

Extra cameratoezicht
in en rond het
Centraal Station

A.H.C.M. Smeets

Camera's in het publieke domein

Privacynormen voor het cameratoezicht op de
openbare orde

INHOUD

A.H.C.M. Smeets

Camera's in het publieke domein

[INHOUD](#)

Privacynormen voor het cameratoezicht op de openbare orde

Publicaties in de serie achtergrondstudies en verkenningen zijn het resultaat van onderzoeken uitgevoerd door of in opdracht van het College bescherming persoonsgegevens (CBP). Met het uitbrengen van deze publicaties beoogt het CBP de discussie en de meningsvorming te stimuleren over ontwikkelingen in de samenleving waarbij de persoonlijke levenssfeer van de burger in het geding is. In veel gevallen wordt in de publicaties het normatieve kader zoveel mogelijk praktisch uitgewerkt voor het onderwerp van de studie. Het CBP wil hiermee een handreiking geven voor het realiseren van de eigen verantwoordelijkheid die de wet een ieder geeft voor de bescherming van persoonsgegevens.

COLOFON

Camera's in het publieke domein. Privacynormen voor het cameratoezicht op de openbare orde.

College bescherming persoonsgegevens, Den Haag, november 2004.

ISBN 90-74087-35-3

COLLEGE BESCHERMING
PERSOONSGEGEVENS

Prins Clauslaan 20
Postbus 93374
2509 AJ Den Haag

TELEFOON 070 381 13 00
FAX 070 381 13 01

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotocopie, microfilm of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van het College bescherming persoonsgegevens.

Ontwerp en opmaak: Proforma, strategie, ontwerp en management: M. Monster
Druk: Deltahage bv

Ten geleide

De belangstelling voor cameratoezicht is in de afgelopen jaren alleen maar toegenomen. Bedrijven en overheden zetten op grote schaal camera's in voor de beveiliging van gebouwen, goederen en personen. Cameratoezicht is min of meer vanzelfsprekend geworden in supermarkten, winkelcentra, het openbaar vervoer en uitgaansgebieden. Camera's worden door het brede publiek geaccepteerd in de verwachting dat cameratoezicht effectief is.

De Registratiekamer – de voorloper van het College bescherming persoonsgegevens (CBP) – publiceerde al in 1997 een studie over de mogelijkheden en grenzen van cameratoezicht. *In beeld gebracht* gaf privacyregels voor het toepassen van cameratoezicht zowel in het particuliere als het publieke domein. Met in achtneming van deze regels achtte de toezichthouder cameratoezicht zeker mogelijk.

Cameratoezicht door de overheid nam vooral na 2000 toe. In 2003 heeft het CBP onderzoek laten doen naar aard en omvang van het cameratoezicht door de Nederlandse gemeenten. Uit dit onderzoek bleek onder meer dat 20 procent van de gemeenten gebruik maakte van camera's en dat in veel van die gemeenten de effectiviteit van het toezicht (nog) niet geëvalueerd was. In behandeling bij het parlement is het wetsvoorstel om de Gemeentewet te wijzigen, opdat cameratoezicht ter handhaving van de openbare orde een expliciete wettelijke basis krijgt.

In *Camera's in het publieke domein* geeft het CBP een praktische verheldering van de privacy-normen die nuttig kan zijn bij de besluitvorming binnen gemeenten over de inrichting van cameratoezicht ter handhaving van de openbare orde. Verder zal het CBP in samenwerking met belanghebbende partijen in 2005 een model-verordening cameratoezicht publiceren.

Vanzelfsprekend zal het CBP deze normen ook hanteren bij zijn toezicht op de praktijk van het cameratoezicht in het publieke domein.

Ulco van de Pol
collegelid

Inhoudsopgave

Ten geleide 3

Inhoudsopgave 5

Definities 7

Vuistregels 9

1 Cameratoezicht in het publieke domein

- 1.1 Omvang van het cameratoezicht 13
- 1.2 Technische mogelijkheden 14
- 1.3 Maatschappelijke discussie 14
- 1.4 Wijzigingen van het wettelijk kader 15

2 Juridische bronnen

- 2.1 Europese rechtsbronnen 19
- 2.2 Nederlandse rechtsbronnen 22

3 Juridisch kader

- 3.1 Openbare plaats in het publieke domein 27
- 3.2 Redelijke verwachting van respect voor de persoonlijke levenssfeer 30
- 3.3 Het verwerken van persoonsgegevens 33
- 3.4 Grondslag voor de verwerking 35
- 3.5 Doel van de verwerking 35
- 3.6 Noodzakelijkheid en selectiviteit 37
- 3.7 Verantwoordelijke en regie 38
- 3.8 Verder gebruik 40
- 3.9 Kwaliteit van gegevens 40
- 3.10 Beveiliging 41
- 3.11 Kenbaarheid 41
- 3.12 Bewaartermijn 42
- 3.13 Rechten van betrokkenen 42
- 3.14 Melding, reglementspllicht, verordening 44

4 Privacynormen voor de praktijk

- 4.1 Publiek domein en openbare plaats 47
- 4.2 Redelijke verwachting van respect voor de persoonlijke levenssfeer 48
- 4.3 Het verwerken van persoonsgegevens 50
- 4.4 Grondslag voor de verwerking 51
- 4.5 Doel van de verwerking 51
- 4.6 Noodzakelijkheid en selectiviteit 52
- 4.7 Verantwoordelijke en regie 54
- 4.8 Verder gebruik 55
- 4.9 Kwaliteit van gegevens 56
- 4.10 Beveiligingsplicht 56
- 4.11 Kenbaarheid 57
- 4.12 Bewaartermijn 57
- 4.13 Rechten van betrokkenen 57
- 4.14 Melding van verwerkingen en reglementspllicht 59

Bijlagen

- 1 Samenvatting *Cameratoezicht in de openbare ruimte* 2003 60
- 2 Achtergrondstudies en verkenningen 63

Definities

- 1 Wat is een openbare plaats?**
Een openbare plaats is een voor het publiek vrij toegankelijke plaats. Er zijn geen belemmeringen voor de burger om die plaats te betreden.
- 2 Wat zijn persoonsgegevens?**
Persoonsgegevens zijn gegevens over een geïdentificeerde of identificeerbare natuurlijke persoon. Persoonsgegevens zijn medebepalend voor de wijze waarop de betrokken persoon wordt beoordeeld of behandeld.
- 3 Wanneer zijn camerabeelden persoonsgegevens?**
Camerabeelden zijn persoonsgegevens als herkenning of identificatie van de betrokken persoon redelijkerwijs mogelijk is.
- 4 Wat is een verwerking van persoonsgegevens?**
Alle handelingen die mogelijk zijn met opgeslagen camerabeelden zijn verwerkingen van persoonsgegevens.
- 5 Wat is een verantwoordelijke?**
Een verantwoordelijke is diegene die formeel zeggenschap heeft over de verwerking van persoonsgegevens. De verantwoordelijke voor de verwerking van camerabeelden ten behoeve van de handhaving van de openbare orde is de burgemeester.
- 6 Wat is een bewerker?**
Een bewerker is een persoon of organisatie die op grond van een overeenkomst tussen verantwoordelijke en bewerker de camerabeelden uitkiijkt en verwerkt. Er is tussen de verantwoordelijke en de bewerker geen gezagsrelatie.
- 7 Wat is een betrokkene?**
Een betrokkene is diegene over wie de gegevens informatie bevatten. Een betrokkene is dus een ieder van wie camerabeelden worden vastgelegd.
- 8 WBP**
De Wet bescherming persoonsgegevens regelt – kort gezegd – of en wanneer persoonsgegevens mogen worden verwerkt. Er worden in deze wet eisen gesteld aan de wijze van verwerking. Voorts geeft de wet regels voor het toedelen van de verantwoordelijkheid voor de verwerking en de rechten van betrokkenen.
- 9 WPOLR**
De Wet politieregisters regelt de verwerking van persoonsgegevens door de politie ten behoeve van de uitvoering van de politietaak. In deze wet is aansluiting gezocht bij begrippen uit de WBP.
- 10 WPOLG**
De Wet politiegegevens zal de Wet politieregisters vervangen als wettelijk kader of regime voor de gegevensverwerkingen van de politie ten behoeve van de politietaak.
- 11 Gewijzigde Gemeentewet**
Onder de gewijzigde Gemeentewet wordt hier verstaan de invoeging van het artikel 151c, waarin een specifieke grondslag wordt gegeven voor cameratoezicht ten behoeve van de handhaving van de openbare orde in het publieke domein.

Vuistregels

De inrichting van cameratoezicht in het publieke domein

Onderstaande lijst van vragen, uitgangspunten en definities vormt een beknopte checklist voor de concrete inrichting van cameratoezicht op openbare plaatsen. Deze punten hebben steeds betrekking op cameratoezicht in het publieke domein met het oog op de handhaving van de openbare orde.

Vragen voor besluitvorming

1 Wanneer kan cameratoezicht ingezet worden?

Cameratoezicht kan worden ingezet als dit noodzakelijk is voor het doel van de toepassing, dat wil zeggen voor de handhaving van de openbare orde. Het cameratoezicht moet zo selectief, dat wil zeggen zo beperkt mogelijk zijn in aard, omvang, intensiteit en duur. Hierbij dient rekening gehouden te worden met de context en de gevoeligheid van de daarin opgenomen beelden. Een prostitutiebuurt is bijvoorbeeld een gevoeliger context dan een winkelstraat. Cameratoezicht moet altijd onderdeel zijn van een pakket maatregelen. De noodzaak van het cameratoezicht dient ook te blijken uit periodieke evaluaties van de inzet van dit middel.

2 Op welke grondslag mag cameratoezicht worden ingezet?

De burgemeester draagt verantwoordelijkheid voor de openbare orde. Hij kan zich voor cameratoezicht onder de WBP dan ook beroepen op zijn publiekrechtelijke taak ingevolge de Gemeentewet. Na inwerkingtreding van de gewijzigde Gemeentewet zal deze wet de specifieke grondslag zijn voor het cameratoezicht. De gemeenteraad dient dan een verordening op te stellen waarin het cameratoezicht nader wordt geregeld.

3 Waar mag cameratoezicht worden ingezet?

Cameratoezicht voor de handhaving van de openbare orde mag in principe alleen worden toegepast in openbare plaatsen. De selectie van de plaatsen waar cameratoezicht zal worden ingezet dient gemotiveerd te worden. Cameratoezicht moet zo selectief mogelijk toegepast worden, waarbij ook rekening gehouden moet worden met het aantal camera's, het aantal uren van toezicht en het aantal mensen dat in beeld gebracht wordt. Overleg binnen de 'driehoek' van burgemeester, politie en openbaar ministerie over de inzet van cameratoezicht is gewenst.

4 Heeft een burger in het publieke domein nog wel recht op privacy?

De overheid moet ook in het publieke domein rekening houden met de redelijke verwachting van de burger ten aanzien van respect voor zijn persoonlijke levenssfeer. Welke verwachting redelijk is, zal van plaats tot plaats verschillen. De burger mag in het algemeen op openbare plaatsen minder respect voor zijn persoonlijke levenssfeer verwachten dan in zijn huis of op zijn werkplek. De context is dus bepalend voor de verwachting.

5 Wat is het doel van het cameratoezicht?

Het doel van cameratoezicht moet helder beschreven zijn. Het is sterk aan te bevelen neven-doelen zoals opsporing van strafbare feiten en de efficiënte en veilige inzet van hulpdiensten expliciet te benoemen.

6 Wie is verantwoordelijk voor het cameratoezicht?

De verantwoordelijke voor de verwerking van de camerabeelden in de zin van de WBP is de burgemeester, ook als in de praktijk de operationele regie in handen van de politie is. Dit geldt ook als onder regie van de politie het cameratoezicht feitelijk geheel door een bedrijf wordt uitgevoerd.

7 Welk wettelijk regime geldt voor cameratoezicht?

De gemeente kan tot de inwerkingtreding van de gewijzigde Gemeentewet, kiezen voor het wettelijk regime van de WBP of de WPOLR. Kiest de gemeente voor de WBP, dan dient er een melding bij het CBP of de gemeentelijke functionaris voor gegevensbescherming gedaan te worden. Kiest de gemeente voor de WPOLR, dan is een reglement verplicht.

8 Wat verandert er bij de inwerkingtreding van de gewijzigde Gemeentewet?

Na inwerkingtreding van de gewijzigde Gemeentewet vallen de bestanden met de camerabeelden onder de WPOLR. Na inwerkingtreding van de nieuwe wet politiegegevens, vervalt de reglementsplicht van de WPOLR. Ook dan moet een regeling voor het cameratoezicht in het publieke domein worden vastgesteld.

Uitgangspunten voor inrichting en uitvoering

9 De politie heeft de operationele regie.

De burgemeester is bij het toezicht op de openbare orde de verantwoordelijke, maar de operationele regie zal in vrijwel alle gevallen bij de politie liggen. Onder het toekomstige artikel 151c Gemeentewet zal dit altijd zo zijn. Ook bij publiek-private samenwerking waarbij cameratoezicht feitelijk door een particuliere organisatie wordt uitgevoerd, is de burgemeester verantwoordelijk en houdt de politie de regie.

10 Cameratoezicht mag niet verborgen zijn.

Cameratoezicht moet voor het publiek duidelijk kenbaar zijn. Heimelijk cameratoezicht ten behoeve van de handhaving van de openbare orde is niet toegestaan.

11 Camerabeelden moeten afdoende beveiligd worden.

De beelden moeten correct, niet manipuleerbaar en voor een selecte groep functionarissen toegankelijk zijn.

12 Camerabeelden mogen niet langer dan noodzakelijk bewaard worden.

Beelden mogen niet langer dan noodzakelijk is, worden bewaard. In het wetsvoorstel cameratoezicht op openbare plaatsen wordt voorgesteld, onder normale omstandigheden een bewaartermijn van zeven dagen te hanteren. Beelden waarop ernstige incidenten waarneembaar zijn, worden overgebracht naar een onderzoeksdossier.

13 Camerabeelden mogen niet zomaar voor andere doelen gebruikt worden.

Verdere verwerking van de beelden (verder dan nodig is voor de handhaving van de openbare orde) is als regel niet toegestaan. Beelden mogen alleen verder verwerkt worden voor de doelen die van te voren expliciet zijn vastgesteld bij de inrichting van het cameratoezicht, tenzij er sprake is van concrete opsporingsdoelen of noodsituaties waarin acuut de hulpverlening op gang moet komen.

Rechten van betrokkenen, toezicht en evaluatie

14 Betrokkenen hebben rechten.

Betrokkenen (zie definitie onder 23) hebben recht op inzage in de beelden en de daaraan gekoppelde gegevens en vastgelegde interpretaties. Daarnaast hebben zij recht om te verzoeken om correctie, afscherming en verwijdering. De uitoefening van deze rechten moet concreet geregeld worden. Deze regeling dient op verzoek aan het publiek bekend gemaakt te worden.

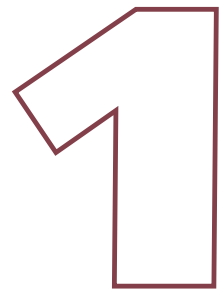
15 Het CBP is toezichthouder voor cameratoezicht.

Het CBP houdt toezicht op de verwerking van camerabeelden door verantwoordelijken, zowel onder de WBP als onder de WPOLR en de toekomstige WPOLG. Toezicht kan ook worden gehouden door een gemeentelijke functionaris voor de gegevensbescherming.

16 Cameratoezicht dient periodiek geëvalueerd te worden.

Cameratoezicht is als middel rechtmatig zo lang als het een noodzakelijk middel blijkt te zijn. Hiertoe moet deze effectiviteit periodiek onderzocht worden. Onder de gewijzigde Gemeentewet rapporteert de burgemeester hierover aan de gemeenteraad.

Cameratoezicht in het publieke domein



- 1.1 Omvang van het cameratoezicht 13
- 1.2 Technische mogelijkheden 14
- 1.3 Maatschappelijke discussie 14
- 1.4 Wijzigingen van het wettelijk kader 15

De laatste jaren is de belangstelling voor cameratoezicht in het publieke domein sterk toegenomen. Cameratoezicht wordt gezien als een snelle oplossing voor allerlei veiligheidsproblemen. Op steeds meer plaatsen hangen camera's, zowel op de openbare weg als in semi-openbare gebieden. Deze camera's worden niet alleen geplaatst door overheden, meestal gemeenten, maar ook door bedrijven in winkelgebieden en rond bedrijventerreinen.

In 1997 concludeerde de voormalige Registratiekamer in de studie *In beeld gebracht, Privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging*, dat cameratoezicht in het publieke domein toegestaan was als aan een aantal voorwaarden werd voldaan. In de studie werden vuistregels geformuleerd voor het vormgeven van cameratoezicht. Deze regels waren bedoeld als hulp bij de afweging wel of geen camera's in te zetten in het publieke domein. Ook werd gestreefd naar zo duidelijk mogelijke richtlijnen met het oog op de rechtmatigheid van het cameratoezicht. Gegevens over de omvang van cameratoezicht waren toen niet beschikbaar.

De studie *In beeld gebracht* uit 1997 behoeft herziening, mede naar aanleiding van de uitbreiding van het cameratoezicht in het publieke domein. In de tussentijdse jaren heeft het CBP veel voorlichtingszaken behandeld ten aanzien van dit cameratoezicht, diverse gemeenten bezocht, meegewerkt aan de handreiking cameratoezicht van het Ministerie van Justitie en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties uit 2000, een enquête gehouden onder alle gemeenten in Nederland en verschillende gemeenten geïnterviewd naar aanleiding van die enquête.

Deze vernieuwde studie is bedoeld om eenieder die te maken heeft met de handhaving van de openbare orde in het publieke domein door middel van cameratoezicht een vernieuwd kader te bieden en te ondersteunen bij de beslissing, de inrichting en de uitvoering van dit cameratoezicht.

1.1 Omvang van het cameratoezicht

In 2003 liet het CBP een onderzoek uitvoeren naar de aard en de omvang van het cameratoezicht in het publieke domein. Het onderzoek is uitgevoerd door middel van een enquête onder alle 489 gemeenten in Nederland. Vrijwel alle gemeenten hebben daaraan meegewerkt en hebben inzicht gegeven in de toepassing van cameratoezicht onder verantwoordelijkheid van de gemeentelijke overheid.

Daarmee werd niet al het cameratoezicht in het publieke domein in beeld gebracht. Er zijn immers vormen van cameratoezicht door bedrijfsleven, particulieren of instellingen in gebruik die niet onder de regie van de gemeentelijke overheid vallen. Het gaat dan om cameratoezicht in winkelcentra waarbij tevens openbare winkelpassages in beeld gebracht worden of cameratoezicht ter beveiliging van parkeerterreinen en gebouwen. Stations en de parkeerterreinen die daarbij horen, zijn een ander voorbeeld. Ook gebeurt het dat de plaatselijke horecabedrijven samen voorzien in cameratoezicht waarbij in samenwerking met de politie of gemeenten ook de toegang tot de horecagelegenheden en kleine delen openbaar gebied onder het bereik van de camera's vallen.

Het bleek dat in 93 gemeenten (20%) de gemeentelijke overheid gebruik maakte van camera's. Van deze gemeenten had 14% korter dan een jaar cameratoezicht terwijl 40% van de gemeenten langer dan 1 jaar en korter dan 3 jaar ervan gebruik maakte. Bijna de helft (46%) van de gemeenten met cameratoezicht oefende langer dan drie jaar cameratoezicht uit. Ruim 25% van de gemeenten met cameratoezicht had plannen om het cameratoezicht uit te breiden. Voor gemeenten zonder cameratoezicht gold dat 6% van plan was om cameratoezicht in te voeren. Grote gemeenten zetten relatief vaker cameratoezicht in dan kleinere gemeenten. De meest genoemde locaties voor cameratoezicht waren de uitgaanscentra, stations en haltes voor openbaar vervoer, openbare gebouwen, winkelcentra en speciale buurten.

1.2 Technische mogelijkheden

Ook in technisch opzicht heeft het toezicht op de openbare ruimte met behulp van camera's een grote ontwikkeling doorgemaakt. De technische standaard was in 1997 nog de vaste camera met videoband. Er werden bandopnamen gemaakt die vaak door nieuwe opnamen overschreven werden. Een meerdaagse cyclus was gebruikelijk. Live uitkijken gebeurde niet in alle gevallen. Wilde men een bepaald beeld nog eens terug zien of voor bewijs gebruiken, dan moest meestal de hele band nagekeken worden, een tijdrovende klus.

In de loop van de tijd zijn de technische mogelijkheden vergroot. Beelden worden nu veelal digitaal opgeslagen of op zijn minst op de band gekoppeld aan markeringen die het terugvinden en selecteren van bepaalde beelden gemakkelijker maken. Ook de kwaliteit van de camera's en de opgeslagen beelden is verbeterd. De vaste camera wordt inmiddels steeds minder gebruikt; tegenwoordig installeert men zogenaamde dome's en beweegbare camera's.

De nieuwste systemen maken de herkenning van personen veel gemakkelijker. Het gaat daarbij steeds vaker om het herkennen van personen, niet meer aan de hand van het beeld zelf, maar door middel van vergelijking met een bestand met afbeeldingen, bijvoorbeeld van gezochte personen of van de plaatselijke top 100 van relschoppers of van verdachten van bepaalde delicten. Vereist is wel een goede camerapositie en goed licht. Door de politie van Manchester is in 2003 een uitgebreide proef gedaan met gezichtsherkenning¹. De proef was geen succes. De nauwkeurigheid bij de vergelijking van actuele opnames met opgeslagen beelden bleek te klein.

Het is al wel mogelijk beelden te verwerken bij het opstellen van processen verbaal. Indien een overtreding wordt gesignaleerd binnen de categorie van feiten die men wil aanpakken, worden de beelden opgeslagen als foto of film en vervolgens wordt via een gekoppeld programma een proces verbaal opgesteld compleet met beeld als bewijsmateriaal.

Programma's gekoppeld aan camera's kunnen ook bewegingspatronen herkennen. Dit zijn de early warningsystemen. Met behulp van deze programma's kunnen bewegingen vastgelegd worden en op basis van in te stellen parameters kunnen afwijkende patronen vastgesteld en gesignaleerd worden. Deze toepassing is bruikbaar voor de beveiliging van objecten en gebieden zoals parkeerterreinen en bedrijfsterreinen.

1.3 Maatschappelijke discussie

De Registratiekamer gaf met *In beeld gebracht* een bijdrage aan de toenmalige maatschappelijke discussie over cameratoezicht. Rond het uitkomen van de studie had de Registratiekamer een aantal kwesties rond cameratoezicht behandeld en uitspraken gedaan over de wijze waarop cameratoezicht uitgevoerd zou kunnen worden. De casussen die onder de aandacht van de Registratiekamer werden gebracht, betroffen vooral incidentele toepassingen. Het ging bijvoorbeeld om prostitutiegebieden in enkele grote steden, uitgaansgebieden, enkele winkelgebieden en bedrijventerreinen. Nu zouden sommige van deze plaatsen 'hotspots' genoemd worden.

Tien tot vijf jaar geleden was cameratoezicht een fenomeen dat ter discussie stond. Was het wel nodig om camera's op te hangen? Hoe ver mag cameratoezicht gaan? Wat is nog wel en wat is niet meer gerechtvaardigd en wanneer is het nog rechtmatig? Veiligheid werd beschouwd als een belangrijk thema, maar het recht zich onbespied in het publieke domein te begeven woog zwaar. De vragen over cameratoezicht richtten zich overigens voornamelijk op de mogelijkheden van cameratoezicht. Wat is het doel en kan dat met camera's bereikt worden? Wat betekent dat voor de privacy van omwonenden en bedrijven in de buurt? Welke

waarborgen zijn nodig bij deze vorm van toezicht en beveiliging? Wie beslist over het wel of niet toepassen en wie ging de beelden uitkijken? Zowel burgers als overheden stelden deze vragen. Het recht op bescherming van de persoonlijke levenssfeer mocht niet geschonden worden of in elk geval zo min mogelijk. Burgers vroegen vrijwel niet om toepassing van cameratoezicht. En soms – in het uitgaansgebied van Breda – protesteerden buurtbewoners tegen cameratoezicht in hun directe woonomgeving.

