

Whitepaper

Wet- en regelgeving camerabewaking



© Federatie Veilig Nederland 2020

Alle rechten voorbehouden. Alle auteursrechten en databankrechten ten aanzien van deze uitgave worden uitdrukkelijk voorbehouden. Deze rechten berusten bij Federatie Veilig Nederland.

Behoudens de in of krachtens de Auteurswet gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, kan voor de aanwezigheid van eventuele (druk)fouten en onvolledigheden niet worden ingestaan en aanvaarden de auteur(s), redacteur(en) en uitgever deswege geen aansprakelijkheid voor de gevolgen van eventueel voorkomende fouten en onvolledigheden en gebruik van de informatie. De informatie is bedoeld voor algemeen gebruik: er kunnen geen rechten aan worden ontleend.

Federatie Veilig Nederland
Postbus 840 | 2700 AV Zoetermeer
T 079 203 50 15
E info@federatieveilignederland.nl
I www.federatieveilignederland.nl



Samenvatting

In deze whitepaper geeft Federatie Veilig Nederland een overzicht van de wet- en regelgeving op het gebied van camerabewaking. De tekst is geschreven voor private partijen die bewakingscamera's willen inzetten. Het doel is duidelijkheid bieden over het toegestane gebruik van camerasystemen, waardoor iedereen een goede afweging kan maken bij de inzet daarvan. De wetgeving is helaas niet in een paar regels samen te vatten: er moet altijd een afweging worden gemaakt tussen het belang van de eigenaar van de camera's versus het recht op privacy van de personen die in beeld komen. De verantwoordelijke voor de camera's moet die afweging maken en legt deze bij voorkeur schriftelijk vast. Dat biedt nooit de garantie dat de verwerking is toegestaan, maar biedt wel de meeste zekerheid om problemen achteraf te voorkomen.



Inleiding

Deze whitepaper geeft een overzicht van relevante Nederlandse wet- en regelgeving op het gebied van camerabewaking.

De belangrijkste wetten en regels

Privacy

Privacy is een ruim begrip: het omvat niet alleen de bescherming van persoonsgegevens, maar ook bescherming van het eigen lichaam en de eigen woning, het familie- en gezinsleven en het recht op vertrouwelijke communicatie per brief, telefoon of e-mail. Daarnaast gaat privacy over het recht om zelf te bepalen wie welke informatie over ons krijgt. Een praktische invulling van het begrip privacy is het recht om met rust te worden gelaten. Dit recht op privacy volgt uit artikel 10 van de Nederlandse Grondwet en uit internationale verdragen, zoals artikel 8 van het Europees Verdrag voor de Rechten van de Mens en het VN-verdrag voor Burgerlijke en Politieke rechten. Elke camera levert een inperking op van de privacy van de personen die in beeld zijn. Die inperking is alleen toegestaan als het noodzakelijk is voor een gerechtvaardigd doel. Wanneer dat het geval is kan nooit in het algemeen worden gezegd. Er is dus geen antwoord op de vraag: “Wat mag wel en wat mag niet?” Het antwoord hangt af van een afweging tussen het privacybelang van de gefilmde personen en het veiligheidsbelang van de verantwoordelijke voor de camera. Die afweging kan alleen maar per afzonderlijk cameraproject worden gemaakt. En het is uiteindelijk altijd aan de rechter om per concreet geval te beoordelen of de afweging goed is gemaakt en of de camera dus wettelijk is toegestaan. Er zijn, kortom, geen standaardoplossingen en elke verantwoordelijke zal zich in de wet moeten verdiepen.

Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) gaat niet alleen over camera's, maar over elke verwerking van persoonsgegevens. Deze wet beschrijft onder welke voorwaarden verwerking van persoonsgegevens is toegestaan. Camerabeelden zijn persoonsgegevens als ze informatie bevatten die tot een individu kan worden herleid. Dat zijn niet alleen gezichten, maar alle gegevens die naar een individu kunnen leiden, dus ook een kenteken. Onder verwerking vallen bijna alle handelingen met persoonsgegevens: opslaan, maar ook verstrekken, gebruiken, doorzenden, verspreiden en vernietigen van persoonsgegevens. Twee belangrijke eisen in deze wet zijn die van kenbaarheid en noodzakelijkheid. Voor de meeste private bewakingscamera's is de Wet bescherming persoonsgegevens het belangrijkste wettelijke kader: de Wet bescherming persoonsgegevens bevat namelijk ook de belangrijkste eisen die volgen uit de algemene privacywetgeving. Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor de doelen waarvoor ze zijn verzameld.



