeren is vaak kostenbesparing: er zijn dan minder mensen nodig, is het idee. De kosten van dergelijke camerasystemen zijn echter niet lager, maar hoger dan reguliere camerasystemen die alleen door mensen worden bekeken. Want voor slimme cameratoepassingen is meer personeel nodig voor onderhoud en beheer: geen enkel "intelligent camerasysteem" kan op zichzelf functioneren. Er is voortdurende *fine tuning* nodig. Een alarmcentrale die met slimme toepassingen werkte ontdekte dat er voor elke zes centralisten één extra medewerker nodig was om de applicaties voortdurend bij te stellen op basis van de ervaringen. Daar kwam nog overkoepelend technisch beheer van de hardware, software en verbindingen bij. Een netwerk met slimme sensoren moet eigenlijk als een soort levend organisme worden beschouwd dat voortdurend moet worden gemonitord. Licenties moeten worden bijgewerkt, software-updates moeten worden geïmplementeerd en nieuwe functionaliteiten moeten worden geïnstalleerd. Ook dat brengt (soms hoge) kosten met zich mee die elk jaar opnieuw moeten worden opgebracht om te voorkomen dat het systeem vastloopt. Veel grote organisaties als Schiphol

kiezen er uit financiële overwegingen vaak voor geen slimme cameratechnieken in te voeren.

5.5 Samenvattend

- Camera's zijn te koop voor enkele tientjes tot enkele duizenden euro's per stuk, afhankelijk van de kwaliteit en bijzondere extra functies;
- De kosten van cameratoezicht hangen niet alleen af van de camera's, maar ook van de verbindingen, toezichtcentrale, personeelskosten, opslag, onderhoud en verzekeringen;
- Kosten van private camerasystemen zijn niet bekend;
- De kosten van gemeentelijke cameraprojecten bedragen in relatief grote gemeenten ongeveer €300.000 tot €500.000 voor de aanschaf van de camera's, verbindingen, centrale en opslag;
- De jaarlijks terugkerende kosten hangen sterk af van de hoeveelheid *live* toezicht: in Utrecht kost dat ongeveer €400.000 per jaar;
- Camera's kunnen zichzelf terugverdienen omdat ze ook baten opleveren;
- De kosten-baten balans is het snelst positief te krijgen als camera's worden ingezet tegen "dure" criminaliteit (mishandelingen, bijvoorbeeld) en als ze worden gericht op preventie in plaats van opsporing achteraf;
- Slimme camera's worden vaak ingezet om te besparen op personeelskosten in de toezichtcentrale, maar de ervaring leert dat de voortdurende *fine tuning* en het technisch beheer de kosten van dit soort camerasystemen juist hoger maakt dan reguliere cameraprojecten.