Na 2000 kwam het tot een omslag in het denken over camera's. Inmiddels accepteren burgers camera's op allerlei plaatsen, ook in hun woonomgeving. Zij vragen bestuurders nadrukkelijk om cameratoezicht omdat zij zich in toenemende mate onveilig voelen. Deze beleving van onveiligheid, zeker op bepaalde plaatsen, werd een zwaarder element in de afweging om wel of geen cameratoezicht toe te passen.

Ook het politieke klimaat wijzigde. Handhaving van regels werd zeker na de vuurwerkramp in Enschede en de brand in een café in Volendam een belangrijk onderwerp. Ongewenst gedrag in het kader van de openbare orde werd scherper benoemd. In sommige delen van het land werd in navolging van het New Yorkse voorbeeld gesproken over zero tolerance. In het publieke debat werd en wordt geëist dat de openbare orde beter gehandhaafd wordt en de criminaliteitsbestrijding meer succes boekt. Daarmee is de druk op politie en justitie toegenomen. Tegelijkertijd wordt van politie en justitie verwacht dat zij niet alleen doeltreffender maar ook doelmatiger werken. Camera's kunnen, zo is de algemene overtuiging, daarbij helpen.

Cameratoezicht was aanvankelijk dus een middel dat incidenteel werd toegepast, terwijl privacykwesties zwaar meewogen in de besluitvorming. Tegenwoordig ligt in de discussie de nadruk vooral op handhaving van de openbare orde, bestrijding van criminaliteit en een terugkeer naar een veilige maatschappij. De omvang van het cameratoezicht is navenant toegenomen, ook al is het in Nederland nog niet zover als in Engeland waar voor iedere 14 personen een camera is opgehangen. Bescherming van de persoonlijke levenssfeer lijkt minder belangrijk gevonden te worden.

Deze omslag in de maatschappelijke houding tegenover cameratoezicht betekent overigens dat op belangrijke vragen lang niet altijd een antwoord wordt gezocht. Het is immers nog maar de vraag hoe effectief cameratoezicht is. In hoeverre is de burger ook daadwerkelijk veiliger? En weegt dat op tegen een voortdurend in beeld zijn zodra men zich in het publieke domein begeeft? De zorgvuldige omgang met en gecontroleerde toegang tot deze beelden is in ieder geval noodzaak om ongewenste neveneffecten te vermijden. Ook de inzet van onvolgende ontwikkelde technologie schept risico's voor de bescherming van de persoonlijke levenssfeer, bijvoorbeeld het risico dat er te vaak fouten gemaakt worden bij het aanhouden van verdachten.

1.4 Wijziging van het wettelijk kader

De studie *In beeld gebracht* was gebaseerd op de Wet persoonsregistraties. Deze wet is in 2001 vervangen door de Wet bescherming persoonsgegevens en ook andere wettelijke kaders zijn inmiddels gewijzigd. De praktijk van het cameratoezicht heeft zich eveneens ontwikkeld. Het CBP is daarom van mening dat er behoefte is aan een nieuwe studie waarin het normenkader opnieuw uitgewerkt wordt in duidelijke en hanteerbare vuistregels voor het toepassen van cameratoezicht in het publieke domein.

Als grondslag voor het cameratoezicht baseerde de overheid zich op het publieke belang en de handhaving van de openbare orde. Een expliciete wettelijke basis ontbrak echter. Eind 1997 verscheen een nota van het toenmalige kabinet waarin de ontwikkeling van cameratoezicht besproken werd en wetgeving werd aangekondigd. Uiteindelijk heeft in februari 2004 het tweede kabinet Balkenende een wetsvoorstel bij de Tweede Kamer ingediend om cameratoe-

zicht in het kader van de openbare orde te regelen. Dit wetsvoorstel, een aanvulling op de Gemeentewet, regelt het inzetten van het cameratoezicht als middel ter handhaving van de openbare orde. Gemeenten krijgen een wettelijke bevoegdheid cameratoezicht toe te passen. Rechten en plichten worden in zowel de Gemeentewet als de Wet politieregisters op hoofdlijnen vastgelegd. De beelden moeten worden opgeslagen in een politieregister, waardoor de Wet politieregisters (in de toekomst de Wet politiegegevens) van toepassing is. Aan de raad moet gerapporteerd worden over de doeltreffendheid en doelmatigheid van het toezicht. Tevens moet worden gerapporteerd of de waarborgen voldoende zijn en goed functioneren. Heimelijk cameratoezicht is sinds 1 januari 2004 strafbaar gesteld in artikel 441b Wetboek van strafrecht.

Deze publicatie van het CBP bespreekt vooral het cameratoezicht in het publieke domein en licht de toepasselijke regelgeving toe. Cameratoezicht is mogelijk op voorwaarde dat er maat wordt gehouden in de omvang en wijze van cameratoezicht. Ook moet in elementaire waarborgen voorzien zijn.

Juridische bronnen



- 2.1 Europese rechtsbronnen 19**
 - 2.1.1 Het Europees verdrag tot bescherming van de rechten van de mens 19
 - 2.1.2 Het Europees Databeschermingsverdrag 19
 - 2.1.3 De Europese Grondwet 20
 - 2.1.4 De Privacyrichtlijn van de Europese Unie 20
 - 2.1.5 Opinie 4/2004 van de Artikel 29-werkgroep 21

- 2.2 Nederlandse rechtsbronnen 22**
 - 2.2.1 De Grondwet 22
 - 2.2.2 De Wet bescherming persoonsgegevens 22
 - 2.2.3 De Gemeentewet 22
 - 2.2.4 Wetboek van Strafrecht 23
 - 2.2.5 Wetboek van Strafvordering 23
 - 2.2.6 Wet politieregisters 24

Dit hoofdstuk schetst de rechtsbronnen voor het normenkader waarbinnen cameratoezicht voor handhaving van de openbare orde georganiseerd dient te worden. Voor dit normenkader zijn zowel Europese regels als Nederlandse wetgeving van belang. Europa speelt immers in toenemende mate een rol op terreinen die de lidstaten voorheen zelfstandig regelden in nationale wetgeving. De regels raken ook steeds meer met elkaar verbonden. De Wet bescherming persoonsgegevens is een uitwerking van de Europese Richtlijn voor de bescherming van persoonsgegevens. Dit hoofdstuk bespreekt kort en in algemene zin de verschillende Europese rechtsbronnen en de Nederlandse regelgeving. In hoofdstuk drie wordt op basis van deze bronnen en jurisprudentie het normenkader verder uitgewerkt.

2.1 Europese rechtsbronnen

De Europese rechtsbronnen zijn het Europees Verdrag van de rechten van de mens¹ (EVRM), het Europees Databeschermingsverdrag van Straatsburg uit 1981² en de nieuwe Europese Grondwet³. Daarnaast zijn de Richtlijn 95/46/EG⁴ en de Opinie 4/2004 van de Working Party 29⁵ (WP 29, want ingesteld op grond van artikel 29, Richtlijn 95/46/EG) van belang voor de wijze waarop de lidstaten en verdragspartijen hun nationale wetgeving kunnen inrichten.

2.1.1 Het Europees Verdrag tot bescherming van de rechten van de mens

Het EVRM is van kort na de Tweede Wereldoorlog en is het eerste Europese verdrag waarin grondrechten vastgelegd werden die voor verdragspartijen gelden. In het eerste lid van artikel 8, is de bescherming van de persoonlijke levenssfeer vastgelegd. In het tweede lid staan de criteria waaraan een inbreuk op het recht op bescherming van de persoonlijke levenssfeer moet voldoen. Als er sprake is van zo'n inbreuk door cameratoezicht in het kader van de handhaving van de openbare orde dan zijn deze criteria van toepassing.

Artikel 8, tweede lid vereist dat de inbreuk bij wet is voorzien en dat deze inbreuk noodzakelijk is in een democratische samenleving. Voor cameratoezicht door de overheid betekent dit dat de inbreuk noodzakelijk moet zijn voor het beschermen van de openbare orde en het voorkomen van wanordelijkheden en strafbare feiten. Jurisprudentie betreffende de reikwijdte van artikel 8 EVRM en de normen van de bescherming van de persoonlijke levenssfeer komt in paragraaf 3.2. aan de orde.

Van belang is tevens artikel 2 van het vierde protocol bij het EVRM⁶. Dit artikel behandelt de verplaatsingsvrijheid van personen in het publieke domein. Het handhaven van gebiedsverboden met cameratoezicht kan een inbreuk vormen op de verplaatsingsvrijheid. Een zogenaamd gebiedsverbod vormt niet in alle gevallen een inbreuk op dit recht. Het is echter wel vereist dat voldaan wordt aan de criteria van het EVRM: gebiedsverboden moeten bij wet zijn voorzien en gerechtvaardigd worden door het algemeen belang in een democratische samenleving⁷.

¹ Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, Rome, 4 november 1950, Trb. 1951, 154; laatste wijziging: Trb. 1988, 95.

² Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, Straatsburg, 28 januari, Trb. 1988.7; laatste wijziging: Trb.2000, 69.

³ Ontwerp Verdrag tot vaststelling van een Grondwet voor Europa, Publicatieblad NR. C 169 van 18 juli 2003. Vindplaats: <http://europa.eu.int/eur-lex/nl/> en www.europesegrondwet.nl.

⁴ Richtlijn 95.46/EG van het Europese Parlement en de Raad van 24 oktober 1995, Publicatieblad van de Europese Gemeenschappen nr.1. 281/40, 23 november 1995.

⁵ Opinie 4/2004 on the Processing of Personal Data by means of Video-surveillance (WP 89), www.europa.eu.int/internal_market/privacy/workinggroup/wp2004.

⁶ Vierde Protocol bij het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, 11 mei 1994, Trb. 1994/165, in werking getreden op 1 november 1998.

⁷ Uitspraak EHRM van 4 juni 2002, NJ 2002, nr. 33 en uitspraak EHRM van 4 juni 2002, NJCM-bulletin jrg.28 (2003) nr. 2.

2.1.2 Het Europees Databeschermingsverdrag

Het Europees Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (het zogenaamde Databeschermingsverdrag) speelt een belangrijke rol in het juridisch kader, omdat hier voor het eerst specifiek aandacht is besteed aan één aspect van de bescherming van de persoonlijke levensfeer namelijk de bescherming van persoonsgegevens.

Artikel 2 van dit verdrag definieert persoonsgegevens als "alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon". Met behulp van camerabeelden kunnen personen zowel direct herkend als geïdentificeerd worden. Deze beelden kunnen daarom een belangrijke bijdrage leveren aan het identificeren van een persoon. Als aan de voorwaarde van identificeerbaarheid is voldaan, dan dienen camerabeelden als persoonsgegevens gezien te worden.

De Raad van Europa bereidt overigens momenteel een aantal richtlijnen voor over de bescherming van individuen bij het verwerken van persoonsgegevens verkregen door middel van video-opnamen.⁸ De inhoud zal vermoedelijk in grote lijnen overeenkomen met de Opinie 4/2004 van de WP 29 (zie ook paragraaf 2.1.5).

2.1.3 De Europese Grondwet

In het ontwerp van de Europese Grondwet⁹ is opnieuw vormgegeven aan de bescherming van de persoonlijke levenssfeer in titel II, de artikelen 7 en 8.

Artikel II.7 stelt dat eenieder recht heeft op de eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie. In de toelichting wordt expliciet vermeld dat voor het begrip communicatie is gekozen in plaats van correspondentie, vanwege de technische ontwikkelingen. Het artikel moet hetzelfde bereik worden toegekend als artikel 8 EVRM.

Artikel II.8 van de Europese Grondwet stelt in het eerste lid dat eenieder recht heeft op bescherming van zijn persoonsgegevens. Het tweede lid van artikel II.8 schrijft voor dat de gegevens op eerlijke wijze moeten worden verwerkt en dat er sprake moet zijn van vastgestelde doeleinden. De grondslag voor verwerking kan worden gebaseerd op de toestemming van degene over wie gegevens worden verwerkt of op een gerechtvaardigde grondslag die in een wet moet zijn voorzien. Verder kent het tweede lid aan eenieder het recht op inzage in de over hem verwerkte gegevens toe evenals het recht om te verzoeken om rectificatie. Het derde lid geeft aan dat een onafhankelijke autoriteit moet toezien op de naleving van deze regels.

In de toelichting wordt het verband gelegd met andere Europese regels. Dit zijn achtereenvolgens artikel 286 van het Verdrag tot oprichting van de Europese Gemeenschap (dit artikel is inmiddels vervangen door artikel 50 van de Grondwet), Richtlijn 95/46/EG (de algemene privacyrichtlijn), artikel 8 EVRM en het Europees Databeschermingsverdrag.

2.1.4 De Privacyrichtlijn van de Europese Unie

De Europese Unie (EU) geeft in richtlijnen bindende aanwijzingen aan de lidstaten welke onderwerpen nadere regelgeving behoeven. Harmonisatie van de regelgeving, in het kader van de bevordering van de interne markt, is daarbij een belangrijk doel. Harmonisatie van regelgeving wil zeggen dat de Europese Unie streeft naar zo gelijk mogelijke regels in de lidstaten. Een van die richtlijnen is de Europese Richtlijn 95/46/EG waarin aan de lidstaten de opdracht is gegeven wettelijke maatregelen te treffen ter bescherming van de persoonsgegevens. Dit heeft in Nederland geleid tot de Wet bescherming persoonsgegevens (WBP).

De Richtlijn definieert in artikel 2 het begrip persoonsgegevens als "iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon", hierna "betrokkene" te

⁸ Opinie 4/2004, pagina 5.

⁹ www.europesegrondwet.nl.

noemen; als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of via een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit”.

Overweging 14 van de Richtlijn stelt dat “gezien het belang van de in het kader van de informatiemaatschappij aan de gang zijnde ontwikkelingen inzake de technieken voor het opvangen, doorsturen, manipuleren, registreren bewaren of mededelen van geluid- en beeldgegevens betreffende natuurlijke personen, deze Richtlijn ook van toepassing zal moeten zijn op verwerkingen die op deze gegevens betrekking hebben”. Daarmee is de Richtlijn (en dus ook de WBP) van toepassing op het verwerken van camerabeelden.

De Richtlijn 95/46/EG is niet van toepassing op cameratoezicht door de politie in het kader van opsporingsonderzoek. Overweging 16 van de Richtlijn zegt immers “dat verwerkingen van geluid- en beeldgegevens, zoals gegevens van videobewaking, niet binnen de werksfeer plaatsvinden met het oog op de veiligheid van de Staat en de activiteiten van de Staat op strafrechtelijk gebied of met het oog op de uitoefening van andere activiteiten die niet onder het Gemeenschapsrecht vallen”. Bij de werkzaamheden van de politie gaat het om observatie door de politie met behulp van al dan niet verborgen camera's. In Nederland voorziet het Wetboek van Strafvordering in artikel 126g en artikel 126o in bevoegdheden voor de politie om stelselmatige observatie te verrichten ten behoeve van de opsporing van strafbare feiten.

2.1.5 **Opinie 4/2004 van de Artikel 29-werkgroep**

Op grond van artikel 29 van de Europese Privacyrichtlijn 95/46/EG is een permanente werkgroep van Europese toezichthouders ingesteld voor de bescherming van persoonsgegevens. De werkgroep wordt de Working Party 29 (WP 29) genoemd. De WP 29 heeft een onafhankelijk en raadgevend karakter. De werkzaamheden van de werkgroep leveren een bijdrage aan de ontwikkeling van Europese normen en gemeenschappelijke interpretaties en in een aantal gevallen ook aan de bewustwording op internationaal niveau.

De belangrijkste taak van de werkgroep is het bevorderen van uniforme toepassing van de privacyrichtlijn in alle lidstaten door middel van samenwerking tussen de Europese toezichthouders. De werkgroep stelt ten behoeve van de uitvoering van de taken opinies op waarin actuele onderwerpen worden besproken in het licht van de Richtlijn 95/46/EG. Deze opinies hebben ook tot doel uitleg te geven op welke wijze de Richtlijn in bepaalde gevallen, zoals cameratoezicht in het kader van de openbare orde, moet worden geïnterpreteerd.

Opinie 4/2004 behandelt daartoe cameratoezicht in de Europese Unie en geeft aan op welke wijze cameratoezicht kan voldoen aan de vereisten van de Richtlijn. Deze Opinie is in februari 2004 vastgesteld en is een nadere uitwerking van de regels voor de verwerking van persoonsgegevens toegepast op cameratoezicht. Hiertoe is geïnventariseerd op welke wijze cameratoezicht in de diverse lidstaten is geregeld. Aan de hand van diverse voorbeelden wordt verduidelijkt in welke situaties cameratoezicht wel of niet kan worden toegepast en op welke wijze opgeslagen beelden verder mogen worden verwerkt.

De Opinie stelt dat artikel 8 EVRM van toepassing is op verwerkingen door politie en justitie. Cameratoezicht is volgens zowel de Richtlijn als de Opinie mogelijk in het kader van de handhaving van de openbare orde als daar in concrete situaties aanleiding toe is. Met andere woorden er moet een concrete noodzaak zijn om cameratoezicht in te zetten. De Opinie stelt eveneens dat “de bevoegde instellingen in de lidstaten moeten videobewaking vanuit een algemeen gezichtspunt beoordelen, met het oog op de bevordering van een algemeen selectieve en systematische benadering van dit vraagstuk. De sterke verspreiding van beeldopnamesystemen op openbare en particuliere plaatsen mag niet leiden tot onverantwoorde beperkingen van de rechten van burgers en de fundamentele vrijheden; burgers zouden anders het slachtoffer kunnen worden van buitensporige gegevensverzamelingsprocedures die hen op een aantal openbare of particuliere plaatsen identificeerbaar kunnen maken.”¹⁰ Voor de overheid zijn

¹⁰ Opinie 4/2004, pagina 4.

buiten het strafrecht gelegen gerechtvaardigde doelen de openbare orde in het publieke domein en de bescherming van personen en eigendommen.

De Richtlijn ziet niet op het gebruik van camera's en beelden door een "natuurlijk persoon"¹¹ voor strikt persoonlijk of huishoudelijk gebruik¹². Dit gebruik dient overigens wel te passen binnen de rechten en vrijheden van anderen. Burgers die menen dat het persoonlijk gebruik van bijvoorbeeld beelden van hen door anderen een inbreuk op hun privacy tot gevolg heeft, staat de weg naar de civiele rechter open. Het gaat hierbij bijvoorbeeld om het gebruik van beelden van webcams. Dit gebruik kan door de rechter worden getoetst aan normen van met name de maatschappelijke zorgvuldigheid.

De Richtlijn ziet volgens overweging 17 en artikel 9 eveneens op het maken van beelden en geluidsopnamen die exclusief voor journalistieke doeleinden, literaire werken of artistieke uitingen zijn bedoeld. Hier gelden wel beperkingen voor de toepasselijkheid van de Richtlijn. Deze beperkingen dienen uitzonderingen en afwijkingen van de bepalingen van de Richtlijn te bevatten die het recht op vrijheid van meningsuiting en het recht op bescherming van de persoonlijke levenssfeer verzoenen¹³.

2.2 Nederlandse rechtsbronnen

Deze paragraaf geeft een korte beschrijving van de Nederlandse rechtsbronnen. Dit zijn de Grondwet, de Wet bescherming persoonsgegevens, de Gemeentewet, het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Wet politieregisters.

2.2.1 De Grondwet

In artikel 10 van de Grondwet is het recht op bescherming van de persoonlijke levenssfeer vastgelegd. De reikwijdte van dit artikel is vergelijkbaar met die van artikel 8 EVRM (zie voor de reikwijdte hoofdstuk 3.2). Het tweede lid van artikel 10 Grondwet geeft de opdracht aan de wetgever nadere regels te stellen ten aanzien van de bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Het derde lid geeft de wetgever de opdracht het inzage en correctierecht ten aanzien van de verwerking van persoonsgegevens te regelen in de vorm van een wet. De Wet bescherming persoonsgegevens (WBP) vloeit zowel voort uit de Nederlandse Grondwet als uit de opdracht van de Europese Richtlijn 95/46/EG aan de lidstaten.

2.2.2 De Wet bescherming persoonsgegevens

Deze wet vloeit, zoals hiervoor al is opgemerkt, voort uit het tweede lid van artikel 10 Grondwet. Daarin staat immers dat bij wet regels gesteld worden met betrekking tot de bescherming van persoonsgegevens.

Ook de Richtlijn 95/46/EG geeft aan de lidstaten de opdracht een wettelijke regeling te maken die voorziet in regels die tot doel hebben de persoonsgegevens te beschermen. De WBP is sinds 1 september 2001 in werking getreden. De voorloper van de WBP, de Wet persoonsregistraties moest naar aanleiding van de Richtlijn aangepast worden. De WBP geeft definities en het algemene normatieve kader ten aanzien van de grondslagen voor verwerking, doelen, toegestaan gebruik van verzamelde persoonsgegevens, verstrekking aan derden en bewaartermijnen. Dit kader wordt verder toegelicht in hoofdstuk drie.

2.2.3 De Gemeentewet

De Gemeentewet kent tot noch toe geen specifieke regels voor het cameratoezicht door gemeenten. Het gebruik van cameratoezicht wordt voor de handhaving van de openbare orde in het publieke domein gebaseerd op artikel 172 Gemeentewet.

¹¹ Richtlijn 95/46/EG, artikel 3, tweede lid en overweging 12.

¹² Opinie 4/2004, pagina 15.

¹³ Aanbeveling 1/97 Working group article 29, pagina 1.

Dit artikel zegt in het eerste lid "De burgemeester is belast met de handhaving van de openbare orde". Het tweede lid geeft de burgemeester de bevoegdheid om "overtreding van wettelijke voorschriften die betrekking hebben op de openbare orde, te beletten of te beëindigen. Hij bedient zich daarbij van de onder zijn gezag staande politie". Het derde lid geeft aan de burgemeester de bevoegdheid om "bij verstoring van de openbare orde of bij ernstige vrees voor het ontstaan daarvan, bevelen te geven die noodzakelijk te achten zijn voor de handhaving van de openbare orde".

Juist omdat deze algemene handhavingsbevoegdheid niet speciaal ziet op cameratoezicht, heeft de regering op 23 februari 2004 een wetsvoorstel¹⁴ tot aanvulling op de Gemeentewet ingediend bij de Tweede Kamer. In het wetsvoorstel wordt het cameratoezicht door gemeenten met als doel de handhaving van de openbare orde, in artikel 151c geregeld. Daarmee worden wettelijke regels voor cameratoezicht in het publieke domein gegeven. Ook wordt de regie ten aanzien van het publieke domein expliciet toegekend aan de overheid.

2.2.4 Wetboek van Strafrecht

Van belang voor wat moet worden verstaan onder de begrippen publieke plaats, een besloten plaats en de informatieplicht zijn de strafbaarstellingen van heimelijk cameratoezicht in de artikelen 139f en 441b van het Wetboek van Strafrecht (zie verder hoofdstuk 3.1 voor een bespreking van deze artikelen).

2.2.5 Wetboek van Strafvordering

Het Wetboek van Strafvordering regelt in artikel 126g (en het overeenkomstige artikel 126o) de stelselmatige observatie met behulp van technische middelen. Dit artikel geeft de politie de bevoegdheid, na een bevel van de Officier van Justitie, verdachten stelselmatig te observeren. Het moet dan wel gaan om een verdenking van een misdrijf.