Voor iedereen die kennisneemt van persoonsgegevens geldt een geheimhoudingsplicht. Voor de verwerking van bijzondere persoonsgegevens gelden strengere regels. Bijzondere gegevens betreffen iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging. De Autoriteit Persoonsgegevens houdt toezicht op naleving van de Wet bescherming persoonsgegevens en publiceerde in januari 2016 beleidsregels voor cameratoezicht.

Wet politiegegevens

Als beelden van bewakingscamera's worden verwerkt door de politie, geldt voor die beelden niet de Wet bescherming persoonsgegevens, maar de Wet politiegegevens (Wpg). Politiegegevens zijn persoonsgegevens die voor de uitoefening van de politietaak worden verwerkt, dus voor handhaving van de rechtsorde en voor hulpverlening (art. 3, Politiewet 2012). Alleen ambtenaren van de politie en militairen van de Koninklijke marechaussee, mogen politiegegevens verwerken. De bewaartermijn van politiegegevens is minimaal een jaar en maximaal vijf jaar. Politiegegevens zijn een bijzondere vorm van persoonsgegevens: de Autoriteit Persoonsgegevens houdt ook toezicht op naleving van de Wet politiegegevens.

Gemeentewet

Artikel 151c van de Gemeentewet gaat over gemeentelijk cameratoezicht voor handhaving van de openbare orde. Daarin staat onder welke voorwaarden een gemeente dit soort camera's voor dit doel mag plaatsen. Deze wet is niet relevant voor private partijen die bewakingscamera's inzetten, omdat die camera's een ander doel dienen: bewaking en niet openbare orde. In sommige gemeenten wordt deze wet echter van toepassing verklaard op alle camera's op openbare plaatsen. Dat is het gevolg van een foutieve interpretatie van de Gemeentewet. Niet de plek waar een camera hangt bepaalt welke wet geldt, maar het doel van de camera is bepalend. Als beveiliging het doel van de camera is (en niet handhaven van de openbare orde), dan is de Gemeentewet niet relevant voor die camera.

Interpretatie wet- en regelgeving

Wanneer is camerabewaking toegestaan en wanneer niet? Die vraag zal nooit in het algemeen kunnen worden beantwoord. De wet- en regelgeving voor bescherming van de persoonlijke levenssfeer werkt namelijk anders. Het gaat altijd om de afweging van verschillende belangen en daar zijn geen algemene uitspraken over mogelijk. In de wet staat vooral wat *niet* is toegestaan en aan welke voorwaarden u moet voldoen als u toch een camera wilt ophangen. Hieronder worden de belangrijkste wetten en regels geïnterpreteerd. De vraag of een specifieke camera is toegestaan kan uiteindelijk alleen door de rechter per geval worden beoordeeld. Dat betekent dat u zich dus ook zelf in de wet- en regelgeving moet verdiepen om een zorgvuldige afweging te kunnen maken.



Algemene privacywetgeving

Privacy

Een praktische omschrijving van privacy is 'het recht om met rust te worden gelaten'. Dit is een grondrecht dat alleen mag worden geschonden voor een wettig en noodzakelijk doel. Wie in beeld wordt gebracht door een camera wordt niet met rust gelaten. Een camera levert dus altijd een schending van de privacy op.

- Camera's leveren per definitie een inperking van de privacy op. Dat is alleen gerechtvaardigd als er een legitiem en belangrijk doel mee gediend wordt.

Heimelijk cameratoezicht

Heimelijk en wederrechtelijk cameratoezicht is verboden in het Wetboek van Strafrecht, zowel in openbare ruimtes als in woningen en andere niet openbare ruimtes. Alleen in uitzonderlijke gevallen en alleen als het doel van het cameratoezicht kan worden bereikt door de camera's geheim te houden, kan dit soms zijn toegestaan. Stelselmatige observatie met behulp van heimelijke camera's is toegestaan aan de politie en opsporingsinstanties als ze voldoen aan alle eisen, onder andere die in het Wetboek van Strafvordering. In vrijwel alle andere gevallen moet de aanwezigheid van de camera duidelijk kenbaar zijn: door informatiestickers, informatieborden of op zijn minst door goed zichtbare camera's te plaatsen.