Met stelselmatige observatie wordt volgens de aanwijzing opsporingsbevoegdheden van het Openbaar Ministerie¹⁵ bedoeld "het al dan niet heimelijk, systematisch en gericht waarnemen en/of volgen van een persoon met als te verwachten resultaat dat daardoor een min of meer volledig beeld kan worden verkregen van bepaalde aspecten van zijn/haar leven".

Stelselmatigheid hangt samen met de "duur van de observatie, de plaats, de intensiteit, de frequentie of het toepassen van een technisch hulpmiddel dat meer biedt dan alleen de versterking van de zintuigen. Elk voor zich, maar met name in combinatie, zijn deze elementen bepalend voor beantwoording van de vraag of een min of meer volledig beeld van bepaalde aspecten van iemands leven wordt verkregen"¹⁶.

Stelselmatige observatie wijkt af van cameratoezicht ten behoeve van de handhaving van de openbare orde in het publieke domein. Immers het gaat hierbij niet om opsporing van verdachten. Ook is er geen sprake van het gericht in beeld brengen van een persoon gedurende langere tijd en het min of meer vormen van een volledig beeld van bepaalde aspecten van het leven van een of meer personen. Daarnaast is onderscheidend dat het bij cameratoezicht in het publieke domein in het algemeen gaat om plaatsen waarbij een persoon minder verwachtingen heeft over de bescherming van zijn persoonlijke levenssfeer. Bij stelselmatige observatie kan het ook gaan om het observeren van personen op plaatsen waarvan personen wel, en op goede gronden, zo'n verwachting ten aanzien van de bescherming van de persoonlijke levenssfeer kunnen hebben.

Overigens is het niet zo dat camera's ten behoeve van de openbare orde uitsluitend voor dat doel gebruikt mogen worden.

¹⁴ Wijziging van de Gemeentewet en de Wet politieregisters in verband met de invoering van regels omtrent het gebruik van camera's ten behoeve van toezicht op openbare plaatsen (cameratoezicht op openbare plaatsen), Kamerstukken II, 2003-2004, 29 440.

¹⁵ <http://www.openbaarministerie.nl/bob/docs/22.htm>, pagina 2.

¹⁶ <http://www.openbaarministerie.nl/bob/docs/22/htm>, pagina 3.

Beelden opgenomen met camera's bedoeld voor de handhaving van de openbare orde mogen ten eerste ook gebruikt worden voor identificatie en opsporing en vervolging van verdachten van strafbare feiten. Dit wordt ook wel de bijvangst genoemd.

Ten tweede kunnen camera's in het publieke domein gebruikt worden ter ondersteuning van de inzet van de politie en hulpdiensten als ambulances en brandweer. Dit gebruik van de camera's kan de inzet van deze diensten efficiënter en effectiever maken en kan bijdragen aan de verkleining van de risico's van de inzet van politie en hulpdiensten.

Ten derde kunnen camera's in het publieke domein ook benut worden voor stelselmatige observatie door observatieteams als er daartoe een bevel tot observatie door het Openbaar Ministerie¹⁷ is afgegeven. Dit gebruik kan als medegebruik gekwalificeerd worden.

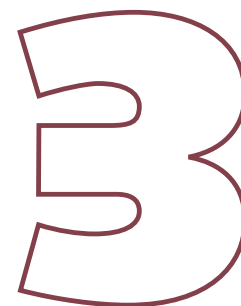
2.2.6 Wet politieregisters

De Wet politieregisters (WPOLR) is op dit moment en in de toekomst relevant. Nu al kan de registratie van beelden als behorend tot de uitvoering van de politietaak, in een politieregister plaatsvinden. Straks zal deze wet bij het inwerkingtreden van het wetsvoorstel cameratoezicht op openbare plaatsen (artikel 151c) het regime voor de opgeslagen camerabeelden bepalen.

De WPOLR geeft de mogelijkheden en de grenzen aan voor het verwerken van persoonsgegevens in politieregisters. Deze wet geeft regels over de noodzakelijkheid van het verzamelen van beelden, de bewaartermijn en op welke wijze met de rechten van betrokkenen omgegaan dient te worden. Die rechten zijn het inzien van de beelden en het eventueel corrigeren laten van beelden en/of bijbehorende gegevens, het afschermen van verder gebruik en het verwijderen van beelden uit bestanden (zie verder paragraaf 3.13 en paragraaf 4.13). Overigens moet vermeld worden dat er eveneens een wetsvoorstel Wet politiegegevens (WPOLG) bij de Tweede Kamer is ingediend. Deze wet is bedoeld als opvolger van de huidige WPOLR.

¹⁷ Artikel 126g WvSv schrijft in het vijfde lid voor dat het bevel tot observatie schriftelijk moet worden gegeven. Artikel 126o WvSv doet hetzelfde in het vierde lid.

Juridisch kader



- 3.1 Openbare plaats in het publieke domein 27
- 3.2 Redelijke verwachting van respect voor de persoonlijke levenssfeer 30
- 3.3 Het verwerken van persoonsgegevens 33
- 3.4 Grondslag voor de verwerking 35
- 3.5 Doel van de verwerking 35
- 3.6 Noodzakelijkheid en selectiviteit 37
- 3.7 Verantwoordelijke en regie 38
- 3.8 Verder gebruik 40
- 3.9 Kwaliteit van gegevens 40
- 3.10 Beveiliging 41
- 3.11 Kenbaarheid 41
- 3.12 Bewaartermijn 42
- 3.13 Rechten van betrokkenen 42
- 3.14 Melding, reglementsplicht, verordening 44

In dit hoofdstuk wordt het juridisch kader uitgewerkt aan de hand van een aantal sleutelbegrippen in de in hoofdstuk 2 genoemde rechtsbronnen. Ook wordt uit jurisprudentie van het Europese Hof voor de rechten van de mens en de Hoge Raad der Nederlanden geput.

Als eerste wordt het begrip openbare plaats in het publieke domein behandeld, omdat met name dit begrip kan leiden tot onduidelijkheid (3.1) en vervolgens de verwachting ten aanzien van het recht op bescherming van de persoonlijke levenssfeer (3.2). Daarna volgen:

- persoonsgegevens en de verwerking van persoonsgegevens (3.3)
- de grondslagen voor de verwerking (3.4)
- de doelen van de verwerking (3.5)
- de noodzakelijkheid en de selectiviteit (3.6)
- de verantwoordelijke voor de verwerking en de regiefunctie (3.7)
- de verdere verwerking (3.8)
- de kwaliteit van persoonsgegevens (3.9)
- de beveiliging (3.10)
- de kenbaarheid (3.11)
- de bewaartermijn (3.12)
- de rechten van betrokkenen (3.13).

De slotparagraaf 3.14 bespreekt de Wet bescherming persoonsgegevens (WBP) en de Wet politieregisters (WPOLR) voor wat betreft de meldingsplicht en de reglementsplicht. Immers, voor cameratoezicht in het kader van de openbare orde is het mogelijk voor de gegevensverwerking te kiezen tussen het regime van WBP of van WPOLR. Deze keuzemogelijkheid zal bestaan tot het in werking treden van het voorgestelde artikel 151c Gemeentewet.

3.1 Openbare plaats in het publieke domein

Het begrip openbare plaats is belangrijk, omdat het voor overheid en publiek helder moet zijn over welke plaatsen het gaat bij cameratoezicht. Wie is bevoegd op welke plaats de openbare orde te handhaven. Het is niet altijd direct duidelijk of een plaats een openbare plaats of een niet-openbare plaats is. Een ander onderscheid is dat tussen een besloten plaats die geen woning is en een besloten plaats die wel een woning is. Van een inbreuk op de bescherming van de persoonlijke levenssfeer door middel van cameratoezicht is op de openbare weg nu eenmaal minder snel sprake dan in een besloten plaats of een woning.

Richtinggevend is het wetsvoorstel tot wijziging van de Gemeentewet en de Wet politieregisters in verband met de invoering van regels omtrent het gebruik van camera's ten behoeve van toezicht op openbare plaatsen (cameratoezicht op openbare plaatsen). Voor wat betreft de WPOLR geldt dat in de Tweede Kamer een wetsvoorstel aanhangig is gemaakt (WPOLG) ter vervanging van de WPOLR.

Openbare plaatsen

Het wetsvoorstel cameratoezicht op openbare plaatsen geeft het meest actuele inzicht voor wat betreft openbare plaatsen in samenhang met de toepassing van cameratoezicht en de handhaving van de openbare orde. Het wetsvoorstel definieert het begrip openbare plaats als een plaats "waar men komt en gaat"¹. Er mag geen sprake zijn van beletselen voor dit vrije komen en gaan zoals een meldingsplicht, eisen van voorafgaand verlof of entreegelden. Onder het begrip openbare plaats vallen de wegen en straten die voor iedereen toegankelijk zijn. In het verlengde hiervan vallen ook openbare plantsoenen, speelweiden en parken en voor ieder vrij toegankelijke gedeelten van overdekte passages en winkelgalerijen binnen de definitie van openbare plaats.

Niet-openbare plaatsen

Voorbeelden van niet-openbare plaatsen zijn stadions, postkantoren, warenhuizen, restaurants en ziekenhuizen.² Ook gemeentehuizen, discotheken en parkeergarages vallen buiten de

¹ Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 8.

² Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 8.

definitie van openbare plaats. Hier kan wel cameratoezicht plaatsvinden in het kader van beveiligingsdoelen, als dat kenbaar is voor aanwezige personen en aan de eerder genoemde voorwaarden is voldaan.

Besloten plaatsen (geen woning)

Besloten plaatsen die geen woning zijn, zijn bijvoorbeeld die gedeelten van bedrijven en overheidsgebouwen die niet toegankelijk zijn voor het publiek.

Woningen

Woningen zijn bij uitstek besloten plaatsen waarbij in het geval van cameratoezicht door anderen dan de bewoners al heel snel sprake zal zijn van een inbreuk op de persoonlijke levenssfeer. Bovendien is in een woning geen sprake van handhaving van de openbare orde.

Het wetsvoorstel cameratoezicht op openbare plaatsen steunt voor de definitie van het begrip openbare plaats op artikel 1, Wet openbare manifestaties: "een plaats die krachtens bestemming of vast gebruik openstaat voor het publiek". Deze definitie is ruimer dan die in het wetsvoorstel cameratoezicht op openbare plaatsen staat. Onder de Wet openbare manifestaties zouden ook de vrij toegankelijke delen van bijvoorbeeld gebouwen, zoals dat in de uitspraak van het Europese Hof voor de rechten van de mens in de zaak Perry tegen het Verenigd Koninkrijk³ is gebeurd, kunnen worden verstaan. Het tweede lid van deze wet sluit de in artikel 6, tweede lid van de Grondwet genoemde openbare plaatsen uit. Het gaat hierbij om openbare plaatsen waar de vrijheid van godsdienst en levensovertuiging beleden wordt, buiten de daarvoor bestemde gebouwen en besloten plaatsen. Met andere woorden, kerken en andere gebouwen bestemd voor het belijden van godsdienst en levensovertuiging zijn wellicht naar hun aard aan te merken als openbare plaatsen, maar zijn om redenen van bescherming van de uitoefening van godsdienst of levensovertuiging uitgesloten.

Kerken

De memorie van toelichting van het wetsvoorstel cameratoezicht op openbare plaatsen zegt hierover: "Dit betekent dat het ook krachtens het voorliggende wetsvoorstel niet toegestaan zal zijn toezichtcamera's in kerken, moskeeën en dergelijke te plaatsen. Indien echter beelden worden gemaakt van een openbare plaats (een straat of plein) waaraan bijvoorbeeld een kerk is gelegen, dan is wel toegestaan dat daarbij het exterieur van de kerk in beeld komt."⁴

De Opinie 4/2004 stelt dat "videobewaking uitsluitend gebaseerd op raciale of etnische afkomst van de opgenomen personen, hun politieke of godsdienstige opvattingen, hun lidmaatschap van een vakvereniging of hun seksuele gedrag moet verboden worden"⁵ op grond van artikel 8 van Richtlijn 95/46/EG. Dat betekent dat het niet is toegestaan de camera's in straten en pleinen te gebruiken uitsluitend met het doel vast te leggen welke personen bepaalde kerken of vergaderingen bezoeken.

Europese interpretatie

In het arrest Perry geeft het Europese Hof voor de rechten van de mens een Europese interpretatie van het begrip openbare plaats. De plaats waar gefilmd was (het gemeenschappelijke administratiegedeelte van het politiebureau) werd beschouwd als een openbare plaats, omdat hier zowel personeel als verdachten door heen gaan. Omdat er sprake was van ander gebruik van de camera's dan voor het vooraf bepaalde doel en omdat er sprake was van systematische vergaring van beelden, meende het hof in overweging 43 dat er sprake was van een inbreuk op de bescherming van de persoonlijke levenssfeer. Zie hiervoor ook paragraaf 3.2.

Hoewel er dus een wettelijke basis kan zijn voor cameratoezicht in openbare en niet-openbare plaatsen, toont deze uitspraak van het Europese Hof voor de rechten van de mens aan dat wat een voor publiek toegankelijke plaats is, niet te eng moet worden uitgelegd. Daarnaast blijkt dat een ander gebruik dan waarvoor de camera's zijn geïnstalleerd, niet zonder meer is

³ <http://hudoc.echr.coe.int>, Straatsburg, 17 oktober 2003.

⁴ Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 8.

⁵ Opinie 4/2004, pagina 26.

toegestaan. Zeker niet als vervolgens aan de gefilmde persoon ook het recht op informatie en de mogelijkheid om commentaar op de beelden te geven wordt onthouden.

Strafrechtelijke criteria

Het Wetboek van Strafvordering spreekt in de artikelen 126g en 126o⁶ over besloten en niet-besloten plaatsen. Onder besloten plaatsen vallen de woning, erf, loods-, fabrieks- en bedrijfsruimten. Niet-besloten plaatsen zijn voor ieder toegankelijke plaatsen en gebouwen (stations, winkels, de hal van openbare instellingen).

In het Wetboek van Strafrecht is de strafbaarstelling van heimelijk cameratoezicht sinds 1 januari 2004 geregeld zowel voor plaatsen die toegankelijk zijn voor het publiek als voor besloten plaatsen. Vóór 1 januari 2004 bestond het verbod op heimelijk cameratoezicht in artikel 441b WvSr alleen uit: “..in een voor het publiek toegankelijke besloten ruimte, waarin spijzen, dranken of andere waren aan particulieren worden geleverd, van een daarin aanwezige persoon een afbeelding vervaardigt.”. In de praktijk gold dit verbod voor publiek toegankelijke plaatsen als winkels of horecagelegenheden. Vanaf 1 januari 2004 is de reikwijdte uitgebreid tot “alle voor het publiek toegankelijke plaatsen”⁷.

Artikel 441b WvSr verbiedt expliciet het heimelijk maken van afbeeldingen op voor publiek toegankelijke plaatsen. De letterlijke tekst luidt: “van een persoon, aanwezig op een voor het publiek toegankelijke plaats, wederrechtelijk een afbeelding vervaardigt”. Dit betekent een uitbreiding van het bereik en volgens de memorie van toelichting valt ook de openbare weg onder de reikwijdte van dit verbod⁸.

Artikel 139f WvSr verbiedt het heimelijk maken van opnamen van personen die in een woning of in een niet voor het publiek vrij toegankelijke plaats verblijven. Artikel 8 EVRM geeft immers aan eenieder het recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Dit betekent dat cameratoezicht in het kader van de handhaving van de openbare orde niet zover mag gaan dat in genoemde plaatsen, beelden van personen worden opgenomen. Dit artikel dwingt de overheid om beelden gedeeltelijk te blokkeren of camera-instellingen aan te passen als bij het in beeld brengen van het publieke domein ook ramen en deuren (geheel of gedeeltelijk) van huizen en bedrijven opgenomen worden.

Wijziging Gemeentewet

Het wetsvoorstel cameratoezicht op openbare plaatsen voorziet in een exclusieve regeling van cameratoezicht in het kader van de openbare orde. De beveiliging van particuliere of publieke eigendommen valt buiten de regeling. Dat betekent dat bijvoorbeeld de bewaking van het gemeentehuis met camera's niet onder de regeling valt, omdat het doel van het cameratoezicht dan niet de handhaving van de openbare orde is, maar de beveiliging van personen en/of eigendom.

Sommige openbare plaatsen zijn in particulier eigendom maar wel geheel of gedeeltelijk vrij voor het publiek toegankelijk. Beslissend voor de vraag welke regels van toepassing zijn, is of de plaats geheel of gedeeltelijk openbaar is. Voorbeelden van plaatsen waar dit speelt, zijn delen van stationsterreinen, stationshallen en sommige winkelpassages. Als de lokale overheid op deze plaatsen cameratoezicht wil hanteren in het belang van de handhaving van de openbare orde, dan is de regeling in het wetsvoorstel cameratoezicht op openbare plaatsen van toepassing.

⁶ Tekst en commentaar Wetboek van strafvordering, Cleiren C.P.M., Nijboer J.F., Kluwer, Deventer, derde druk 1999.

⁷ Wetsvoorstel 27 732, wijziging van de artikelen 139f en 441b van het wetboek van Strafvordering (uitbreiding strafbaarstelling heimelijk cameratoezicht), Kamerstukken II, 2000-2001, 27 732, nr.3, pagina 1.

⁸ Kamerstukken II, 2000-2001, 27 732, nr.3, pagina 1.

De Nederlandse Spoorwegen (NS) hebben volgens het wetsvoorstel cameratoezicht op openbare plaatsen een eigen publiekrechtelijke verantwoordelijkheid voor de veiligheid en orde op grond van de Spoorwegwet en het daaruit voortvloeiende Algemeen Reglement Vervoer (ARV)⁹. Dat betekent concreet dat het gemeentebestuur in situaties waarbij door de NS camera's in stationshallen zijn geplaatst, niet in overleg hoeft te treden met de NS. De wetgever is van mening dat "in dit licht zal in de praktijk uitsluitend in uitzonderlijke gevallen en in overleg met de NS aanleiding bestaan om in het kader van dit wetsvoorstel tot plaatsing van camera's in stationshallen over te gaan"¹⁰.

3.2 Redelijke verwachting van respect voor de persoonlijke levenssfeer

Niet alleen de aard van de plaats is van belang, maar ook de redelijke verwachting van respect voor de persoonlijke levenssfeer bepaalt of "zonder meer" toezicht mag worden uitgeoefend.

Artikel 8 van het EVRM kent eenieder het recht op respect voor de persoonlijke levenssfeer toe. Het gaat om het recht op een privé-leven, familie- en gezinsleven, de bescherming van de woning en de correspondentie. Hoever de bescherming van de persoonlijke levenssfeer reikt, wordt uitgekristalliseerd in jurisprudentie. De interpretatie van wat de persoonlijke levenssfeer is, is in de loop der tijd ook veranderd. Niet alleen in de woning en in de privé-sfeer geldt de bescherming van de persoonlijke levenssfeer, ook op de werkplek en in het publieke domein heeft de burger het recht om onbespied zijns wegs te gaan. Het strafrecht voorziet door middel van artikel 139f in de strafbaarstelling van heimelijk cameratoezicht in woningen of andere niet voor publiek toegankelijke plaatsen.

Het recht op bescherming van de persoonlijke levenssfeer is echter niet absoluut. Dit wil zeggen dat niet onder alle omstandigheden dit recht op bescherming van de persoonlijke levenssfeer voor gaat. Er kan sprake zijn van situaties waarin de burger een inbreuk op zijn persoonlijke levenssfeer moet dulden.

Criteria voor een inbreuk op de persoonlijke levenssfeer

Uit artikel 8 EVRM eerste lid vloeit voort dat er een drietal vragen gesteld moet worden om te kunnen bepalen of er sprake is van een inbreuk. De eerste kwestie is of de bescherming van de persoonlijke levenssfeer in het geding is. Zo ja, dan is de vraag of er in die bepaalde situatie een inbreuk op die persoonlijke levenssfeer is gepleegd. Indien dat het geval is, moet de vraag beantwoord worden of die inbreuk gerechtvaardigd is. In het tweede lid van artikel 8 EVRM worden de gronden opgesomd die ertoe kunnen noodzaken dit recht te beperken. Dit zijn de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Uit artikel 8 EVRM blijkt dat de beperking van het recht op bescherming van de persoonlijke levenssfeer ook noodzakelijk moet zijn in een democratische samenleving. In zijn *Opinie 4/2004* haalt de WP 29 artikel 2 van het vierde protocol bij het EVRM aan. De beperkingen moeten proportioneel zijn, dit wil zeggen in verhouding staan tot de doelen van het cameratoezicht. En ook moeten de maatregelen noodzakelijk zijn in een democratische samenleving.¹¹

Burgers hebben dus het recht zich in beginsel onbespied te kunnen bewegen in zowel het private als het publieke domein. Een inperking van dit recht moet een wettelijke basis hebben. De inperking moet ook noodzakelijk zijn in een democratische samenleving. Het doel van de beperking moet gebaseerd zijn op één van de gronden die limitatief zijn opgesomd in het tweede lid van artikel 8 EVRM.

⁹ Kamerstukken II, 2003-2004, 29 440, nr. 3, pagina 9.

¹⁰ Kamerstukken II, 2003-2003, 29 440, nr. 3, pagina 9.

¹¹ *Opinie 4/2004*, pagina 6.

Reasonable expectation in Europese jurisprudentie

In de rechtspraak in Europa en Nederland wordt, in navolging van de rechtspraak in de Verenigde Staten, de leer van de “reasonable expectation” gehanteerd. Het begrip ziet op wat een burger wel of niet, onder de gegeven omstandigheden redelijkerwijs mag verwachten als het gaat om inbreuken op de persoonlijke levenssfeer.

Dat betekent dat een persoon geen volledige privacy kan verwachten, indien hij zich begeeft in het publieke domein of in voor het publiek toegankelijke plaatsen¹². Maar van een volledig ontbreken van rechten en vrijheden, zoals die veel sterker in de privé-sfeer bestaan, mag ook in het publieke domein geen sprake zijn. Dit hangt samen met het recht om zich in beginsel vrij en onbespied te bewegen, indien men rechtmatig binnen een land verblijft. In elk geval wordt uitgegaan van bescherming van de persoonlijke levenssfeer zodra iemand zich in zijn of haar huis bevindt. Het gaat onder normale omstandigheden niet aan iemand met behulp van een camera te bespieden, terwijl hij of zij in de eigen of een andere woning vertoeft. Ook de rechter heeft zich daar in nationaal en internationaal verband over uitgesproken.

Het Europese Hof vereist dat beperkingen van het recht op bescherming van de persoonlijke levenssfeer door de overheid bij “wet” worden voorzien. Er dient dus een wettelijke basis te zijn. Door een wettelijke regeling wordt tevens voldaan aan de eis dat het voor burgers voorzienbaar moet zijn op welke wijze inbreuk op de persoonlijke levenssfeer kan worden gepleegd.

In de zaak Niemietz versus Duitsland¹³ sprak het Europese Hof voor de rechten van de mens sprak zich uit over een huiszoeking in een advocatenkantoor. In deze zaak oordeelde het Hof in rechtsoverweging 29 met betrekking tot het begrip privé-leven dat “het te restrictief zou zijn het concept te beperken tot een – binnencirkel – waarin het individu zijn persoonlijk leven kan leiden zoals hij wenst en daarvan de hele buitenwereld uit te sluiten als niet behorend tot die binnencirkel”. In rechtsoverweging 31 zegt het Hof: “het interpreteren van de woorden privé-leven en woning als eveneens omvattend bepaalde professionele of zakelijke activiteiten of locaties is overeenkomstig met het object en het doel van artikel 8 EVRM”. Bovendien staat deze ruime interpretatie van de begrippen woning en privé-leven de verdragstaten niet in de weg om inbreuken op grond van het tweede lid van artikel 8 EVRM toe te passen.