- Heimelijk cameratoezicht is verboden in het Wetboek van Strafrecht: artikelen 139f en 441b.

Aangebrachte camera's

Het verbod op heimelijk cameratoezicht geldt alleen voor aangebrachte camera's. Wat onder 'aangebracht' moet worden verstaan is niet geheel duidelijk. Een vuistregel is dat een aangebrachte camera continu dezelfde plek in beeld brengt. Dat geldt voor vast gemonteerde camera's in een pand, aan een muur of op een paal. Maar ook voor een 'losse' webcam op de vensterbank die altijd dezelfde plek in beeld brengt. Een camera die in de hand wordt gehouden brengt niet continu dezelfde plek in beeld en wordt dus niet als een aangebrachte camera gezien. Dat geldt ook voor smartphones, bodycams, drones en camera's op het dashboard. Dat soort 'niet-aangebrachte' camera's hoeven dus niet vooraf te worden aangekondigd. Wel kunnen er nog altijd andere wetten dan het Wetboek van Strafrecht zijn die het gebruik van dit soort beelden aan banden leggen, zoals het portretrecht of wet- en regelgeving op het gebied van strafvordering. Daarnaast kan het met het oog op de mogelijke preventieve of de-escalerende werking van uw camera verstandig zijn ook het gebruik van niet-aangebrachte camera's duidelijk kenbaar te maken.

- De kenbaarheidseis geldt alleen voor aangebrachte camera's, niet voor camera's in de hand, smartphones, bodycams, drones of dashcams.



Openbare plaats

Filmen op openbare plaatsen is in principe toegestaan, mits de aanwezigheid van de camera's duidelijk wordt aangegeven. Iedereen weet immers dat je op een openbare plaats kan worden gezien door anderen. Daardoor is het minder logisch daar een beroep te doen op je privacy dan op een niet-openbare plaats. In besloten ruimtes zijn de regels strenger: daar moet een zwaarwegend belang zijn om camerabeelden te maken.

- Hoe openbaarder de plek, hoe kleiner de schending van de privacy.

Noodzakelijkheid

Camera's moeten niet alleen een legitiem doel dienen, maar ook noodzakelijk zijn om dat doel te bereiken. De eis van noodzakelijkheid geldt voor alle vormen van cameratoezicht en camerabewaking, omdat deze eis volgt uit de Grondwet en het Europees Verdrag voor de Rechten van de Mens (EVRM). Veel andere wetgeving die van belang is voor cameratoezicht, zoals de Wet bescherming persoonsgegevens, bouwt daarop door. Maar wanneer is een camera noodzakelijk? Moet het dan gaan om ernstige criminaliteit of overlast? Nee, met de ernst van het probleem heeft noodzakelijkheid niets te maken. De noodzakelijkheid hangt af van de proportionaliteit (niet verder gaan dan nodig voor het doel) en subsidiariteit (minder ingrijpende middelen leveren niet het gewenste resultaat op). Elke andere uitleg van noodzakelijkheid is subjectief en dus onbruikbaar.

- Cameratoezicht moet noodzakelijk en dus proportioneel en subsidiair zijn: Grondwet artikel 10 en EVRM artikel 8.

Per geval beoordelen

De vraag of het gerechtvaardigd is een bewakingscamera op te hangen, hangt af van de afweging tussen twee belangen. Ten eerste is er het belang van de eigenaar van de camera die bijvoorbeeld een gebouw, zijn eigendommen of zijn werknemers wil beveiligen. Ten tweede is er het algemene privacybelang van iedereen die wordt gefilmd: iedereen heeft er recht op zoveel mogelijk met rust te worden gelaten. Hoe de afweging tussen deze twee belangen uitvalt hangt van meerdere factoren af: de aard van het gebied (openbaar of besloten), de aard en omvang van de problemen, het aantal voorbijgangers en bewoners in het gebied, de beveiliging van de opgeslagen beelden en nog minstens twintig andere factoren. Daarom kan nooit in het algemeen worden gezegd of een bepaalde camera wel of niet legitiem is. Het vergt een belangenafweging per geval.