De redelijke verwachtingen ten aanzien van de persoonlijke levenssfeer hoeven zich dus niet te beperken tot locaties die strikt genomen als privé worden gezien, zoals bijvoorbeeld de eigen woning. Ook op de werkplek heeft een burger, conform de uitspraak in Niemietz versus Duitsland, recht op bescherming van de persoonlijke levenssfeer. Immers een werknemer brengt daar een relatief groot gedeelte van de dag door, waarbij zeker het element identiteit en persoonlijke ontwikkeling, al dan niet in relatie tot contacten met anderen, van belang zijn.

In de zaak Perry tegen het Verenigd Koninkrijk¹⁴ maakt het Europese Hof duidelijk waar grenzen bereikt zijn van het toestaan van cameragebruik in het publieke domein. De casus ging over het speciaal afstellen van een beveiligingscamera in het politiebureau ten behoeve van het maken van opnamen van een verdachte voor identificatiedoelen. Het Europese Hof achtte dit gebruik van de camera onrechtmatig en overwoog dat in het algemeen onder punt 1 “artikel 8 EVRM, ook het recht op identiteit en persoonlijke ontwikkeling omvat. Het recht om relaties aan te gaan met andere mensen in de buitenwereld kan ook activiteiten in een professionele of werkomgeving omvatten. Daarmee kunnen ook activiteiten met andere personen, zelfs in het publieke domein, binnen het bereik van privé-leven vallen”.

Reasonable expectation in Nederlandse jurisprudentie

Twee voorbeelden van uitspraken van de Hoge Raad der Nederlanden, beiden van 19 maart 1996, zijn: NJ 1997/85 over het openen van een op de openbare weg staande auto met beslagen ramen waarin een drugs gebruikende man werd aangetroffen en NJ 1997/86 over

¹² Opinie 4/2004, pagina 5.

¹³ NJ 1993/ 400, 16 december 2000 Niemietz v. Duitsland.

¹⁴ <http://hudoc.echr.coe.int>, Straatsburg, 17 oktober 2003.

cameratoezicht in de cel waarmee werd waargenomen dat een verdachte door middel van het urineren over zijn handen kruitsporen trachtte te verwijderen.

Bij het arrest NJ 1997/85 gaat het om de vraag of de verbalisanten, zonder wettelijke basis, het portier van een op de openbare weg staande auto met beslagen ramen, waarin iemand zat, mochten openen. De aangetroffen persoon was bezig met het gebruiken van drugs. De Hoge Raad is van mening dat de verbalisanten in kwestie, omdat de man achter het stuur zat, niet er van uit hoefden te gaan dat deze persoon onbevangen zichzelf wilde zijn. Op grond van het oude artikel 28 Politiewet mochten de verbalisanten de deur openen van deze niet afgesloten auto, om na te gaan in welke toestand de man verkeerde. Er was volgens de Hoge Raad geen schending van de persoonlijke levenssfeer.

Het arrest NJ 1997/86 beantwoordt de vraag of heimelijke en continue observatie door de politie in de verhoorfase met behulp van een videocamera en monitor is toegestaan. Daarnaast of het observatieverslag daarvan bruikbaar is voor het bewijs. In deze zaak werd met behulp van de camera gezien dat een verdachte van een dodelijke schietpartij, in de politiecel trachtte de kruitsporen te verwijderen door over zijn handen te urineren. Volgens de Hoge Raad mag een verdachte die op grond van artikel 62, eerste lid WvSv die opgehouden is voor verhoor "aan geen andere beperkingen worden onderworpen dan voor het doel van die ophouding of in het belang van de orde volstrekt noodzakelijk zijn" (rechtsoverweging 5.4.).

Verder stelt de Hoge Raad in dezelfde rechtsoverweging dat, om te voorkomen dat bewijsmateriaal verdwijnt of onbruikbaar wordt gemaakt, er in het belang van het onderzoek bewaking door een politieambtenaar mogelijk is. Deze vorm van bewaking is ook mogelijk door middel van visuele controle eventueel met een technisch hulpmiddel (camera) waarbij de verdachte in een andere ruimte is ondergebracht. Vereist is dan echter wel dat de verdachte op de hoogte is gesteld van deze vorm van controle en bewaking. In deze casus bleek dat niet het geval te zijn en omdat de verdachte zich onbespied mocht wanen (de controle was niet medegedeeld en ook niet kenbaar) was er sprake van een verstrekkende maatregel die zonder afzonderlijke voorziening bij of krachtens formele wet in strijd is met artikel 10 Grondwet, artikel 1 WvSv en artikel 8, eerste lid EVRM.

Deze uitspraak is in overeenstemming met de uitspraak in het arrest Perry versus het Verenigd Koninkrijk waarin het Europese Hof voor de rechten van de mens oordeelde dat de politie camerabeelden, gelet op de afwijking van het normale gebruik, niet voor bewijs mocht gebruiken, ondermeer omdat de verdachte niet op de hoogte was gesteld van het afwijkend gebruik van de camerabeelden. Samengevat, geheime en continue camera-observatie in die fase van het opsporingsonderzoek is niet toegestaan, tenzij bij of krachtens wet in deze maatregel is voorzien.

In Nederlandse jurisprudentie worden soortgelijke uitspraken gedaan over het bereik van de bescherming van de persoonlijke levenssfeer.

In het Zwolsman-arrest, Hoge Raad der Nederlanden van 19 december 1995, NJ 1996/249 was ondermeer de vraag in het geding naar het vereist zijn van een wettelijke grondslag voor het plegen van een inbreuk op de persoonlijke levenssfeer. Daarnaast speelt de vraag voor welke onderzoekshandelingen van de politie wettelijke grondslagen vereist zijn. Beide kwesties werpen ook licht op de vraag naar het bereik van de bescherming van de persoonlijke levenssfeer en het moment waarop hierop een inbreuk wordt gepleegd. In de casus had de politie onder andere vuilniszakken van verdachte opgehaald en onderzocht ten behoeve van het opsporingsonderzoek. Daarnaast was er onder valse voorwendselen een scanner geplaatst op een locatie in de nabijheid van de woning van verdachte met als doel telefoongesprekken af te luisteren. Ook werden inkijkoperaties uitgevoerd in de pro-actieve fase van het onderzoek. De Hoge Raad was overigens van mening dat de inkijkoperaties zowel in de pro-actieve fase als in een later stadium hebben plaatsgevonden.

Voor het onderzoek van de vuilniszakken gold volgens de Hoge Raad het principe van de res nullius, dat wil zeggen dat de eigenaar door het buiten zetten van het huisvuil geen verwachting meer kon hebben ten aanzien van de bescherming van zijn persoonlijke levenssfeer. Hij had immers afstand gedaan van de zaken. Ten aanzien van het op afstand af luisteren van de telefoongesprekken redeneerde de Hoge Raad dat het een bekend feit is dat mobiele gesprekken gemakkelijk af te luisteren zijn. Wel mag ook bij mobiele telefonie enig respect voor de persoonlijke levenssfeer worden verwacht, zeker als het gaat om het gedurende een langere tijd (drie weken) met behulp van speciale voorzieningen “doelbewust en stelselmatig” af luisteren en opnemen van mobiele gesprekken. Met stelselmatig wordt hier het begrip bedoeld zoals geformuleerd in artikel 126g en 126o WvSv. Het af luisteren en opnemen van mobiele telefonie vormt dus een inbreuk op artikel 8 EVRM en artikel 10 Grondwet en vereisen volgens de Hoge Raad dus een grondslag in een wet in formele zin.

Gebruik van beelden voor een niet-kenbaar doel

Wanneer er sprake is van een situatie waarin de bescherming van de persoonlijke levenssfeer aan de orde is, luidt de vervolgvraag, op welk moment er een inbreuk plaats vindt.

In rechtsoverweging 38 zegt het Europese Hof in de Perry-zaak versus het Verenigd Koninkrijk: “het enkel monitoren van een persoon in het publieke domein, dus zonder opslag van de beelden, is op zichzelf geen inbreuk op het privé-leven. Echter het opslaan van de beelden en het systematische of permanente karakter van het bestand kan aanleiding zijn om wel te spreken over een inbreuk.” Hoewel de camera zichtbaar was opgehangen, hoefde de verzoeker er geen rekening mee te houden dat de beelden gebruikt zouden worden voor een ander doel, te weten identificatie en bewijs in een strafzaak. En hoewel er regels waren voor het gebruik van camera's en er toestemming gevraagd was bij hogere autoriteiten, was toch in strijd met de regels gehandeld. De verzoeker was namelijk niet geïnformeerd over het maken van de beelden voor een ander doel, er was niet gevraagd om toestemming voor dit specifieke gebruik van de beelden en de verzoeker noch de advocaat waren in de gelegenheid gesteld het tonen van de video aan getuigen bij te wonen.

De inbreuk was daarmee (rechtsoverweging 49) niet in overeenstemming met de wet zoals het tweede lid van artikel 8 EVRM vereist. Het cameratoezicht op zichzelf en de doelen waarvoor het cameratoezicht wordt gebruikt, dienen vooraf kenbaar te zijn. Beperkingen op de bescherming van de persoonlijke levenssfeer moeten bij wet geregeld worden, zodat voorzienbaar is dat die beperking mogelijk is.

3.3 Het verwerken van persoonsgegevens

De beginselen voor de bescherming van persoonsgegevens zijn voor het eerst in het Europees Databeschermingsverdrag vastgelegd. Artikel 2 omschrijft het begrip persoonsgegevens als “any information relating to an identified or identifiable individual”. Dit betekent dat er onderscheid gemaakt moet worden tussen gegevens die informatie verschaffen over een persoon (relating to) en de vraag of de identiteit van die persoon redelijkerwijs kan worden vastgesteld (identifiable).

De vraag of camera- of videobeelden wel persoonsgegevens zijn, is in diverse rechtsbronnen verduidelijkt. In de Richtlijn 95/46/EG wordt gesteld dat camerabeelden persoonsgegevens zijn. In de rechtspraak is uitgemaakt dat videobeelden persoonsgegevens kunnen zijn. Ook in het wetsvoorstel cameratoezicht op openbare plaatsen wordt ervan uitgegaan dat videobeelden van personen persoonsgegevens zijn.

Er zijn drie categorieën beelden te onderscheiden. De eerste categorie wordt gevormd door beelden die als zodanig kunnen leiden tot identificatie van personen. De tweede categorie bevat beelden die in combinatie met andere gegevens leiden tot identificatie en identificeer-

baarheid. De derde categorie beelden zijn beelden die na bewerking kunnen leiden tot identificatie en identificeerbaarheid van personen.

Beelden die leiden tot identificatie van personen

In het kader van cameratoezicht zijn beelden uit de eerste categorie altijd persoonsgegevens. Als een persoon duidelijk is afgebeeld, dan heeft de opname altijd betrekking op die persoon. Naam en adresgegevens zijn niet noodzakelijk om het beeld op zichzelf als identificerend aan te merken. Vaak verschaft het beeld nadere informatie over die persoon. De beelden geven meestal weer op welke plaats iemand was, wat diens uiterlijke kenmerken zijn, bevatten de elementen van een signalement en laten zien hoe iemand zich gedraagt. Daarom zijn volgens de *Opinie 4/2004* van WP 29 beelden die binnen een gesloten televisiecircuit gebruikt en opgeslagen worden, ook al zijn ze niet gekoppeld aan andere kenmerken van personen, toch persoonsgegevens¹⁵. Voor wat betreft de gedraging geldt dat dit natuurlijk ook een kwestie van interpretatie is. Een voorbeeld van dit laatste, was het geval dat op de monitor iemand te zien was die iets goudkleurigs in een apparaat stopte. Gedacht werd dat de betrokkene voor het station op straat een pistool aan het laden was. Bij aanhouding van de persoon bleek dat hij de batterijen van zijn muziekkaraat had verwisseld.

Beelden die in combinatie met andere gegevens leiden tot identificatie

Bij cameratoezicht kan het ook gaan om het met behulp van videobeelden herkennen van personen door deze beelden te koppelen aan informatie die op een andere wijze is verkregen. Ook in zo'n geval zijn de beelden aan te merken als identificerende gegevens en dus als persoonsgegevens. Een toepassing waarmee al gewerkt wordt, is de koppeling aan en vergelijking met een beeldbestand ten behoeve van gezichtsherkenning. Van het combineren van persoonsgegevens is ook sprake als er geen gezichten van personen worden gefilmd, maar kentekens of pincodes (verkregen bij pinautomaten). Als er in combinatie met andere gegevens een identificerend gegeven ontstaat, dan is er voldaan aan het vereiste van de mogelijkheid tot identificatie.

Of beelden persoonsgegevens zijn, is niet afhankelijk van het gebruik van technische hulpmiddelen¹⁶. De kwestie is of de beelden personen identificeerbaar maken en daar kunnen technische hulpmiddelen of aanvullende gegevens voor gebruikt worden. Dus ook als kentekens worden gefilmd naar aanleiding van een snelheidsovertreding is er sprake van verwerking van persoonsgegevens, als de verantwoordelijke via een koppeling met andere gegevens waarover hij de beschikking heeft de identiteit van de kentekenuhouder kan vaststellen.

Volgens de *Opinie* van de WP 29 ontstaat identificeerbaarheid eveneens door het vergelijken van gegevens afkomstig van derden of door inzet van specifieke technieken. De bron van herkomst van die aanvullende gegevens is niet van belang voor het kunnen aanmerken van gegevens als persoonsgegevens. Een voorbeeld hiervan is het koppelen van beelden van klanten aan hun bankactiviteiten die gelogd worden in de banksystemen. Een ander voorbeeld is het vergelijken van beelden van camera's met foto's of vingerafdrukken van diezelfde klanten.

Met de huidige stand van de techniek en als de camera's goed geïnstalleerd zijn, zal de kwaliteit van de beelden in het algemeen steeds beter worden; terwijl ook de geautomatiseerde beeldverwerking steeds beter wordt. In het verleden werden de meeste beelden gemaakt met zogenaamde analoge camera's. De beelden werden opgeslagen op videobanden. Terugkijken was alleen mogelijk door middel van het terugspoelen van de band. Voor de toepasselijkheid van de WBP is onder andere vereist dat wordt voldaan aan de criteria die zijn gesteld aan een bestand. Het moet dan gaan om een gestructureerd geheel van persoonsgegevens, volgens een bepaald criterium toegankelijk en betrekking hebbend op verschillende personen. Er moet sprake zijn van een zodanig gesystematiseerde opslagstructuur, dat het gericht zoeken en raadplegen mogelijk is. Hiervan is ook sprake als met behulp van een logboek het tijdstip of de datum in combinatie met een vermelding van hetgeen is opgeslagen op de band wordt geregistreerd. Vervolgens werden analoge systemen met terugzoekfuncties ontwikkeld. Deze

¹⁵ *Opinie 4/2004*, pagina 16.

¹⁶ *Opinie 4/2004*, pagina 15.

systemen vallen onder het bereik van de WBP, evenals de recent ontwikkelde digitale camera's die de analoge camera's – zeker die zonder terugzoekfunctie – zullen vervangen.

Beelden die na bewerking leiden tot identificatie en identificeerbaarheid

Onduidelijke beelden zijn niet zonder meer als identificerende gegevens te kwalificeren. Van belang is of de verantwoordelijke redelijkerwijs in staat is tot identificatie te komen. Daarom zijn luchtfoto's die niet uitvergroot kunnen worden totdat personen duidelijk zichtbaar zijn, geen persoonsgegevens. Ook beelden van verkeersstromen of mensenmassa's die niet uitvergroot kunnen worden, vallen niet onder de definitie¹⁷ en daarmee buiten de toepasselijkheid van de WBP.

Het verwerken van persoonsgegevens

De verwerking van persoonsgegevens omvat volgens artikel 1, sub b, WBP alle handelingen of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van toezending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Deze definitie is niet limitatief en maakt duidelijk dat alle handelingen ten aanzien van beelden die aangemerkt moeten worden als persoonsgegevens, onder het begrip verwerking van persoonsgegevens moeten worden verstaan.

3.4 Grondslag voor de verwerking

De verwerking van persoonsgegevens in het kader van cameratoezicht heeft een wettelijke grondslag nodig. Voor cameratoezicht in het kader van de openbare orde ligt de grondslag voor wat betreft de WBP met name in de goede vervulling van de publiekrechtelijke taak door een bestuursorgaan (artikel 8 onder e WBP). Voor de WPOLR geldt de in artikel 2 van de Politiewet gedefinieerde politietaak. Aan de burgemeester is de taak handhaving van de openbare orde opgedragen.

Het systematisch en langdurig bewaken van gedeelten van het publieke domein op gezag van het lokale bestuur ten behoeve van de handhaving van de openbare orde is een vorm van cameratoezicht die na de wijziging van de Gemeentewet op een uitdrukkelijke wettelijke grondslag berust.¹⁸

Deze wettelijke grondslag schept echter geen verplichting voor gemeenten cameratoezicht toe te passen. Het schept een bevoegdheid om – door middel van een raadsverordening – het instrument cameratoezicht in te zetten. Het wetsvoorstel cameratoezicht op openbare plaatsen voorziet in een regeling van cameratoezicht in het kader van de handhaving van de openbare orde. Daaronder valt ook bestuurlijke voorkoming van strafbare feiten.

Artikel II.8 van de Europese Grondwet geeft in het tweede lid als grondslag voor verwerking: "met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet". Daarmee wordt opnieuw bevestigd dat een gerechtvaardigd belang dat als grondslag voor verwerking van persoonsgegevens kan dienen, ook een wettelijke basis moet hebben. De Europese Grondwet grijpt hiermee terug op zowel de Richtlijn 95/46/EG en artikel 8 van het EVRM als op het Europese Databeschermingsverdrag uit 1981.

3.5 Doel van de verwerking

Het doel van het gebruik van camerabeelden moet helder omschreven en precies bepaald zijn. Veel voorkomende doelen in de praktijk van het cameratoezicht zijn het voorkomen van

¹⁷ Opinie 4/2004, pagina 17.

¹⁸ Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 3.

strafbare feiten, beveiliging van personen en goederen, handhaving van de openbare orde, het gericht inzetten van hulpverleningsdiensten en de politie en het opsporen van strafbare feiten.

In de memorie van toelichting bij het wetsvoorstel cameratoezicht op openbare plaatsen schrijft de regering over het toetsingskader voor het gebruik van cameratoezicht: “de gebruiker dient een redelijk belang te hebben bij het gebruik als het gaat om de private sector. In de (semi)-publieke sector dient het gebruik noodzakelijk te zijn voor diens taak”¹⁹. Dat betekent dat voor de overheid geldt dat het moet gaan om een te beschermen publiek belang en dat het concreet moet gaan om cameratoezicht dat noodzakelijk is in het kader van de openbare orde. Voor private partijen geldt dat er sprake moet zijn van een gerechtvaardigd belang. Dit gerechtvaardigd belang kan bijvoorbeeld liggen in het voorkomen van winkeldiefstal. Wel dient dit noodzakelijk te zijn hiervoor en dient het privacybelang van de geregistreerde niet te prevaleren.

Het wetsvoorstel cameratoezicht op openbare plaatsen voorziet in een regeling van camera-toezicht in het kader van de handhaving van de openbare orde. Daaronder valt ook bestuurlijke voorkoming van strafbare feiten, tenminste als deze invloed kunnen hebben op de orde en rust in de gemeente. Dit doel begrenst de bevoegdheid van het lokale bestuur tot inzet van toezichtcamera's. De memorie van toelichting sluit de opsporing van strafbare feiten door de lokale overheid expliciet uit. Hiermee wordt, naar het CBP aanneemt, bedoeld de opsporing van strafbare feiten als zodanig en niet de toezichthoudende taak op grond van bijzondere wetten. De beelden kunnen echter “onder strikte voorwaarden” wel voor de opsporing van een concreet strafbaar feit worden gebruikt²⁰. Het wetsvoorstel stelt dat: “Indien de verzamelde gegevens in een concreet geval relevant zijn voor de opsporing van strafbare feiten, biedt artikel 9 van het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Trb. 1988, 7) de mogelijkheid van doelafwijkend gebruik, indien dit is voorzien bij wet en het een noodzakelijke maatregel is in een democratische samenleving in het belang van (onder meer) de publieke veiligheid en de onderdrukking van strafbare feiten”²¹. Artikel 151c Gemeentewet voorziet in die wettelijke regeling. In het kader van de proportionaliteit en de subsidiariteit moet er echter wel sprake zijn van een concrete aanleiding op grond waarvan verondersteld kan worden dat de beelden gegevens bevatten die noodzakelijk zijn voor de opsporing van een gepleegd strafbaar feit.²²

Cameratoezicht moet dus beperkt blijven tot noodzakelijke beelden van uitsluitend openbare plaatsen. Dat betekent dat het gebied waar cameratoezicht plaatsvindt, niet groter dan noodzakelijk mag zijn. Dit betekent ook dat het in huizen, tuinen of bedrijven meekijken niet is toegestaan. Om dit te vermijden kan bijvoorbeeld de camera gedeeltelijk geblindeerd worden om deuren en ramen niet in beeld te brengen. Ook beperking van de tijdsduur per dag of week kan leiden tot het voldoen aan de noodzakelijkheidseis. Er zijn in veel situaties specifieke uren aan te wijzen waarin met enige regelmaat overlast plaats vindt, zoals bijvoorbeeld in uitgaansgebieden.

Een doel dat niet is toegestaan, is de inzet van cameratoezicht ten behoeve van het vastleggen op beeldmateriaal van bepaalde groeperingen of personen op grond van ras, religieuze of politieke overtuiging, het lidmaatschap van een vakbond of seksuele gewoonten. De lokale overheid heeft niet de bevoegdheid controles of toezicht uit te oefenen op het bezoek aan bijvoorbeeld vakbondsbijeenkomsten als zodanig²³. Bij gebrek aan bevoegdheden ontbreken eveneens de verantwoordelijkheden van de lokale overheid. Dat betekent bijvoorbeeld dat in het kader van de openbare orde in bekende prostitutiebuurten en -straten cameratoezicht is toegestaan, waarbij het brandpunt van de belangstelling is gericht op de straat en niet de deuren en ramen van de betreffende panden in beeld gebracht mogen worden. Met andere

¹⁹ Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 4.

²⁰ Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 9.

²¹ Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 9.

²² Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 8, pagina 13.

²³ Richtlijn 95/46/EG, artikel 8 en Opinie 4/2004, pagina 26.

woorden alleen de straat en het trottoir mogen door de camera's worden bestreken. Dat er wel controles mogen plaatsvinden op bijvoorbeeld illegale werknemers betekent niet dat met camera's binnen de werkruimtes in prostitutiebuurten gekeken mag worden. Als het gaat om cameratoezicht in prostitutiestraten door de ondernemingen in die straten, dan geldt het principe dat de focus moet zijn gericht op ramen en deuren van de bedrijven. Deze camera's mogen niet meer in beeld brengen dan onvermijdelijk is, dus niet meteen de hele "Walletjes" in Amsterdam bestrijken.

De instelling van het blikveld van de camera is dus een punt waar aandacht aan besteed moet worden in elke context. In die zin kent bescherming van de persoonlijke levenssfeer ook een technische kant. Bij de technische specificaties moet gekeken worden naar de effecten op de bescherming van de persoonlijke levenssfeer.

3.6 Noodzakelijkheid en selectiviteit

Een belangrijk voorwaarde voor een rechtmatige grondslag is de noodzakelijkheid van het verwerken van de betreffende persoonsgegevens. De noodzakelijkheid wordt getoetst met behulp van de vraag of het inzetten van cameratoezicht proportioneel en subsidiair²⁴ is.

Proportionaliteit is de evenwichtige verhouding tussen doel en middel (cameratoezicht). De ernst van de feiten kan cameratoezicht rechtvaardigen. Voor kleine vergrijpen die op zichzelf staan, ligt cameratoezicht niet voor de hand. Immers de inbreuk op de persoonlijke levenssfeer moet gerechtvaardigd worden door de ernst van de feiten. Voor bijvoorbeeld de bestrijding en voorkoming van kleine overtredingen, zoals het te vroeg buiten zetten van huisvuil, is cameratoezicht niet proportioneel. Er blijft een belangenafweging noodzakelijk tussen het recht op de persoonlijke levenssfeer en het voorkomen van die feiten. Wat een gemeente mag rekenen tot de openbare orde moet in een Algemene plaatselijke verordening worden vastgelegd. Voor de inzet van cameratoezicht dient er dus een relatie te zijn met de openbare orde en een zekere ernst van de feiten die een gemeente wil voorkomen en bestrijden.

Subsidiariteit verwijst naar de beoordeling of, als het doel er om vraagt, een middel voldoende kan dienen ter voorkoming of bestrijding van de gebeurtenissen. Dit wil zeggen dat het doel of de doelen de inzet van dit middel vereisen en dat het past binnen en bij de overige getroffen maatregelen. Met andere middelen ter preventie en andere veiligheidsmaatregelen is nog geen afdoende resultaat bereikt of kunnen niet bereikt worden. Als, bijvoorbeeld, het plaatsen van een hek bij een winkelpassage de winkels na sluitingstijd afdoende beveiligd, dan is cameratoezicht niet meer nodig en daarmee bovenmatig.

Voordat tot de inzet van cameratoezicht kan worden overgegaan, dus voor installatie van de camera's, dient aangetoond te worden dat cameratoezicht in het belang van de handhaving van de openbare orde noodzakelijk is.²⁵ De regering is in het wetsvoorstel cameratoezicht op openbare plaatsen van mening dat het in de rede ligt vooraf een analyse van de veiligheids-situatie ter plekke te maken. Hierbij dient aandacht besteed te worden aan de mate van onveiligheid of het voorkomen van wanordelijkheden, de andere getroffen maatregelen en de effectiviteit daarvan, de mogelijke inbreuk op de persoonlijke levenssfeer en de afweging van dit belang tegen het belang van de openbare orde.

Selectiviteit

Ook in situaties waarin cameratoezicht niet bij wet is voorzien, of waarin een discretionaire bevoegdheid bestaat om te kiezen voor dit middel, dient de verantwoordelijke een zorgvuldige afweging te maken in hoeverre cameratoezicht is toegestaan. Selectiviteit bij de inzet van cameratoezicht is essentieel voor de rechtmatigheid. Afgewogen moet worden of er sprake is van een juiste maatvoering en of de inbreuk op de persoonlijke levenssfeer evenredig is

²⁴ Opinie 4/2004, pagina 18.

²⁵ Kamerstukken II, 2003-2004, 29 440, nr. 3, pagina.4.

aan het doel van het toezicht. Met andere woorden, de verantwoordelijke dient selectief te zijn bij de inzet van het middel cameratoezicht, naar plaats, duur, kring van te registreren personen, aantal camera's en tijdstippen. Het horen van betrokken partijen in het toezichtsgebied voorafgaand aan besluitvorming is voor een dergelijke afweging dienstig. Ook dient aandacht besteed te worden aan het aantal personen dat toegang heeft tot de beelden en aan de wijze waarop beelden op welke gronden aan derden worden verstrekt.

De adequaatheid van het ingezette cameratoezicht in relatie tot het doel vereist verder dat de verzameling van gegevens tot een minimum wordt beperkt. Dat is niet alleen in het belang van de bescherming van persoonsgegevens, maar tevens voor het op orde en beheersbaar houden van de informatiehuishouding. Selectiviteit is in artikel 6, eerste lid sub c van de Europese privacyrichtlijn gedefinieerd als een situatie waarin de verzamelde persoonsgegevens "toereikend, ter zake dienend en niet bovenmatig [...] zijn, uitgaande van de doeleinden waarvoor ze worden verzameld of waarvoor ze vervolgens worden verwerkt".

3.7 Verantwoordelijke en regie

Uit de bevoegdheid voor het door middel van cameratoezicht verzamelen van persoonsgegevens volgt wie verantwoordelijk is voor de inzet van cameratoezicht en voor de regie en uitvoering. De vraag naar de regie wordt in juridische termen bepaald door wie de verantwoordelijke is.

De verantwoordelijke voor het cameratoezicht is diegene die doel en werkwijze voor de gegevensverwerking vaststelt. Deze definitie is afkomstig uit artikel 1 sub d, WBP, dat weer is gebaseerd op de Europese Richtlijn 95/46/EG.

Gemeente

Verantwoordelijke in het kader van gemeentelijk cameratoezicht ten behoeve van de handhaving van de openbare orde is de burgemeester. Deze is immers verantwoordelijk voor de openbare orde. Het kan ook zijn dat het gemeentebestuur in brede zin zich verantwoordelijk acht. Met name zal zich dit voordoen als het lokaal bestuur cameratoezicht inpast in een samenhangend gemeentelijk veiligheidsbeleid. Dan ligt voor de hand dat de verantwoordelijkheid door het college van B&W wordt gedragen. Na de invoering van het wetsvoorstel cameratoezicht op openbare plaatsen zal echter de burgemeester de voor de uitvoering verantwoordelijke zijn op basis van een gemeentelijke verordening.

Voor wat betreft de operationele uitvoering van cameratoezicht in het kader van de handhaving van de openbare orde door de politie is de korpsbeheerder de verantwoordelijke. De gegevens worden in deze situatie opgeslagen in een politieregister.

Politie

De WPOLR definieert in artikel 1 de korpsbeheerder (een burgemeester uit de politieregio) als verantwoordelijke. Het wetsvoorstel cameratoezicht op openbare plaatsen geeft geen uitsluitel over de bevoegdheidsverhouding tussen burgemeesters die tevens korpsbeheerder zijn en burgemeesters die dat niet zijn. In het regio-overleg zullen de betreffende burgemeesters deze bevoegdheidsverdeling nader moeten regelen.

Openbaar Ministerie

Gaat het om de strafrechtelijke opsporing van strafbare feiten, dan is de verantwoordelijke degene die de leiding heeft over het opsporingsonderzoek, dit wil zeggen de Officier van Justitie.

Particulier toezicht

In situaties waarin het gaat om cameratoezicht ter beveiliging van particulier eigendom, is de particulier of het bedrijf dat het toezicht uitvoert of laat uitvoeren de verantwoordelijke. Voor particulier cameratoezicht geldt dat daarbij rekening moet worden gehouden met de rechten van anderen en de begrenzing van wat er precies in beeld gebracht kan worden. Het

bewaken door middel van camera's van de openbare weg als deel van het publieke domein behoort exclusief tot de taak van de overheid.

Publiek-private samenwerking

Het wetsvoorstel cameratoezicht op openbare plaatsen is duidelijk over situaties waarin sprake is van gemengd toezicht: publiek/private samenwerking bij cameratoezicht in het publieke domein, is gebonden aan de vereisten van de te wijzigen Gemeentewet. Met andere woorden de regels zoals die staan beschreven in het wetsvoorstel cameratoezicht op openbare plaatsen, gelden dan voor zowel de publieke partij (gemeente en eventueel politie) als voor de private partij waarmee samengewerkt wordt.

In een brief aan de Tweede Kamer over de inzet van particuliere veiligheidszorg in het publieke domein²⁶ laat de Minister van Justitie weten dat voor deze inzet instemming gevraagd moet worden aan de gemeenteraad en de lokale driehoek. Ook in deze situatie moet het cameratoezicht ingebed zijn in het lokale veiligheidsbeleid en dient de politie de operationele regie te behouden. Afspraken over informatieverstrekking, dit wil zeggen de voorlichting aan het publiek, de uitwisseling van gegevens tussen partijen en het gebruik van deze gegevens moeten worden vastgelegd.

Overigens is het mogelijk dat de voor het toezicht verantwoordelijke organisaties niet zelf het cameratoezicht uitvoeren. Het uitkijken van de beelden kan eventueel door een particuliere beveiligingsorganisaties plaatsvinden. De verantwoordelijkheid van de overheid voor het cameratoezicht in het publieke domein moet in een dergelijk samenwerkingsverband wel duidelijk tot uitdrukking komen.

Nieuwe Gemeentewet

De burgemeester is op grond van artikel 172 Gemeentewet verantwoordelijk voor de handhaving van de openbare orde. Het voorgestelde artikel 151c Gemeentewet specificereert deze verantwoordelijkheid nog eens en wijst de burgemeester aan als degene die op grond van een verordening van de gemeenteraad en in overleg met de Officier van Justitie het cameratoezichtsgebied vaststelt. De tekst luidt "...de gemeenteraad de burgemeester bij verordening de bevoegdheid kan verlenen om te besluiten tot toepassing van cameratoezicht op een openbare plaats, indien het belang van de handhaving van de openbare orde daartoe noodzaakt"²⁷.

De burgemeester bedient zich bij het cameratoezicht in dit kader van de politie. Daarmee wordt de operationele regie bij de politie neergelegd. De politie is immers de instantie die bij openbare ordehandhaving de uitvoerende taak heeft. Het cameratoezicht heeft volgens de memorie van toelichting een aanvullende functie en mag het menselijk toezicht niet vervangen²⁸. Het wetsvoorstel cameratoezicht op openbare plaatsen spreekt over de burgemeester in zijn rol als korpsbeheerder. Hierbij is niet geregeld hoe dit georganiseerd dient te worden ten aanzien van burgemeesters die geen korpsbeheerder zijn.

De regiefunctie bij de politie betekent niet dat uitsluitend politieambtenaren de beelden mogen uitkijken. Ander personeel kan, als dat onder regie van de politie plaats vindt, de beelden uitkijken. Het besluit om actie te ondernemen naar aanleiding van de waargenomen beelden ligt uitsluitend bij de politie. In de praktijk zullen beelden hiertoe worden doorgesluisd naar de politie zodat een bevoegde politieambtenaar een beslissing kan nemen over het wel of niet opvolgen van de signalen.

Een sluitstuk van het cameratoezicht zal de periodieke evaluatie door de burgemeester ten behoeve van de gemeenteraad zijn. Dit is een verplicht meetinstrument waarmee geëvalueerd kan worden of het cameratoezicht effectief is geweest en beoordeeld kan worden of het cameratoezicht wel of niet gehandhaafd moet worden tijdens een volgende periode. Niet effectief cameratoezicht kan een ongeoorloofde inbreuk op de bescherming van de persoonlijke levenssfeer betekenen.

²⁶ Brief Ministerie van Justitie, 7 mei 2004, kenmerk 5266617/504, aan de Voorzitter van de Tweede Kamer.

²⁷ Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 8.

²⁸ Kamerstukken II, 2003-2004, 29 440, nr.3, pagina 11.

3.8 Verder gebruik

In het kader van de handhaving van de openbare orde en onder regie van de politie zal verstrekking van beelden in principe niet verder moeten gaan dan aan personeel betrokken bij het videocameratoezicht. Het principe is immers het zo beperkt mogelijk verwerken van persoonsgegevens. Als er een concrete aanwijzing is dat er strafbare feiten waarneembaar zijn op de beelden of als er aanwijzingen op de beelden staan die kunnen leiden tot het opsporen van verdachten, getuigen of slachtoffers, dan mogen de beelden ook aan het Openbaar Ministerie verstrekt worden.

Volgens de memorie van toelichting van het wetsvoorstel cameratoezicht op openbare plaatsen, mag cameratoezicht ook functioneren als hulpmiddel bij het gedoseerd en gericht inzetten van politiemensen²⁹. Ook het bekijken van situaties ten behoeve van de veiligheid van hulpverleners is toegestaan, zowel tijdens de inzet van de hulpverleners, als achteraf ten behoeve van de opsporing van verdachten die zich gewelddadig hebben gedragen ten opzichte van die hulpverleners. In de praktijk kijkt de politie al dan niet in samenwerking met hulpverleners naar dit soort beelden en gebruikt men de beelden vooraf om te bezien of de route voor bijvoorbeeld de brandweer vrij is.

Op grond van artikel 30 WPOLR mogen de beelden voor beveiligings- of bewakingsdoelen ook aan particulieren worden verstrekt. Op die particulier rust dan wel een geheimhoudingsplicht en is het gebruik beperkt tot het doel waarvoor ze zijn verstrekt. Een voorbeeld zou kunnen zijn dat de beelden van een probleemsituatie bij een stadion worden verstrekt aan de leiding van dat stadion ten behoeve van het nemen van passende beveiligingsmaatregelen in de toekomst.

Zoals hiervoor is aangegeven ziet de Gemeentewet niet op cameratoezicht door particulieren. De burgemeester kan ten behoeve van de handhaving van de openbare orde niet zonder meer gebruik maken van de particuliere camera's of samen met particulieren het toezicht uitoefenen. Gemeenten zullen bij samenwerking met anderen dan de politie altijd moeten voldoen aan de vereisten van artikel 151c Gemeentewet.

3.9 Kwaliteit van gegevens

Richtlijn 95/46/EG schenkt in artikel 6 aandacht aan de kwaliteit van de gegevens. Hieronder worden begrepen, de eerlijke en rechtmatige verwerking, de toereikendheid en de niet-bovenmatigheid van gegevens in relatie tot het doel, de nauwkeurigheid van gegevens en de rechten van betrokkenen. De kwaliteit van persoonsgegevens is cruciaal voor een juiste beoordeling van de situatie ter plaatse en daarmee voor een juiste beoordeling van de individuele burger. Dit vereist de inzet van goede apparatuur onder toereikende omstandigheden. Dit wil zeggen goede verlichting en een behoorlijk transport van beelden naar de meldkamer.

Eerlijke en rechtmatige verwerking wil zeggen dat het verwerken van de beelden kenbaar dient te zijn en dat deze alleen voor de omschreven doelen verder worden verwerkt. Ook de rechten van betrokkenen, de geregistreerde burger, dienen gehonoreerd te worden conform de voorschriften van de Richtlijn en de vertaling daarvan in nationale wetgeving. Verder wordt onder de kwaliteit van de gegevens verstaan dat de omvang zo beperkt mogelijk gehouden wordt zowel als het gaat om het aantal als de soort gegevens. De juistheid van gegevens is een essentiële voorwaarde, ook al om een correcte beoordeling van de waarde van de gegevens te kunnen maken. De kwaliteit van gegevens is daarmee een element van de eerlijke en rechtmatige verwerking.

Het doel van de verwerking dient gespecificeerd, expliciet en gelegitimeerd te zijn. De beelden moeten in overeenstemming met deze eis verwerkt worden. De verwerking moet ook

adequaat, relevant en niet bovenmatig zijn. Ook dient de verdere verwerking overeenkomstig de doelen te zijn. Dit betekent met name dat cameragebruik selectief dient te zijn. Zie ook paragraaf 3.6. De gegevens mogen slechts een beperkte periode bewaard worden, zie verder paragraaf 3.12.

3.10 Beveiliging

Beveiligingsmaatregelen zijn noodzakelijk om te voorkomen dat onbevoegden kennis nemen van de beelden, maar ook om de beelden te beschermen tegen manipulatie, wijziging of vernietiging. Daartoe dient bijvoorbeeld de toegang tot de informatie beperkt te worden tot een zo klein mogelijke groep bevoegde functionarissen, die in verband met het doel van het cameratoezicht en uit hoofde van hun functie toegang nodig hebben. Ook onderhoud aan de installatie kan een grond zijn om toegang te krijgen tot de beelden.

Als de beelden exclusief bedoeld zijn voor de preventie en opsporing van strafbare feiten, dan verdient het de voorkeur te werken met een twee-sleutelsysteem. Een sleutel is dan in beheer bij de politie, zodat alleen met behulp van de politie toegang tot de opgeslagen beelden verkregen kan worden.

Als er sprake is van automatische signaalopvolging naar aanleiding van de beelden, dan dienen er specifieke veiligheidsmaatregelen getroffen te worden. Geautomatiseerde signaalopvolging betekent dat naar aanleiding van de beelden, zonder menselijke tussenkomst, signalen worden gegenereerd die direct leiden tot acties van bijvoorbeeld de politie. Dit is denkbaar bij camerasystemen die op grond van bepaalde bewegingspatronen signalen doorgeven die indicaties vormen dat er onmiddellijk moet worden ingegrepen.

De gebruikte apparatuur dient van goede kwaliteit te zijn, zodat bijvoorbeeld bij herhaald gebruik van de opslagmedia, de beelden volledig overschreven worden³⁰.

Een element van de beveiliging is het voldoende trainen van het personeel dat beelden uitkijkt en de opslag en de vermenigvuldiging verzorgt. Het bekijken van beelden en de interpretatie daarvan vergt training. Op welke wijze de werkzaamheden moeten worden uitgevoerd, dient minimaal onderdeel te zijn van de training. Het onjuist interpreteren van beelden of het niet onderkennen van foutmarges bij het herkennen van personen vergroot het risico van inbreuken op de bescherming van de persoonlijke levenssfeer en kan leiden tot onterechte acties en verdenkingen.

3.11 Kenbaarheid

Cameratoezicht moet kenbaar zijn, zowel dat het plaats vindt als voor welke doelen, opdat degenen die met behulp van cameratoezicht in beeld worden gebracht, hun rechten kunnen uitoefenen (zie verder paragraaf 3.13). Alle Europese regels, en ook de WBP geven aan dat de betrokkenen (degenen van wie beelden worden gemaakt) geïnformeerd dienen te zijn dat er beelden worden opgenomen en voor welk doel. Het wetsvoorstel cameratoezicht op openbare plaatsen benadrukt deze kenbaarheid eveneens.

Er geldt een zogenaamde notificatieplicht. Dit wil zeggen dat de verantwoordelijke de plicht heeft ervoor te zorgen dat de in beeld gebrachte personen kunnen weten dat hun gegevens worden verwerkt en waarvoor. Om die reden is de strafbaarstelling van heimelijk cameratoezicht in het WvSr uitgebreid. Met borden, publicaties en informatie-avonden kan aan deze informatieplicht worden voldaan. Het precies aangeven waar welke camera hangt is niet noodzakelijk. Wel moet duidelijk zijn dat en om welke reden in een bepaald gebied de camera's gebruikt worden. Borden voorzien van symbolen en met vermelding van de verantwoordelijke zijn in principe voldoende.

³⁰ Opinie 4/2004, pagina 25.

3.12 Bewaartermijn

Ook de opslag van beelden dient goed geregeld te worden. De vraag is ten eerste of beelden opgeslagen moeten worden en ten tweede voor hoe lang. De Richtlijn 95/45/EG en ook de Opinie van de WP 29 schrijven voor dat de bewaartermijn zo kort mogelijk moet zijn en bij het specifieke doel moet passen. De Opinie spreekt over een maximale bewaartermijn van een week³¹. Geautomatiseerde vernietiging is mogelijk en wordt aanbevolen in de Opinie 4/2004.

Het wetsvoorstel cameratoezicht op openbare plaatsen spreekt eveneens van een bewaartermijn van zeven dagen. Deze termijn geldt in situaties waarin de beelden geen aanleiding vormen tot nader onderzoek of specifiek opsporingsonderzoek. De bewaartermijn kan verlengd worden als er een concrete aanleiding is te vermoeden dat informatie over strafbare feiten op de beelden is opgeslagen. De beelden kunnen dan vervolgens worden gebruikt als informatie ten behoeve van het opsporen van die strafbare feiten en daarna in het strafdossier gevoegd worden als bewijsmateriaal.

3.13 Rechten van betrokkenen

Om controle op de verwerking van persoonsgegevens te kunnen uitoefenen worden aan de betrokkenen rechten toegekend. Dit zijn met name het recht op inzage en het recht om te verzoeken om correctie, afscherming of verwijdering van persoonsgegevens. Deze rechten zijn niet absoluut. Eveneens heeft een betrokkene in principe het recht op verzet tegen opname van zijn beeltenis.

Dit laatste recht is niet aanwezig als op grond van wettelijke voorschriften beelden worden opgenomen. Bedoeld wordt hier het cameratoezicht ten behoeve van de handhaving van de openbare orde en het observeren door de politie op grond van strafvorderlijke bevoegdheden.

Inzage

Betrokkenen moeten inzage kunnen krijgen in de over hen verwerkte persoonsgegevens. Dit recht is vastgelegd in zowel de Europese Richtlijn, als in de WBP, de WPOLR en het wetsvoorstel cameratoezicht op openbare plaatsen. Het recht op inzage in de opgenomen beelden geldt echter niet in alle omstandigheden. Deze beperkingen moeten dan wel in rechtsregels vastgelegd zijn. Deze uitzonderingen op deze rechten worden uitgewerkt in de paragrafen over de Gemeentewet, de Wet bescherming persoonsgegevens en de Wet politieregisters.

Uitzonderingen op het inzagerecht

Een persoon heeft het recht op kennisname van de beelden waarop hij of zij staat, ook als op die beelden andere personen zichtbaar zijn. Deze anderen kunnen immers, omdat het camera-toezicht kenbaar is gemaakt, weten dat zij in beeld gebracht zijn. Het feit dat ook anderen zichtbaar zijn voor de verzoeker, is in principe geen reden om het recht op inzage niet te honoreren. Hierop is echter een uitzondering mogelijk op grond van artikel 43, sub e WBP. Op grond van dit artikel kan het belang van die andere persoon of personen dermate zwaar wegen dat op grond daarvan het verzoek tot inzage kan worden geweigerd.

Voor beelden opgeslagen in politieregisters geldt artikel 21 WPOLR. Dit artikel geeft twee uitzonderingen, te weten de goede uitvoering van de politietaak en de gewichtige belangen van derden. Van de eerste uitzonderingsgrond kan sprake zijn als de politie nog bezig is de beelden te onderzoeken. Er is in beginsel geen reden om de beelden niet te laten inzien, omdat vanwege de kenbaarheid van de beelden, er geen reden is om op grond van de politietaak de beelden vooralsnog geheim te houden. Alleen als er sprake is van een concreet opsporingsonderzoek kan deze weigeringsgrond van toepassing zijn. De tweede uitzonderingsgrond, het gewichtige belang van derden, moet worden afgewogen tegen het belang van de verzoeker die om inzage vraagt.

De verzoeker die om inzage vraagt hoeft dit inzageverzoek niet te motiveren. Dit betekent dat de verzoeker geen belang hoeft aan te geven of hoeft op te geven voor welk doel hij verzoekt om inzage. In voorkomende gevallen kan het inzageverzoek tot doel hebben een klacht tegen de politie in te dienen en deze klacht te onderbouwen met door de politie te tonen beelden.

Ook als de gewijzigde Gemeentewet van kracht zal zijn, dan kan de situatie zich voordoen dat na het verstrijken van de bewaartermijn het inzageverzoek wordt ingediend. Als in die situatie de beelden niet zijn overgeheveld in het kader van de opsporings- en vervolgingsonderzoek, dan is er feitelijk geen inzage in de beelden meer mogelijk. Het kunnen voldoen aan een eventueel inzageverzoek is geen zelfstandige reden om beelden langer te bewaren. Dat geldt echter niet voor aanvullende gegevens zoals naam, adres en commentaar op de beelden die naar aanleiding van de beelden zijn opgeslagen in een journaal, tenzij die ook weer verwijderd zijn binnen dezelfde termijn. Is dit niet het geval dan dient de politie inzage te verlenen in die andere gegevens.

Correctierecht

Het correctierecht kan ingeroepen worden op grond van artikel 36 van de WBP en artikel 22 van de WPOLR. De verantwoordelijke moet op grond van artikel 20 WPOLR binnen vier weken beslissen of een verzoek tot correctie van persoonsgegevens wordt gehonoreerd. Van het weigeren van het verzoek moet de verantwoordelijke de betrokkene binnen vier weken na het indienen van het verzoek, gemotiveerd op de hoogte stellen. Een verzoek dat na het verstrijken van de bewaartermijn binnenkomt zal, tenzij de beelden langer voor met name opsporing van strafbare feiten worden bewaard te laat komen. Als een verzoek binnen de bewaartermijn wordt gedaan zijn twee werkwijzen denkbaar. De beslissing wordt snel genomen zodat de bewaartermijn niet wordt overschreden. De tweede werkwijze voorziet in het selecteren en bewaren van de betreffende beelden direct na ontvangst van het verzoek. Vervolgens kan binnen de termijn van vier weken worden beslist of inzage en correctie mogelijk is of niet. Bij weigering van inzage dienen de beelden, met het oog op de rechtsbescherming die tegen deze beslissing openstaan, ook te worden bewaard.

In principe kan tegelijkertijd met het verzoek om inzage ook een verzoek om correctie worden ingediend. Gelet op de voorgestelde bewaartermijn van zeven dagen, onder normale omstandigheden, ligt het in de rede een gecombineerd verzoek in te dienen. Vanwege het registrerende karakter van de beelden, zal een correctieverzoek niet snel toegewezen worden. Camera's nemen alleen beelden op van wat er binnen het bereik van de camera valt waar te nemen. Echter de opnamehoek van de camera en de vertekening die daarvan het gevolg kan zijn, kunnen leiden tot niet-correcte interpretaties. Een toelichting op de beelden kan dan leiden tot een andere interpretatie van hetgeen waar te nemen is. De correctie kan zo betrekking hebben op bij de beelden opgeslagen andere gegevens, zoals bijvoorbeeld gegevens in een bijbehorend journaal over de persoon: naam, interpretatie van de beelden of het commentaar op de beelden. Deze gegevens kunnen wel voor correctie in aanmerking komen. Een reële mogelijkheid hiertoe zal onderdeel moeten zijn van de procedures voor cameratoezicht. Dit geldt ook voor beelden en gegevens die inmiddels werden opgeslagen in andere politieregisters, omdat de beelden voldeden aan de criteria voor opname in die andere registers. Het inzage en correctierecht voor deze andere registers is nader geregeld in de desbetreffende politiereglementen.

Recht op afscherming

Het recht op afscherming van de beelden en eventuele aanvullende gegevens is verwoord in artikel 22, eerste lid van de WPOLR en artikel 36, eerste lid van de WBP.

Een gefilmde persoon kan vragen de beelden niet verder te verwerken of af te schermen als de beelden niet ter zake dienend zijn. Dit afschermingsrecht is van toepassing binnen de reguliere bewaartermijn, maar ook nadat beelden zijn overgeheveld naar opsporingsdossiers.

Recht van verwijdering

Artikel 36 WBP en artikel 22 WPOLR geven de betrokkene het recht te verzoeken om verwijdering van diens persoonsgegevens. Voor camerabeelden geldt doorgaans een bewaartermijn van zeven dagen, zie ook paragraaf 3.12. Worden de beelden gebruikt voor opsporings- en vervolgingsdoelen dan worden de beelden overgeheveld naar reguliere politieregisters, zodat de bewaartermijnen van die registers van toepassing zijn.

3.14 Melding, reglementsplicht, verordening

Totdat het wetsvoorstel voor aanpassing van de Gemeentewet in werking treedt, kunnen gemeenten het cameratoezicht in het kader van de openbare orde zowel onder het wettelijk regime van de WBP brengen of onder het regime van de WPOLR, indien althans de politie een reglement conform de vereisten van de WPOLR opstelt. Na het overgangsjaar zal niet de WBP, maar de WPOLR of de mogelijke opvolger van deze laatste wet van toepassing zijn.

Onder het WBP-regime is het vrijstellingsbesluit en meer specifiek artikel 38, niet van toepassing zodra sprake is van cameratoezicht in het kader van de handhaving van de openbare orde. Dat betekent dat lokale overheden die deze vorm van cameratoezicht toepassen, moeten voldoen aan de meldingsplicht van artikel 27 WBP. Indien een gemeente een functionaris voor de gegevensbescherming heeft aangesteld en deze bij het College bescherming persoonsgegevens is aangemeld, dan kan de melding ook bij deze functionaris plaatsvinden.

De Wet politieregisters ziet op de verwerking van persoonsgegevens door de politie met het oog op de politietoek. In het huidige wettelijk regime valt het cameratoezicht onder de regels van de reguliere registers. Dat betekent dat de korpsbeheerder voor het cameratoezicht in het publieke domein de verwerking van de beelden in een politieregister onderbrengt. Voor een register dient een reglement opgesteld te worden waarin het doel, de werkwijze, de verantwoordelijke en de rechten van betrokkenen nader worden vastgelegd binnen het kader van de regels van de WPOLR.

Het voorstel cameratoezicht op openbare plaatsen regelt het onderbrengen van de camera-beelden in een tijdelijk register, zoals geformuleerd in artikel 13 van de WPOLR. De zogenaamde tijdelijke registers zijn speciale bestanden bestemd voor onderzoeken die gericht zijn op het opsporen van een of meer bepaalde, zware delicten. Oorspronkelijk zijn deze registers bedoeld om met spoed aan bepaalde opsporingsonderzoeken die naar hun aard tijdelijk waren, snel te kunnen beginnen. Om die reden werd op grond van onder andere artikel 8 Besluit politieregisters de reglementsplicht uitgesteld. Dit uitstel is in eerste instantie 12 maanden en kan vervolgens nog eens met 6 maanden verlengd worden. Deze regeling werd in het leven geroepen met het oog op het veelal spoedeisende karakter van de onderzoeken. De politie hoefde dan niet te wachten totdat er een reglement was opgesteld. De tweede reden was de beperking van de mogelijkheden tot verstrekking verbonden aan de tijdelijke registers. Gegevens uit een tijdelijk register kunnen worden verstrekt ten behoeve van de zogenaamde registers zware criminaliteit, het voorlopig register of voor het doel waarvoor het register zelf is aangelegd.

De genoemde redenen spelen echter bij cameratoezicht geen rol. Er is geen sprake van een spoedeisend opsporingsonderzoek. Het gaat immers om een instrument in het kader van de openbare orde. Als er beelden zijn waarop incidenten zichtbaar zijn, kunnen die beelden langer bewaard en gebruikt worden voor opsporing en vervolgingsdoeleinden. Een reden voor geheimhouding is evenmin aanwezig. In tegendeel, het cameratoezicht ten behoeve van de handhaving van de openbare orde moet kenbaar gemaakt worden op die plaatsen waar het cameratoezicht is ingezet. Voor de periode waarin de WPOLR van kracht is, een reglement echter nog steeds vereist. Dit betekent dus dat voor cameratoezicht, wanneer de registratie plaatsvindt in een politieregister, een reglement dient te worden opgesteld en aangemeld bij

het CBP. Binnen de politie wordt gewerkt aan een modelreglement voor cameratoezicht in het publieke domein. Dat reglement kan dan door alle politieregio's gebruikt worden voor de nadere afspraken omtrent cameratoezicht in het publieke domein.

Onder het regime van de Wet politiegegevens zal de reglementsplicht vervallen. Dat ontslaat de overheid en in casu de politie niet van de plicht behoorlijke procedures en afspraken vast te leggen over de toepassing van dit instrument, de verwerking van de beelden en de eventuele verstrekking.

In het wetsvoorstel cameratoezicht op openbare plaatsen wordt de bevoegdheid tot het overgaan van cameratoezicht geregeld in een verordening van de gemeenteraad. Hierin worden de afspraken vastgelegd. Met een reglement ter aanvulling van de verordening scheidt de overheid voor burgers en beslissers duidelijkheid over de toepassing van het instrument cameratoezicht. Burgers kunnen aan de hand van de verordening en het reglement hun rechten effectueren en de Raad wordt zo in staat gesteld de inzet van dit middel te evalueren.

Privacynormen voor de praktijk



- 4.1 Publiek domein en openbare plaats 47
- 4.2 Redelijke verwachting van respect voor de persoonlijke levenssfeer 48
- 4.3 Het verwerken van persoonsgegevens 50
- 4.4 Grondslag voor de verwerking 51
- 4.5 Doel van de verwerking 51
- 4.6 Noodzakelijkheid en selectiviteit 52
- 4.7 Verantwoordelijke en regie 54
- 4.8 Verder gebruik 55
- 4.9 Kwaliteit van gegevens 56
- 4.10 Beveiligingsplicht 56
- 4.11 Kenbaarheid 57
- 4.12 Bewaartermijn 57
- 4.13 Rechten van betrokkenen 57
- 4.14 Melding van verwerkingen en reglementsplicht 59

Het juridisch kader wordt in dit hoofdstuk verder uitgewerkt in praktische termen en voorbeelden. De concrete afwegingen bij het al dan niet introduceren of continueren van cameratoezicht moeten uiteindelijk door de raad en de burgemeester worden gemaakt. Deze afwegingen hebben betrekking op de specifieke omstandigheden in de gemeente. Deze context is van invloed op de inzet van bevoegdheden, de mate van de inbreuk op de persoonlijke levenssfeer en de redelijke verwachting die burgers mogen hebben ten aanzien van de bescherming hiervan.

De privacynormen voor cameratoezicht worden hieronder uitgewerkt in paragrafen die corresponderen met de juridische paragrafen van hoofdstuk drie over de sleutelbegrippen:

- publiek domein en de openbare plaats;
- redelijke verwachting;
- persoonsgegevens en de verwerking van persoonsgegevens;
- de grondslagen voor de verwerking;
- de doelen van de verwerking;
- de noodzakelijkheid en de selectiviteit;
- de verantwoordelijke voor de verwerking en de regiefunctie;
- de verdere verwerking;
- de kwaliteit van persoonsgegevens;
- de beveiliging;
- de kenbaarheid;
- de bewaartermijn;
- de rechten van betrokkenen;
- de melding van verwerkingen en de reglementsplicht.

4.1 Publiek domein en openbare plaats

Wat moet worden verstaan onder het publieke domein bij de inrichting van cameratoezicht? Het onderscheid tussen het publieke en het private domein is niet altijd even duidelijk. Het is een schaal met het publieke domein aan de ene kant en het private domein aan de andere kant.

Openbare plaats

Een openbare plaats is een plaats waar men komt en gaat en waarvoor geen beletselen gelden zoals een meldingsplicht, toestemming vooraf of entreegeld.

Voorbeelden van openbare plaatsen zijn de voor iedereen toegankelijke wegen, straten, openbare plantsoenen, speelweiden en parken. Ook vrij toegankelijke winkelpassages en winkelgalerijen, voor publiek toegankelijke gebouwen, stationspleinen en openbare (gemeentelijke) parkeerterreinen zijn openbare plaatsen.

Niet-openbare plaats

Tot een niet-openbare plaats heeft het publiek alleen onder voorwaarden toegang.

Voorbeelden van niet-openbare plaatsen zijn stadions, postkantoren, warenhuizen, restaurants en ziekenhuizen. Ook gemeentehuizen, discotheken en parkeergarages zijn dus geen openbare plaatsen. Hier kan met camera's toezicht worden gehouden waarbij het gaat om beveiliging van die plaats. Dit is van belang voor de vraag wie bevoegd is tot uitoefening van het cameratoezicht. Verder moet ook hier aan allerlei voorwaarden zijn voldaan zoals kenbaarheid voor de bezoekers en andere aanwezigen op deze plaatsen.

In plaatsen zoals stadions, ziekenhuizen, gemeentehuizen en discotheken kan het gaan om incidenten die de openbare orde verstoren en waarbij vervolgens opsporing aan de orde kan zijn. Voorbeelden zijn stadionrellen en vechtpartijen in uitgaansgelegenheden. Bij parkeergarages speelt het beveiligingsdoel de hoofdrol, maar kan bij vernielingen en diefstal de opsporing een belangrijke rol gaan spelen.

Besloten plaats (geen woning)

Een besloten plaats die geen woning is, is in beginsel niet vrij voor het publiek toegankelijk.

Voorbeelden zijn (gedeelten) van bedrijven en overheidsgebouwen die niet zonder meer voor het publiek toegankelijk zijn. Cameratoezicht is hier mogelijk voor de beveiliging van personeel, eigendommen of bedrijfsprocessen. Ook in deze situatie moet cameratoezicht aan voorwaarden voldoen en moet het kenbaar zijn voor bezoekers en personeel.

Besloten plaats (woning)

Een woning is de besloten plaats bij uitstek, waarbij cameratoezicht door anderen dan de bewoners al heel snel een inbreuk zal zijn op de persoonlijke levenssfeer. Het gaat hier bij uitstek om het privé-domein.

Cameratoezicht in het kader van de openbare orde is dus niet toegestaan. Cameratoezicht in het kader van de strafrechtelijke rechtshandhaving vereist een bevel op grond van het Wetboek van Strafvordering en valt buiten het bestek van deze studie. Cameratoezicht ter beveiliging kan alleen toegepast worden door de bewoner op voorwaarde dat het kenbaar wordt gemaakt.

Schematisch samengevat levert dat het volgende overzicht op van de relatie tussen het karakter van de plaats en het doel van het cameratoezicht:

Plaats en doelen van cameratoezicht

Plaats/doel	Beveiliging	Openbare orde	Opsporing
Openbare plaats	ja	ja	ja
Niet-openbare plaats	ja	bepaalde gevallen	bepaalde gevallen
Besloten plaats, niet de woning	ja	nee	bepaalde gevallen
Besloten plaats, woning	ja	nee	bevel OvJ

4.2 Redelijke verwachting van respect voor de persoonlijke levenssfeer

Het uitgangspunt bij cameratoezicht dient in het algemeen te zijn dat inbreuken op de persoonlijke levenssfeer zoveel mogelijk worden beperkt. Of dat het geval is, wordt ook bepaald door de verwachting die betrokkenen redelijkerwijs mogen koesteren ten aanzien van de mate van privacy die zij op een bepaalde plaats of in een context genieten. Deze redelijke verwachting van respect voor de persoonlijke levenssfeer bepaalt of cameratoezicht “zonder meer” mag worden uitgeoefend.

Ook voor de redelijke verwachting van respect voor de persoonlijke levenssfeer geldt dat er sprake is van een glijdende schaal die afhankelijk is van de context. Een persoon kan redelijkerwijs geen volledige privacy verwachten, indien hij zich begeeft in het publieke domein of in voor het publiek toegankelijke plaatsen. Maar het is ook niet zo dat daar de rechten en vrijheden zoals die veel sterker in de privé-sfeer bestaan, volledig ontbreken. Dit is eveneens gerelateerd aan het recht om zich in beginsel vrij en onbespied te bewegen, indien men rechtmatig binnen een land verblijft. In het publieke domein is de context mede bepalend hoe ver toezicht kan gaan en in hoeverre personen een redelijke verwachting van privacy mogen koesteren. Belangrijke doorgangswegen of knooppunten zijn een andere context voor cameratoezicht dan prostitutiestraten. De gegevens en beelden die op deze twee verschillende plaatsen worden verzameld, zijn van een andere orde als het gaat om het beschermen van de persoonlijke levenssfeer. Het bezoek aan een prostitutiebuurt wordt immers maatschappelijk en in het privé-leven anders beoordeeld dan het rijden op de openbare weg.

Voorbeeld: Een gemeente wilde ten behoeve van het handhaven van het prostitutieverbod buiten de tippelzone de overlastgevende bezoekers een sanctie opleggen. Daartoe wilde deze gemeente de naam en adresgegevens van deze bezoekers via de kentekens van de gebruikte auto's bij de Rijksdienst voor het wegverkeer (RDW) opvragen. De RDW was van mening dat zijn registratie van kenteken en persoonsgegevens voor dit doel niet gebruikt konden worden.

Naast de gevolgen van het opleggen van een dwangsom kan het bekend worden van bezoek aan prostituees verstreckende maatschappelijke gevolgen hebben. Mede om die reden is het naar het oordeel van het CBP dan ook niet toegestaan dat de gemeentelijke overheid in het kader van de openbare orde de naam en adresgegevens van prostituanten tracht te achterhalen op basis van kentekens. Gegevens over prostitutiebezoek moeten beschouwd worden als gevoelige gegevens. Hoewel de prostituanten zich op openbare plaatsen bevonden, mochten zij toch een zekere redelijke verwachting van privacy koesteren. Het onderscheid tussen openbare, niet-openbare en besloten plaatsen valt dus niet één op één samen met de gradaties van een redelijke verwachting van privacy.

De redelijke verwachting zich onbespied te weten mag een persoon hebben ten aanzien van het eigen of andermans huis. Zodra iemand zich in zijn of andermans huis bevindt, gaat het onder normale omstandigheden niet aan deze persoon met behulp van een camera in beeld te brengen of zelfs te bespieden.

Naast de woning zijn er ook andere locaties waar men een redelijke verwachting mag hebben zich onbespied te weten, bijvoorbeeld in kleedhokjes in gemeentelijke zwembaden of sportcomplexen of in al dan niet openbare toiletruimtes. Dergelijke ruimtes vallen niet onder het publieke domein. Het zijn plaatsen waar de burger terecht verwacht dat er sprake is van bescherming van de persoonlijke levenssfeer.

In ziekenhuizen en afdelingen voor eerste hulp mag de burger redelijkerwijs eveneens verwachtingen hebben ten aanzien van de bescherming van de persoonlijke levenssfeer. Er zijn ziekenhuizen die vooral ter beveiliging van het personeel en patiënten de ingangen en de eerste hulpafdelingen voorzien van camera's. Dit heeft meestal beveiliging als doel, daarnaast worden de beelden ook gebruikt voor opleidingsdoelen en kwaliteitsbewaking. Op bepaalde tijdstippen en bij bepaalde incidenten kan ook de openbare orde een doel van het cameratoezicht zijn. Vereist is wel dat het cameratoezicht kenbaar moet zijn voor het personeel, de patiënten en bezoekers, ook omdat hier sprake is van het verwerken van gevoelige gegevens, te weten medische gegevens. Door middel van het cameratoezicht worden medische gegevens verwerkt die vallen onder het medisch beroepsgeheim.

Voorbeeld: In Noorwegen is in een ziekenhuis in Oslo een experiment gestart met cameratoezicht in de eerste hulpafdeling. Hoewel het cameratoezicht in strijd kan zijn met het basisprincipe dat iedereen die medische zorg nodig heeft, deze onbelemmerd moet kunnen krijgen, heeft de Noorse privacytoezichthouder ingestemd met dit experiment. De beelden worden gemaakt voor opleidingsdoelen en worden maximaal 2 dagen bewaard. In Nederland heeft de Nederlandse vereniging van ziekenhuizen een handreiking opgesteld voor het inrichten van cameratoezicht in ziekenhuizen voor de beveiliging van personen en eigendommen. Omdat het medisch beroepsgeheim hier in het geding is, wordt het gebruik van de beelden voor opsporingsdoelen alleen in zeer uitzonderlijke situaties toegestaan.

Ook op de werkplek mag een mate van redelijke verwachting van respect voor de persoonlijke levenssfeer gekoesterd worden. De Europese rechter is van mening dat het begrip privé-leven niet alleen beperkt is tot de strikte privé-sfeer. Privé-leven kan zich ook uitstrekken tot zakelijke activiteiten en locaties. Een werknemer brengt immers een groot gedeelte van de dag op de werkplek door, terwijl ook daar identiteit en persoonlijke ontwikkeling, al dan niet in relatie tot contacten met anderen, van belang zijn. De redelijke verwachting ten aanzien van privacy op de werkplek wordt mede bepaald door context en plaats van die werkplek. Een medewerker op een gewone werkplek, waarvoor geen bijzondere omstandigheden gelden, mag de verwachting hebben onbespied het werk te kunnen uitvoeren.

Bijzondere omstandigheden kunnen dat anders maken, zoals bijvoorbeeld bij het werken in een casino aan de speeltafel. In deze context kan het, gelet op het financiële belang, en het

bestrijden van fraude of diefstal, redelijk zijn hierop toezicht te houden. Hierbij kan in samenhang met andere controlemaatregelen ook van camera's gebruik gemaakt worden. Ook een kassa in een winkel waar met enige regelmaat frauduleus handelen of diefstal door het personeel is geconstateerd, is een werkplek in een bijzondere context geworden. In samenhang met andere toezichts- en controlemaatregelen, kunnen ook hier camera's gebruikt worden. Het kan ook zijn dat de plaats waar gewerkt wordt in het publieke domein is gelegen. Dit geldt bijvoorbeeld voor de politie, hulpdiensten en parkeerwachten die een deel van hun werktijd in het cameratoezichtsgebied doorbrengen. Op dat moment is het onvermijdelijk dat deze werknemers in beeld worden gebracht.

Verder spelen het doel, het eventueel afwijkend gebruik en de intensiteit van het cameratoezicht evenals de eventuele opslag van beelden een rol bij het vaststellen van wat een redelijke verwachting is.

Beelden die overeenkomstig het doel – de handhaving van de openbare orde – worden gemaakt, mogen in principe niet voor een ander doel worden gebruikt, tenzij het gaat om de opsporing van ernstige strafbare feiten. Dit nevensdoel moet bij voorkeur bij de inrichting van het cameratoezicht worden vastgesteld en uitgewerkt om problemen met het gebruik van de beelden te vermijden. Uit Europese jurisprudentie blijkt dat camera's die voor beveiliging van een politiegebouw worden gebruikt, niet ook mogen worden gebruikt voor identificatiedoelen als de gefilmde persoon met die mogelijkheid geen rekening had hoeven houden en als de betreffende persoon en zijn advocaat geen gelegenheid hebben gekregen de beelden te bekijken en eventueel van commentaar te voorzien.

Ook de intensiteit van het cameratoezicht, de omvang van het gebied met camera's in samenhang met de duur van het toezicht, zijn van invloed op de verwachting die een burger mag hebben ten aanzien van de bescherming van zijn persoonlijke levenssfeer. Als een wijk vrijwel volledig en 24 uur per dag wordt bewaakt met camera's, dan hebben bewoners en bezoekers, ook degenen die niets te verbergen hebben, geen reële mogelijkheid meer zich vrij en zonder controle te bewegen in dat gedeelte van het publieke domein. Van een redelijke verwachting kan dan geen sprake meer zijn. Dit effect kan overigens ook een beslissende contra-indicatie opleveren voor een dergelijke massieve inzet van cameratoezicht.

4.3 Het verwerken van persoonsgegevens

Bij cameratoezicht met het oog op het handhaven van de openbare orde gaat het vrijwel altijd om het verwerken van persoonsgegevens, zeker indien de beelden ook worden opgeslagen.

Alles wat met deze beelden gedaan kan worden, moet beschouwd worden als een verwerking van persoonsgegevens inclusief het bewaren, verstrekken aan anderen of vernietigen ervan. Dat het bij het bekijken van camerabeelden gaat om het verwerken van persoonsgegevens, ook al zijn er in eerste instantie nog geen aanvullende gegevens zoals de naam, betekent dat de Wet bescherming persoonsgegevens (WBP) of de Wet politieregisters (WPOLR) van toepassing is.

Beelden moeten als persoonsgegevens worden beschouwd als de verantwoordelijke redelijkerwijs in staat is om tot identificatie of herkenning van personen te komen. Bij cameratoezicht doet zich doorgaans één van de volgende situaties voor:

- *personen worden direct geïdentificeerd* aan de hand van camerabeelden. De camerabeelden zijn dan zo duidelijk en helder dat deze beelden direct leiden tot identificatie van in beeld gebrachte personen. Het beeld kan in dit geval leiden tot een signalement zonder dat er andere gegevens nodig zijn om tenminste een beschrijving van een persoon te geven. De beelden geven weer waar iemand zich bevindt, diens uiterlijke kenmerken en hoe hij zich gedraagt.

- *personen worden herkend en geïdentificeerd door beelden te koppelen aan andere gegevens. Deze andere gegevens kunnen kentekens of pincodes (bij geldautomaten) zijn, maar ook al eerder gemaakte beelden die met het oog op een dergelijke vergelijking zijn opgenomen in een bestand.*
- *personen worden herkend en geïdentificeerd door de beelden te bewerken met technische hulpmiddelen.*

Aan het verwerken van beelden die redelijkerwijs niet leiden tot herkenning van personen, zijn dus minder voorwaarden gebonden dan beelden waarop personen wel herkenbaar zijn. Luchtfoto's die niet zodanig bewerkt kunnen worden dat ze leiden tot het herkennen van personen, bevatten geen persoonsgegevens. Ook beelden van verkeersstromen die niet uitvergroot kunnen worden, bevatten geen persoonsgegevens evenmin als beelden van mensenmassa's die niet uitvergroot kunnen worden.

4.4 Grondslag voor de verwerking

Voor de verwerking van persoonsgegevens – dus ook voor cameratoezicht in het publieke domein – is een wettelijke grondslag vereist.

De huidige grondslag is een algemene grondslag in de Gemeentewet, de WBP en de WPOLR. Deze algemene grondslag geeft op dit moment aan de burgemeester de bevoegdheid om cameratoezicht in te zetten in het publieke domein. Uit het CBP-onderzoek naar cameratoezicht in Nederlandse gemeenten blijkt dat het gebruikelijk is dat voordat de camera's worden ingezet, de burgemeester overleg voert met het College van Burgemeester en Wethouders en de gemeenteraad. Daarnaast wordt veelal overleg gevoerd met de korpschef en het Openbaar Ministerie¹ vanwege de relatie met de opsporing van strafbare feiten.

Na inwerkingtreding van de gewijzigde Gemeentewet is er een specifieke wettelijke regeling voor cameratoezicht voor de handhaving van de openbare orde. Deze grondslag voor cameratoezicht in het publieke domein zal dan uitgewerkt moeten worden in een verordening van de gemeenteraad. Daarin moet vastgelegd worden op welke plaatsen en hoe lang cameratoezicht voor de handhaving van de openbare orde mogelijk is.

Er is een bevoegdheid maar geen verplichting het middel cameratoezicht in te zetten. Voor de overheid geldt dat er sprake moet zijn van noodzaak tot het inzetten van dit middel. Voor de private sector geldt dat er een redelijk belang gediend moet worden met het cameratoezicht. Zodra er sprake is van een samenwerkingsverband tussen publieke en private organisaties, bijvoorbeeld tussen gemeente en horeca in een uitgaansgebied, zijn de regels die gelden voor de overheid van toepassing.

De noodzaak van de inzet van cameratoezicht in het publieke domein moet aantoonbaar zijn. Voordat camera's ingezet kunnen worden, moeten andere middelen, zoals een betere verlichting, horeca-afspraken of extra inzet van surveillanten op bepaalde tijdstippen, al toegepast worden. Ook de signaalopvolging dient geregeld te worden. Van noodzaak tot cameratoezicht kan dus alleen sprake zijn binnen een geheel van reeds genomen maatregelen.

4.5 Doel van de verwerking

Cameratoezicht in het publieke domein ten behoeve van de handhaving van de openbare orde, is een publiekrechtelijke taak. Daarbij hoort dat het doel helder omschreven en precies bepaald moet zijn.

Naast het hoofddoel kunnen er nevendoelen worden onderscheiden, waarvoor geldt dat dringend aanbevolen wordt ook die precies te omschrijven. Een eerste nevendoel is de zoge-

¹ Cameratoezicht in de openbare ruimte, Rapport 1; College bescherming persoonsgegevens, Den Haag, november 2003, pagina 16.

naamde bijvangst. Dat betekent dat beelden opgenomen met camera's bedoeld voor de handhaving van de openbare orde ook gebruikt worden voor identificatie en opsporing en vervolging van verdachten van strafbare feiten. Het gaat dan om feiten die in het strafrecht strafbaar zijn gesteld.

Een ander bekend nevendoeel is dat camera's in het publieke domein gebruikt worden ter ondersteuning van de inzet van de politie en hulpdiensten als de ambulancedienst en de brandweer. Dit gebruik van de camera's kan de inzet van deze diensten efficiënter en effectiever maken en kan bijdragen aan de verkleining van de risico's van de inzet van politie en hulpdiensten. Voor de inzet van hulpdiensten kan dan bijvoorbeeld nagegaan worden of de toegangswegen vrij zijn zodat een snelle inzet ook mogelijk is.

Een derde nevendoeel is het gebruik van de camera's in het publieke domein voor stelselmatige observatie door observatieteams. Hieraan is echter wel de voorwaarde verbonden dat de Officier van Justitie een bevel daartoe heeft afgegeven.

Bij de opsporing van strafbare feiten moet het gaan om ernstige feiten en incidenten die de openbare orde verstoren. Het gebruik van de beelden voor de opsporing van strafbare feiten betekent dat er een concrete aanwijzing of verdenking moet zijn dat de beelden gegevens bevatten die noodzakelijk zijn voor het opsporen van een strafbaar feit.

Voorbeeld: Gebruik voor meerdere doelen is gerealiseerd in een grote Nederlandse stad die een deel van het centrum en de aanlooproutes naar het centrum heeft voorzien van camera's. De handhaving van de openbare orde is het primaire doel. Met behulp van de camera's wordt ook de fietsenstalling bij het NS-station in beeld gebracht. Op die plaats vinden regelmatig drugsdeals en fietsendiefstallen plaats. Afhankelijk van de beschikbare capaciteit van de politie wordt opgetreden.

Het is niet toegestaan bepaalde groepen personen in beeld te brengen en eventueel de beelden vast te leggen, als daarbij geselecteerd wordt op grond van kenmerken als ras, religieuze of politieke overtuiging, lidmaatschap van een vakbond of seksuele gewoonten. Het filmen van bezoekers van bijvoorbeeld een moskee, om na te gaan wie deze plaats bezoekt, is dus niet toegestaan.

4.6 Noodzakelijkheid en selectiviteit

Cameratoezicht in het publieke domein, waarbij personen herkenbaar in beeld worden gebracht, moet noodzakelijk zijn. Deze noodzakelijkheidseis hangt samen met het recht op bescherming van de persoonlijke levenssfeer en de redelijke verwachting die een persoon hierover mag koesteren. Ook in het publieke domein heeft een persoon in beginsel, tot op zekere hoogte, het recht zich vrij en onbespied te bewegen.

Cameratoezicht kan, afhankelijk van de plaats, de intensiteit en in het algemeen de context ervan, een inbreuk zijn op de persoonlijke levenssfeer die een gerechtvaardigde grondslag moet hebben in de overheidstaak. Een prostitutiebuurt en een homo-ontmoetingsplaats zijn voorbeelden van plaatsen waar noodzaak, selectiviteit en redelijke verwachting in samenhang moeten worden gezien. Deze plaatsen behoeven meer bescherming van de persoonlijke levenssfeer dan een gewone straat of een verkeersplein.

De noodzakelijkheid van cameratoezicht kan ook blijken uit de aanleiding om over te gaan tot cameratoezicht. Een enkel incident is niet voldoende om aan de noodzakelijkheidseis te voldoen. Er moet sprake zijn van aantoonbare, ernstige feiten die de openbare orde bedreigen. Een serie van serieuze overlastgevende situaties in een uitgaansgebied kan dus wel aanleiding zijn om te bezien of cameratoezicht kan bijdragen aan de handhaving van de openbare orde. Incidenten die zich slechts sporadisch voordoen, zijn niet voldoende aanleiding om cameratoezicht in het publieke domein te rechtvaardigen. De aard, de frequentie en de ernst van de incidenten moeten de inzet van het middel dus rechtvaardigen.

Van belang is ook dat geregeld wordt in een Algemene plaatselijke verordening (APV), voor welke kleinere feiten het cameratoezicht gebruikt zal worden. Deze feiten moeten een relatie hebben met de openbare orde en er moet sprake zijn van een zekere ernst en regelmaat.

Het toepassen van cameratoezicht moet onderdeel zijn van een samenhangend pakket van maatregelen dat genomen is om de openbare orde te handhaven. Het vooraf maken van een veiligheidsanalyse en het op basis daarvan nemen van passende, op elkaar afgestemde maatregelen, voorkomt dat er onnodige en mogelijk overmatige inbreuken op de persoonlijke levenssfeer plaatsvinden.

Samenhangende maatregelen zijn bijvoorbeeld afspraken met ondernemers in het uitgaansgebied over sluitingstijden, of een betere verlichting en de inzet van extra politie op bepaalde tijdstippen. Het moet duidelijk zijn dat andere middelen zoals meer verlichting en meer surveillance, niet voldoende hebben bijgedragen aan het bewaren en herstellen van de openbare orde.

Cameratoezicht kan alleen effectief zijn, als het signaleren van ongewenste situaties wordt opgevolgd door de inzet van de politie. Camera's registreren incidenten maar grijpen niet in. Signaalopvolging is van belang voor het vertrouwen van het publiek in dit middel en in de overheid. Als in een gebied camera's hangen maar er wordt bij incidenten niet ingegrepen, dan zal het vertrouwen bij het publiek snel verdwijnen.

Voorbeeld: Een voorbeeld uit de praktijk betrof het niet opsporen van verdachten van zware mishandeling onder het oog van de camera. De politie kon vanwege capaciteitsproblemen en de prioriteittoekenning aan andere zaken deze verdachten niet opsporen. De slachtoffers waren in de met behulp van camera's geschapen veiligheid teleurgesteld. Nadat de slachtoffers van de mishandeling in de media de gebeurtenis en het niet vervolgen door de politie hadden bekend gemaakt, werd door de politie alsnog overgegaan tot opsporing van de verdachten.

De noodzakelijkheid van het cameratoezicht kan op termijn alleen onderbouwd worden door periodieke evaluatie van het cameratoezicht en de overige maatregelen. In de gemeentelijke verordening dient evaluatie van de inzet van camera's dus ook vastgelegd te worden en concreet vorm te krijgen.

Selectiviteit bij de inzet van cameratoezicht is van belang om het evenwicht tussen het belang van de openbare orde en de bescherming van de persoonlijke levenssfeer te realiseren. Het soort camera's, het aantal camera's, de duur van het toezicht, het aantal personen dat in beeld gebracht wordt en de tijdstippen waarop het middel wordt ingezet, moeten goed worden afgewogen. Als immers grote gedeelten van een stad opgenomen worden in het cameratoezichtsgebied, dan is de mogelijke inbreuk op de persoonlijke levenssfeer aanmerkelijk groter dan in een situatie waarin slechts een paar camera's zijn geïnstalleerd. Een punt van aandacht is tevens het zogenaamde verplaatsingseffect. Als gevolg van het aanwijzen van een bepaald gebied als cameratoezichtsgebied kunnen ongewenste activiteiten zich verplaatsen naar andere delen van de gemeente of de regio. In interviews voor deze studie met gemeenten bleek dat deze activiteiten zich niet geheel verplaatsen, maar zeker wel voor een deel. Onderzoekscijfers zijn echter niet beschikbaar.

Selectiviteit vereist ook dat bedrijfsruimtes, woonhuizen, of woonverdiepingen via deuren en ramen niet toch in beeld worden gebracht. Hiervoor kan de oplossing gezocht worden door het opnamebereik van camera's gedeeltelijk te beperken. In verschillende grote en middelgrote steden wordt dat al gedaan. Bij het in beeld brengen van het publieke domein c.q. de openbare plaatsen worden gedeelten van opnamen geblindeerd of vergrendeld. Daar waar camera's deuren en ramen van woningen of bedrijven in beeld komen, worden deze gedeelten van het beeld geblindeerd.

Ook beperking van de tijdsduur per dag of week is een vorm van selectiviteit. Vaak vindt overlast plaats op bepaalde locaties met een zekere regelmaat en op specifieke uren, zoals bijvoorbeeld in uitgaansgebieden. Cameratoezicht kan dan tot die tijdstippen beperkt worden. Deze laatste vorm van selectiviteit brengt ook met zich mee dat de kosten van de inzet van personeel beter beheersbaar blijven.

4.7 Verantwoordelijke en regie

De burgemeester is vanuit zijn verantwoordelijkheid voor de openbare orde, de verantwoordelijke voor het cameratoezicht, dat wil zeggen dat hij bepaalt dat er cameratoezicht wordt ingezet, voor welk doel en binnen welke grenzen. Dat betekent niet dat de uitvoering ook door de verantwoordelijke organisatie moet geschieden. Het is mogelijk dat bijvoorbeeld een particuliere beveiligingsorganisatie het feitelijke cameratoezicht uitvoert onder regie van de verantwoordelijke. Dit kan bijvoorbeeld in een bewerkersovereenkomst afgesproken worden. In deze overeenkomst wordt onder meer vastgelegd op welke wijze het personeel te werk gaat bij het uitkijken en hoe met de beelden verder om gegaan dient te worden.

In de huidige praktijk zijn de verantwoordelijkheid, regie en uitvoering verschillend geregeld. Binnen een gemeente is doorgaans de burgemeester de verantwoordelijke voor de openbare orde dan wel het gemeentebestuur in brede zin. De uitvoering van het cameratoezicht of de operationele regie wordt vaak aan de politie overgelaten; het regime voor de gegevensverwerking is dan de WPOLR. De burgemeester is dan in zijn functie als korpsbeheerder de verantwoordelijke. De operationele regie is daarbij in handen van de politie; de beelden worden verwerkt onder het regime van de WPOLR.

Het komt ook voor dat de gemeente de initiatiefnemer is en dat de politie een bescheidener rol speelt. Een enkele keer is de burgemeester de verantwoordelijke en voert de brandweer de regiefunctie uit; het regime voor de gegevensverwerking is dan de WBP.

Voorbeeld: Een gemeente heeft in samenwerking met de politie het cameratoezicht in de binnenstad gerealiseerd. De politie heeft nadrukkelijk de regierol gekregen, terwijl de beelden uitgekeken worden door beveiligingspersoneel dat speciaal is ingehuurd. Zodra sprake is van een incident, wordt dit doorgegeven aan de coördinator en deze beoordeelt en beslist of politiecapaciteit moet worden ingezet of niet.

Na wijziging van de Gemeentewet geldt voor het cameratoezicht in het kader van de handhaving van de openbare orde het volgende:

- exclusieve verantwoordelijkheid voor de burgemeester;
- inzet van cameratoezicht alleen op basis van een verordening vastgesteld door de gemeenteraad;
- gemeenteraad is niet verplicht een verordening op te stellen;
- operationele regiefunctie bij de politie;
- WPOLR (en de opvolger van de wet) vormt het regime voor de gegevensverwerking
- gemeenten die al cameratoezicht toepassen, krijgen met een overgangstermijn van een jaar de tijd om alsnog een verordening op te stellen na het van kracht worden van de gewijzigde Gemeentewet.

Ook particulieren en bedrijven kunnen cameratoezicht toepassen. Het gaat dan meestal om de bewaking van het eigendom. De eigenaar-verhuurder of de huurder zijn in deze situaties de verantwoordelijke. Ook als de verantwoordelijke een beveiligingsbedrijf heeft ingehuurd voor de uitvoering van het cameratoezicht, blijft de inhurende partij de verantwoordelijke. Verantwoordelijkheid en regie liggen bij degene die het cameratoezicht toepast of laat toepassen.

Voor het bedrijfsleven geldt dat bijvoorbeeld winkels en horecabedrijven cameratoezicht mogen toepassen als dat nodig is. Het is echter in principe verboden heimelijk cameratoezicht toe te passen. Het cameratoezicht moet kenbaar zijn voor het publiek, de bewoners en bezoekers. In deze situatie komt geen verandering als gevolg van de voorgestelde wijziging van de Gemeentewet.

Op cameragebruik door particulieren zijn de regels van de WBP of de Gemeentewet niet van toepassing, tenminste als er sprake is van persoonlijk gebruik. De normale regels voor het maatschappelijk verkeer tussen burgers gelden. Deze regels zijn vastgelegd in het Burgerlijk Wetboek.

Publiek-private samenwerking

Het toepassen van cameratoezicht in het publieke domein door overheid in samenwerking met het bedrijfsleven is in de huidige situatie niet duidelijk geregeld. Op diverse bedrijfsterrainen, heeft de gemeente samen met het bedrijfsleven cameratoezicht ingericht. Wie de verantwoordelijke is en wie de regie voert, is vaak naar eigen idee afgesproken. Soms is ook de politie erbij betrokken, zoals bij toezicht op uitgaansgebieden, stations en het openbaar vervoer.

In de toekomst zal ook bij publiek-private samenwerking, de burgemeester de verantwoordelijke zijn en de politie zal de regie voeren. Samenwerking tussen overheid en bedrijfsleven (zoals horecabedrijven en bedrijven langs cruciale toegangswegen en bedrijventerreinen) bij cameratoezicht in het kader van de openbare orde blijft wel mogelijk. Voor het bedrijfsleven gelden dan ook de regels die voor de overheid gelden.

Wanneer particuliere beveiligingsorganisaties worden ingezet bij het cameratoezicht in het publieke domein, ontstaat een speciale situatie. De verantwoordelijkheid berust dan bij de gemeente, in de persoon van de burgemeester. De Minister van Justitie geeft aan dat voor de inzet van particuliere veiligheidszorg in het publieke domein² instemming gevraagd moet worden aan de gemeenteraad en de lokale driehoek. Voor het overige gelden dezelfde normen. Ook in deze situatie moet het cameratoezicht ingebed zijn in het lokale veiligheidsbeleid en dient de politie de operationele regie te behouden. Afspraken over informatieverstrekking en het gebruik van informatie moeten worden gemaakt.

4.8 Verder gebruik

Onder verder gebruik wordt verstaan het gebruik van beelden anders dan voor het doel waarvoor de beelden zijn gemaakt. Voorbeelden van niet toegestaan verder gebruik zijn het verkopen van beelden, het afgeven of laten zien van beelden aan anderen die niet vanuit hun functie die beelden zouden moeten zien of het leveren van de beelden aan de media voor bijvoorbeeld een programma over bloopers. Het verder gebruik van de beelden dient zo beperkt mogelijk te zijn. Het verstrekken van beelden aan anderen is in principe niet toegestaan, tenzij er sprake is van verstrekking binnen samenwerkingsverbanden voor de taken van dat samenwerkingsverband. Een voorbeeld van publiek-private samenwerking is het samenwerkingsverband tussen de beveiligingstak van Schiphol en de op Schiphol gestationeerde marechaussee. Uitwisseling tussen deze twee organisaties is op grond van de doelstelling mogelijk.

In het algemeen geldt dat de beelden primair ten dienste van de handhaving van de openbare orde in het publieke domein worden gemaakt. Deze taak ligt bij de burgemeester. Wel mogen de beelden worden verstrekt voor opsporings- en vervolgingstaken aan de politie en het Openbaar Ministerie. Dit betekent dus dat:

- de beelden ook gebruikt mogen worden voor het gedoseerd inzetten van politie en hulp-

² Brief Ministerie van Justitie, 7 mei 2004, kenmerk 5266617/504, aan de Voorzitter van de Tweede Kamer der Staten-Generaal.

- diensten in situaties die de openbare orde verstoren;
- opgeslagen beelden eveneens gebruikt mogen worden voor het opsporen van verdachten die zich gewelddadig hebben gedragen ten opzichte van de politie en hulpverleningsinstanties als de brandweer;
- opgeslagen beelden ook aan het Openbaar Ministerie kunnen worden verstrekt als er een concrete aanwijzing bestaat om te veronderstellen dat er strafbare feiten waarneembaar zijn op de beelden, of als er aanwijzingen zijn dat de beelden bijdragen aan het opsporen van verdachten, getuigen of slachtoffers.

Het verdient aanbeveling deze mogelijkheden ook op te nemen in de doelomschrijving van het cameratoezicht in het publieke domein. Het doorleveren aan derden is in principe alleen mogelijk als dat voortvloeit uit de doelomschrijving.

4.9 Kwaliteit van gegevens

Op basis van de camerabeelden worden personen beoordeeld met eventueel grote gevolgen voor hun persoonlijk leven. De gevolgen van een onjuiste herkenning kunnen voor de betrokkene verstrekking en onaangenaam zijn. De kwaliteit van de beelden is daarom van groot belang; beelden dienen verder met de nodige zorgvuldigheid geïnterpreteerd te worden. Hoe goed de kwaliteit van de beelden moet zijn, is afhankelijk van het doel waarvoor ze worden gemaakt. Voor het herkennen van personen ten behoeve van bijvoorbeeld het handhaven van gebiedsontzeggingen is een goed beeld nodig. Om te kunnen dienen als bewijsmateriaal is er een goede close-up nodig.

Voorbeeld: In een gemeente wordt in het uitgaansgebied voor sluitingstijd tot een afgesproken tijd na sluitingstijd de verlichting in het desbetreffende gebied versterkt. Dit heeft tot gevolg dat voor het uitkijkend personeel goed zichtbaar is wat er gebeurt op het plein en dat de camera's goede beelden opleveren voor de politie voor het geval zich incidenten voordoen die opsporing en identificatie vereisen.

Een systeem dat kan bijdragen aan de veiligheid in het publieke domein is het zogenaamde early-warningsysteem. Dit is software waarmee aan de hand van vooraf ingestelde parameters bewegingspatronen worden ingesteld. Het systeem geeft een waarschuwing als er sprake is van afwijkingen van het patroon. Deze systemen zijn denkbaar bij het bewaken van parkeerterreinen, maar ook bij het in beeld brengen van grote groepen mensen en mogelijke incidenten die de openbare orde verstoren. Van belang daarbij is dat de beslissing hoe te handelen na een dergelijk signaal door mensen genomen wordt. Een afwijkend patroon is een indicatie en dient beoordeeld te worden door gekwalificeerde mensen.

Een systeem dat ook in het buitenland wordt gebruikt, is cameratoezicht gekoppeld aan een bestand met foto's ten behoeve van gezichtsherkenning. Nabij Manchester is in 2003³ een dergelijk systeem overigens door de politie buiten gebruik gesteld omdat het aantal onjuiste koppelingen te groot bleek te zijn. Leeftijden, geslacht en huidskleur bleken niet voldoende onderscheiden te worden door het systeem. Technische hulpmiddelen, zoals systemen voor gezichtsherkenning en gedragspatroonherkenning, werken verre van foutloos. Deze systemen kunnen wel een indicatie of een waarschuwingssignaal geven, maar niet de situatie interpreteren en beoordelen. Het is noodzakelijk dat een beslissing of er wel of geen actie moet worden ondernomen, wordt genomen na menselijke tussenkomst.

4.10 Beveiligingsplicht

Beelden moeten beveiligd worden tegen kennisname, manipulatie of vernietiging door onbevoegden.

De groep van functionarissen die kennis kan nemen van de beelden, dient zo klein mogelijk te zijn. De toegangen tot de uitkijkruijnte en de opslagruimte dienen goed beveiligd te zijn. De apparatuur dient in alle opzichten adequaat te zijn voor een rechtmatige verwerking. Bijvoorbeeld op het punt van het hergebruik van opslagmedia dienen beelden bij het overschrijven ook daadwerkelijk overschreven te worden. In Manchester worden bijvoorbeeld de beelden die gebruikt worden voor opsporing en vervolging fysiek uit de omgeving van de toezichthouders weggehaald en in een aparte kamer in een kluis op een andere gegevensdrager opgeslagen. De toegang tot de kamer en de kluis is voorbehouden aan een zeer kleine groep medewerkers die verplicht hun handelingen noteren in een logboek.

4.11 Kenbaarheid

Cameratoezicht in het publieke domein dient kenbaar te zijn. Dit betekent dat publiek of bezoekers die een bepaald gebied met cameratoezicht betreden, moeten kunnen weten dat er cameratoezicht wordt toegepast en wie de verantwoordelijke is.

Het kenbaar maken kan met borden die goed zichtbaar zijn opgehangen aan de grenzen van het toezichtsgebied. Daarnaast kan door middel van berichtgeving in kranten en andere media het publiek vooraf geïnformeerd worden en eventueel betrokken worden bij besluitvorming. Ook informatie-avonden voor omwonenden en ondernemers zijn een goed voorlichtingsmiddel. In Manchester wordt op goed zichtbare borden vermeld dat er cameratoezicht is en door wie het wordt toegepast. De burger weet dat er cameratoezicht is, kan zijn handelen daarop afstemmen en weet zo ook direct bij wie hij moet zijn mocht hij informatie over het cameratoezicht wensen.

Deze kenbaarheidseis geldt niet bij camera's ten behoeve van het toezicht op verkeerstromen. In de eerste plaats kunnen borden verkeersdeelnemers afleiden en daardoor gevaarlijk rijgedrag veroorzaken en in de tweede plaats worden de gefilmde kentekens niet gebruikt als persoonsgegevens. Dit wil zeggen dat in normale situaties er geen relatie wordt gelegd tussen kenteken en eigenaar van de auto.

4.12 Bewaartermijn

De bewaartermijn dient zo kort mogelijk te zijn, gerelateerd aan het doel van het cameratoezicht. In de huidige praktijk varieert de bewaartermijn tussen een en enkele dagen. In het wetsvoorstel Cameratoezicht op openbare plaatsen wordt een maximale bewaartermijn van zeven dagen voorgesteld. Dit geldt voor de beelden waarop geen incidenten in de openbare orde of strafbare feiten waarneembaar zijn.

Als er een concrete aanwijzing is dat er vermoedelijk strafbare feiten op de beelden waarneembaar zijn, dan kunnen de betreffende beelden apart worden opgeslagen en worden gebruikt voor de opsporing van die strafbare feiten en de vervolging. Voor dergelijke beelden geldt dat de bewaartermijn verlengd wordt tot het tijdstip waarop de beelden niet meer nodig zijn voor de opsporing, vervolging en berechting van de zaak.

4.13 Rechten van de betrokkenen

De rechten van betrokkenen moeten worden gewaarborgd. Betrokkenen hebben onder meer een inzagerecht, een correctierecht, een afschermingsrecht en een verwijderingsrecht. Het inzagerecht is het recht op het kunnen bekijken van gegevens over hem of haarzelf. Het correctierecht is het recht om gegevens over hem of haarzelf te mogen corrigeren, aanvullen of toelichten. Het afschermingsrecht is een recht op grond waarvan de persoon kan vragen om

de beelden en/of andere gegevens over hemzelf niet verder te gebruiken of te laten zien aan anderen. Het verwijderingsrecht is het recht van een persoon om te vragen beelden en/of gegevens over hem of haar te verwijderen uit de bestanden.

Uit het onderzoek naar cameratoezicht in gemeenten bleek dat vrijwel nooit om inzage wordt gevraagd. Voor het uitoefenen van het inzage-, correctie-, afschermings- of verwijderingsrecht was geen enkel verzoek door verantwoordelijken ontvangen. Het publiek is niet bekend met deze rechten en niet alle verantwoordelijken zijn zich bewust van het feit dat een betrokkene deze rechten heeft.

Inzagerecht

Het inzagerecht geeft een persoon die in beeld gebracht is, het recht inzage te vragen in die beelden en de eventueel daarbij opgeslagen andere gegevens. Het recht op inzage is niet absoluut: de politie kan inzage weigeren als dat noodzakelijk is voor de goede uitvoering van de politietoek of als er sprake is van gewichtige belangen van derden. Als een burger inzage vraagt, heeft de verantwoordelijke vier weken de tijd dit verzoek wel of niet in te willigen. Deze termijn verandert niet door het wetsvoorstel cameratoezicht op openbare plaatsen.

In de praktijk zal iemand die opnamen van hemzelf wil zien, binnen de zeven dagen het verzoek tot inzage moeten indienen. De beelden blijven immers na de voorgestelde wijziging van de Gemeentewet doorgaans maximaal zeven dagen bewaard. Het ligt in de rede dat de verantwoordelijke de beelden waarin inzage is gevraagd, zolang bewaart totdat de beslissing over het wel of niet toestaan van de inzage is genomen. Gezien het doel van het toezicht, namelijk handhaving van de openbare orde, zal er niet snel aanleiding zijn om inzage te weigeren. Immers, inzage in beelden waarop verder niets bijzonders is te zien, stuit niet op de criteria van de wettelijke weigeringsgronden.

Het is denkbaar is dat de verzoeker geen inzage krijgt, als er een serieuze verstoring van de openbare orde heeft plaatsgevonden. Als de politie nog bezig is met het uitkijken van het materiaal en het zoeken naar getuigen en/of verdachten, kan er aanleiding zijn om geen inzage toe te staan. Ook als de verzoeker kennelijk wil weten wie er allemaal nog meer betrokken waren bij een incident, kan het belang van derden in deze situatie zwaarder wegen.

Voor inzageverzoeken ten aanzien van beelden en aanvullende gegevens die opgenomen zijn in andere registers in het kader van een opsporingsonderzoek, gelden dezelfde weigeringsgronden. Beide verzoeken vragen om een afweging waarbij het recht op inzage wordt getoetst aan de weigeringsgronden. Bij opsporingsonderzoek zijn de weigeringsgronden eerder van toepassing.

Correctierecht

Met correctierecht wordt bedoeld dat een betrokkene (een in beeld gebrachte persoon) kan vragen de gegevens over hem of haar te corrigeren. Omdat het in feite gaat om een beeldregistratie van wat er op een bepaald moment is gebeurd, ligt correctie van beelden zelf niet voor de hand. De beelden worden vanuit een bepaalde camera-instelling en invalshoek genomen. Het beeld geeft daardoor mogelijk niet geheel weer wat er feitelijk is gebeurd. Een beeld kan achteraf echter niet vanuit een andere invalshoek nog eens opgenomen worden. Dit kan anders zijn voor eventueel opgeslagen aanvullende gegevens en voor de interpretatie van de beelden. Correctie betekent dan dat de verzoeker vraagt om een toelichting op de beelden te mogen geven, of om de aanvullende gegevens te mogen corrigeren. Een correctieverzoek kan plaatsvinden nadat iemand inzage heeft gehad. Echter om zowel de verzoeker als de organisatie niet te veel te belasten, kan een correctieverzoek tegelijkertijd met het inzageverzoek ingediend worden.

Recht van afscherming

Het recht van afscherming van beelden is een verzoek tot het niet verder gebruiken van bepaalde beelden. Dit is mogelijk zowel in de fase van de voorgestelde reguliere bewaartermijn van zeven dagen als na overbrenging van de beelden in een onderzoeksdossier van de politie. Het zal dan meestal gaan om beelden die intieme details weergeven over de verzoeker, die in sommige situaties niet van belang zijn voor het opsporingsonderzoek. Ook als de beelden wel van belang zijn voor de opsporing kan in verband met het karakter van de beelden gevraagd worden om de beelden niet of in elk geval zo min mogelijk verder te gebruiken.

Recht van verwijdering

Een in beeld gebrachte persoon kan in beginsel vragen de opgeslagen beelden te verwijderen voordat de zeven dagen termijn verstreken is. Ook kan een in beeld gebrachte persoon vragen beelden van hem uit het opsporingsdossier te verwijderen en te vernietigen. Dit recht op verwijdering kan gaan om de beelden zelf, maar ook om de aanvullende informatie of interpretaties die in bestanden is opgeslagen. Of dit verzoek gehonoreerd kan worden, is afhankelijk van de concrete situatie, met andere woorden van de vraag of de verwijdering van beelden en/of aanvullende gegevens het opsporingsbelang niet in de weg staat.

4.14 Melding van verwerkingen en de reglementsplicht

Gemeenten kunnen op dit moment het cameratoezicht in het kader van de openbare orde zowel onder het wettelijk regime van de WBP als onder het regime van de WPOLR brengen.

Onder de WBP geldt een meldingsplicht van deze vorm van cameratoezicht. Het vrijstellingsbesluit en meer specifiek artikel 38, is niet van toepassing zodra sprake is van cameratoezicht in het kader van de handhaving van de openbare orde. Indien een gemeente een functionaris voor de gegevensbescherming heeft aangesteld en deze bij het CBP is aangemeld, kan de melding ook bij de functionaris voor de gegevensbescherming plaatsvinden. Onder de WPOLR is de regel dat de politie voor deze verwerking van beelden een reglement dient op te stellen.

Na inwerkingtreding van de gewijzigde Gemeentewet geldt het regime van de WPOLR. De beelden worden vastgelegd in een tijdelijk register waarvoor het regime van deze registers geldt. Er is geen reden om voor de opgeslagen beelden geen reglement te maken, omdat geheimhouding niet aan de orde is. Het cameratoezicht moet immers kenbaar gemaakt worden. Een spoedeisend politie onderzoek is eveneens niet aan de orde omdat het gaat om cameratoezicht ten behoeve van de handhaving van de openbare orde.

Onder het regime van de toekomstige Wet politiegegevens zal de reglementsplicht vervallen. Dat ontslaat de overheid en in casu de politie niet van de plicht behoorlijke procedures en afspraken te maken en vast te leggen over de toepassing van dit instrument, de verwerking van de beelden en de eventuele verstrekking. Deze afspraken zullen primair vastgelegd zijn in de verordening van de raad. Een reglement of protocol kan helpen bij het maken van nadere afspraken tussen gemeentebestuur, politie en Openbaar Ministerie. Met de verordening en een protocol of reglement schept de overheid duidelijkheid voor burgers en beslissers. Burgers kunnen aan de hand van het reglement hun rechten effectueren en de gemeenteraad wordt zo in staat gesteld de inzet van dit middel te evalueren.

Bijlage 1

Cameratoezicht in de openbare ruimte

Onderzoek naar de inzet van cameratoezicht in alle Nederlandse gemeenten
College bescherming persoonsgegevens, november 2003

Samenvatting

In veel gemeenten zijn in de afgelopen jaren stappen gezet om met behulp van cameratoezicht overlast en criminaliteit terug te dringen en veiligheidsgevoelens te vergroten. Er bestaat nog geen compleet beeld van de manier waarop gemeenten camera's voor het toezicht in de openbare ruimte inzetten. Het College Bescherming Persoonsgegevens (CBP) voert daarom een onderzoek uit naar de inzet van camera's voor toezicht in de openbare ruimte en de mogelijke inbreuk op de privacy van burgers. Het gaat hierbij om cameratoezicht onder de verantwoordelijkheid van gemeenten.

Het onderzoek is in de zomer van 2003 uitgevoerd met behulp van een schriftelijke vragenlijst, die onder alle gemeenten is uitgezet. Om een zo hoog mogelijke respons te bereiken is er driemaal gerappelleerd (tweemaal schriftelijk en éénmaal telefonisch). De respons is zeer goed.

Cameratoezicht in gemeenten

In bijna een vijfde van de Nederlandse gemeenten vindt cameratoezicht plaats. Grote gemeenten hebben relatief vaker cameratoezicht dan kleinere gemeenten. Overijssel, Limburg en Zeeland hebben relatief veel gemeenten met cameratoezicht, in de noordelijke provincies en Flevoland zijn er juist weinig gemeenten met cameratoezicht.

Het cameratoezicht wordt vooral toegepast in uitgaanscentra, op stations of haltes van het openbaar vervoer en bij openbare gebouwen. In bijna de helft van de gemeenten bestaat het cameratoezicht al meer dan drie jaar. Ruim een kwart van de gemeenten met cameratoezicht heeft plannen om het cameratoezicht uit te gaan breiden. Zes procent van de gemeenten zonder cameratoezicht heeft plannen om het in de toekomst in te voeren.

Van de 93 gemeenten met cameratoezicht geven er 39 aan de cameraregistraties aangemeld te hebben bij het CBP. Als gemeenten de registraties niet gemeld hebben, wordt als voornaamste reden genoemd dat de gemeente niet op de hoogte was dat aanmelding moet plaatsvinden. Een aantal gemeenten gaat de registraties alsnog aanmelden.

Toepassing

Door 19 procent van de gemeenten met cameratoezicht worden de beelden live uitgekeken. In 42 procent van de gemeenten worden camerabeelden uitsluitend achteraf uitgekeken in geval van bijzondere gebeurtenissen. In 36 procent van de gemeenten worden beelden live uitgekeken op vastgestelde tijdstippen en op de overige momenten alleen achteraf in geval van bijzondere gebeurtenissen. In 90 procent van de gemeenten worden beelden opgenomen. Driekwart van de gemeenten bewaart de beelden langer dan 24 uur. Ruim een vijfde van de gemeenten die beelden opnemen, zegt geen bijzondere maatregelen te hebben genomen om de beelden tegen manipuleren te beveiligen. De overige gemeenten doen dat wel, door fysieke beveiliging (84%), digitale beveiliging (44%) of het vastleggen van bevoegdheden (65%).

Meer dan de helft van de gemeenten heeft analoge camera's (52%). Van de gemeenten gebruikt 37 procent digitale camera's en de overige 11 procent gebruikt een combinatie van deze twee soorten camera's.

In bijna alle gemeenten met cameratoezicht (95%) is het toezicht kenbaar voor het publiek. In bijna driekwart van de gemeenten (73%) gebeurt dit doordat camera's duidelijk zichtbaar zijn opgehangen, 68 procent heeft attenderingsborden in het gebied met camera's geplaatst. Meer dan de helft van de gemeenten maakt gebruik van publicaties in lokale bladen. Eén op de acht gemeenten gebruikt posters, folders of flyers.

In tweevijfde van de gemeenten met cameratoezicht is het voor gefilmde personen niet mogelijk om kennis te nemen van beelden en is het evenmin mogelijk om correctie of verwijdering van beelden te vragen.

Van de gemeenten met cameratoezicht werkt 61 procent samen met andere instanties. Bijna altijd is er samenwerking met de politie. In mindere mate is er samenwerking met openbaar vervoerbedrijven, ondernemingen, buurtorganisaties, betaald voetbalorganisaties en met winkeliersverenigingen. De samenwerking bestaat uit periodiek overleg (53%), incidenteel overleg (39%), het uitwisselen en verstrekken van beelden (31%) en gezamenlijke financiering (28%). In bijna tweederde van de gemeenten met cameratoezicht zijn camerabeelden wel eens gebruikt voor opsporing, in bijna éénvijfde van de gemeenten zijn ze gebruikt door observatieteams van de politie.

Er zijn 15 gemeenten waarin beelden voor opsporing worden gebruikt, terwijl deze gemeenten aangeven geen protocol of reglement te hebben waarin procedures en afspraken over het bekijken van beelden zijn vastgelegd. Van deze 15 gemeenten zijn er 7 waarin beelden ook worden uitgewisseld en verstrekt (aan politie, ondernemers, openbaar vervoerbedrijven, ondernemers en betaald voetbalorganisaties) en 4 gemeenten waarin beelden ook worden gebruikt door observatieteams van de politie.

Van de gemeenten met cameratoezicht kan 28 procent een overzicht van de jaarkosten geven. De kosten variëren sterk per gemeente, van 950 euro per jaar tot 250.000 euro per jaar. Hierbij moet opgemerkt worden dat weinig gemeenten de vragen over de kosten van cameratoezicht hebben beantwoord. De kosten van cameratoezicht komen in driekwart van de gemeenten voor rekening van de overheid (gemeenten en/of politie). In ééntiende van de gemeenten dragen particuliere instellingen de kosten. In de overige gemeenten delen overheid en particuliere instellingen de kosten.

In 45 procent van de gemeenten met cameratoezicht is het effect van cameratoezicht gemeten en vastgelegd. In respectievelijk 46 procent en 35 procent van deze gemeenten wordt een afname van vermogensdelicten en geweldsdelicten gerapporteerd. In twee gemeenten heeft zich juist een toename van vermogens- / of geweldsdelicten voorgedaan. Ruim een kwart van de gemeenten meldt een verhoging van het oplossingspercentage. Van de gemeenten geeft 8 procent aan dat cameratoezicht geen van de genoemde effecten heeft.

Besluitvorming

In ruim zeventig procent van de gevallen neemt de gemeente het initiatief tot cameratoezicht. In bijna driekwart van de gemeenten wordt het cameratoezicht ook door gemeenten geïnstalleerd en beheerd.

In 44 procent van de gemeenten is voor de invoering van cameratoezicht overleg geweest met omwonenden en in bijna zestig procent van de gemeenten is vooraf overleg geweest met ondernemers. In bijna alle gevallen hebben de omwonenden en ondernemers ingestemd met de toepassing van cameratoezicht.

De belangrijkste aanleiding om cameratoezicht in te voeren is de wens om veiligheid te bevorderen. Andere belangrijke aanleidingen zijn vandalisme en overlast. Door tweederde van de gemeenten die geen cameratoezicht hebben is als reden genoemd dat er geen aanleiding is voor cameratoezicht. Andere redenen zijn dat cameratoezicht nog nooit aan de orde is geweest, dat de kosten van cameratoezicht te hoog zijn of dat andere maatregelen om de problematiek van openbare orde op te lossen afdoende zijn.

Meer dan de helft van de gemeenten met cameratoezicht heeft openbare orde en toezicht als doel gesteld. Andere doelen, die door ongeveer de helft van de gemeenten zijn gesteld, zijn veiligheid van de burger, het tegengaan van overlast en de beveiliging van eigendommen. Van

de gemeenten met cameratoezicht heeft 86 procent vóór de invoering van cameratoezicht andere maatregelen getroffen om de gestelde doelen te bereiken, meestal surveillance of de toepassing van betere verlichting. De meest genoemde overweging om alsnog cameratoezicht in te voeren is de ernst van de problematiek, gekoppeld aan de beperkte effectiviteit van de eerder genomen maatregelen.

Naleving van vuistregels voor cameratoezicht

Alle gegevens overziend lijkt er geen sprake van onzorgvuldige afwegingen bij de instelling van cameratoezicht; wel lijken verschillende vuistregels uit "In beeld gebracht", het juridisch raamwerk dat door de toenmalige Registratiekamer in 1997 is neergelegd, niet te worden nageleefd. Dit geldt vooral voor de bewaartermijnen, de aanmelding bij het CBP, de regeling voor kennisneming en correcties, de beveiliging van de registratie en de levering aan derden (vooral de politie).

Bijlage 2

Achtergrondstudies en verkenningen

In de serie **Achtergrondstudies en verkenningen** zijn verschenen:

drs. S. Lieon en mr. M. Th. van Munster-Frederiks, **De zieke werknemer en privacy. Regels voor de verwerking van persoonsgegevens van zieke werknemers.** A&V 27; College bescherming persoonsgegevens, Den Haag 2004.

mr. drs. T.F.M. Hooghiemstra, **Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg.** A&V 26; College bescherming persoonsgegevens, Den Haag 2003.

Versmissen, J.A.G. en A.C.M. de Heij, **Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid.** A&V 25; College bescherming persoonsgegevens, Den Haag 2002.

Eijk, M.M.M. van en Helden, W.J. van, **Klant te koop. Privacyregels voor adressenhandel.** A&V 24; College bescherming persoonsgegevens, Den Haag 2001.

Blarkom, G.W. van, **Beveiliging van persoonsgegevens.** A&V 23; Registratiekamer, Den Haag 2001.

Versmissen, J.A.G., **Sleutels van vertrouwen, TTP's, digitale certificaten en privacy.** A&V 22; Registratiekamer, Den Haag 2001.

Terstegge, J.H.J., **Goed werken in netwerken. Regels voor controle op e-mail en internetgebruik van werknemers.** A&V 21; (1e druk; Registratiekamer, Den Haag 2000) 2e druk herzien door drs. S. Lieon, College bescherming persoonsgegevens, Den Haag 2002.

Buitenhuis, R., Campen, N.G.M. van, Helden, W.J. van, Vries, H.H. de, **Bankverzekeraars en privacy. Gegevensverwerking in financiële conglomeraten.** A&V 20; Registratiekamer, Den Haag 2000.

Helden, W.J. van, **Herkomst van de klant. Privacyregels voor etnomarketing.** A&V 19; Registratiekamer, Den Haag 2000.

Wishaw, R.W.A. **De gewaardeerde klant. Privacyregels voor credit scoring.** A&V 18; Registratiekamer, Den Haag 2000.

Artz, M. en Eijk, M.M.M. van, **Klant in het web. Privacywaarborgen voor internettoegang.** A&V 17; Registratiekamer, Den Haag 2000.

Zeeuw, J. de. **Informatieverstrekking. Ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving.** A&V 16; Registratiekamer, Den Haag 2000.

Hes, R., Borking, J.J. en Hooghiemstra, T.F.M. **At face value. On biometrical identification and privacy.** A&V 15; Registratiekamer, Den Haag 1999.

Artz, M.J.T., **Koning Klant. Het gebruik van klantgegevens voor marketingdoeleinden.** A&V 14; Registratiekamer, Den Haag 1999.

Borking, J.J., e.a., **Intelligent software agents and privacy.** A&V 13; Registratiekamer, Den Haag 1999.

Hooghiemstra, T.F.M., **Privacy & Managed care.** A&V 12; Registratiekamer, Den Haag 1998.

Hes, R. en J. Borking, **Privacy-enhancing technologies: the path to anonymity**. A&V 11 revised edition; Registratiekamer, Den Haag 1998.

Almelo, L. van, e.a., **Gouden bergen van gegevens. Over datawarehousing, datamining en privacy**. A&V 10; Registratiekamer, Den Haag 1998.

Zandee, C., **Doelbewust volgen. Privacyaspecten van cliëntvolgsystemen en andere vormen van gegevensuitwisseling**. A&V 9; Registratiekamer, Den Haag 1998.

Zeeuw, J. de, **Informatiegaring door de fiscus. Privacybescherming bij derdenonderzoeken**. A&V 8; Registratiekamer, Den Haag 1998.

Hulsman, B.J.P. en P.C. Ippel, **Gegeven: de Genen. Morele en juridische aspecten van het gebruik van genetische gegevens**. A&V 7; Registratiekamer, Den Haag 1996.

Gardeniers, H.J.M., **Chipcards en privacy. Regels voor een nieuw kaartspel**. A&V 6, Registratiekamer, Den Haag 1995.

Rossum, H. van e.a., **Privacy-enhancing technologies: the path to anonymity, volume I and II**. A&V 5; Registratiekamer, Den Haag 1995.

Rommelse, A.F., **Zwarte lijsten. Belangen en effecten van waarschuwingssystemen**. A&V 4; Registratiekamer, Rijswijk 1995.

Rommelse, A.F., **Ziekteverzuim en privacy. Controle door de werkgever en verplichtingen van de werknemer**. A&V 3; Registratiekamer, Rijswijk 1995.

Casteren, J.P.M. van, **Bevolkingsgegevens: Wie mag ze hebben? Verstrekking van gegevens uit de GBA aan vrije derden**. A&V 2; Registratiekamer, Rijswijk 1995 (niet meer beschikbaar).

Hulsman, B.J.P. en Ippel, P.C., **Personeelsinformatiesystemen - de Wet persoonsregistraties toegepast**. A&V 1; Registratiekamer, Rijswijk 1994 (niet meer beschikbaar).

Vrijwel alle publicaties van het CBP kunt u inzien en/of downloaden van de website www.cbpweb.nl. Voor het toezenden van meerdere gedrukte publicaties worden kosten in rekening gebracht.

COLLEGE BESCHERMING PERSOONSGEGEVENS

Prins Clauslaan 20
Postbus 93374
2509 AJ Den Haag

TELEFOON 070 381 13 00

FAX 070 381 13 01

E-MAIL info@cbpweb.nl

INTERNET www.cbpweb.nl