- Of de verwerking van persoonsgegevens is toegestaan hangt af van de afweging tussen het recht op privacy van gefilmde personen en het belang van de camera-eigenaar bij het vergroten van de veiligheid.



Privacy aan de 'achterkant'

De mate waarin een camera de privacy van voorbijgangers schendt hangt niet zozeer af van de camera, maar van de beelden die worden gemaakt en wat daar vervolgens mee gebeurt. De inperking van de privacy van gefilmde personen is minder groot als er minder camera's worden opgehangen – dat is logisch. Maar de inperking wordt ook minder groot als de camerabeelden korte tijd worden opgeslagen en zeer goed worden beveiligd. Of als de beelden alleen maar worden gebruikt door de politie, bijvoorbeeld na aangifte van een strafbaar feit. Kortom: u kunt aan de voorkant van het camerasysteem de schending van de privacy inperken door minder camera's op te hangen, maar ook aan de 'achterkant' door heel zorgvuldig om te gaan met de persoonsgegevens.

- Privacyschending kan worden ingeperkt door de verwerking van persoonsgegevens aan de 'achterkant' van de camera zo beperkt mogelijk te houden.

Grondslagen voor camerabewaking

Expliciete grondslag

Cameratoezicht en het gebruik van camerabeelden staat zoals gezegd altijd op gespannen voet met het grondrecht op bescherming van de persoonlijke levenssfeer. Een voorwaarde om gebruik te mogen maken van cameratoezicht of de gegevens die daarmee verzameld worden, is een legitieme grondslag. Soms is er een expliciete wettelijke grondslag, zoals in de Gemeentewet of in het Wetboek van Strafvordering. Maar deze twee wetten kunnen alleen een grondslag bieden voor camera's van een gemeente of een opsporingsinstantie, niet voor die van private partijen.

- Specifieke grondslagen voor cameratoezicht zijn te vinden in de Gemeentewet en het Wetboek van Strafvordering (WvSv). Deze gelden echter alleen voor de overheid en niet voor particulieren of ondernemingen.

Impliciete grondslag

Impliciete grondslagen voor cameratoezicht zijn te vinden in de Algemene wet bestuursrecht (Awb), de Wegenverkeerswet 1994 (WVW), de Wet werk en bijstand (WWB) en de Algemene wet inzake rijksbelastingen (Awr). De Politiewet 2012 biedt ook een impliciete grondslag voor cameratoezicht, maar alleen door de politie en alleen als de inperking van de privacy gering is. Deze wetten gaan allemaal niet expliciet over cameratoezicht. En ze gelden wederom allemaal niet voor private partijen.

- De meeste grondslagen voor camera's zijn niet expliciet, maar impliciet.



Doelbinding

Doelbinding is een cruciaal element bij de beoordeling of een verwerking legitiem is. Dat is vastgelegd in artikel 9 van de Wet bescherming persoonsgegevens en artikel 6 van de Europese privacyrichtlijn. Camerabeelden mogen alleen worden gebruikt voor een legitiem doel én voor een doel dat in logisch en direct verband staat met het originele doel waarvoor de camera is opgehangen. Het is dus niet toegestaan camerabeelden die zijn bedoeld om inbraken tegen te gaan, ook te gebruiken om werknemers in de gaten te houden.

- Camerabeelden mogen alleen worden gebruikt voor een legitiem doel en voor het oorspronkelijke doel.

Persoonsgegevens

Beelden zijn belangrijker dan de camera

Er zal zoals gezegd nooit een eenduidig antwoord worden gegeven op de simpele vraag: “Mag ik hier een camera ophangen?” Dat komt vooral door het feit dat er nauwelijks wet- en regelgeving is die expliciet over camera’s gaat: er zijn bijna geen wetten waar het woord ‘camera’ in voorkomt. De camera zelf is juridisch nauwelijks interessant. Wel belangrijk is wat er gebeurt met de beelden die door de camera worden gemaakt. Wie kunnen de beelden zien? Worden de beelden opgenomen? Hoe lang worden ze bewaard? Hoe wordt oneigenlijk gebruik van de persoonsgegevens voorkomen? Juridisch zijn beelden belangrijker dan de camera.

- Wet- en regelgeving specifiek over camera’s is er nauwelijks: juridisch is de camera veel minder van belang dan de beelden die met die camera worden gemaakt.

Verwerking van persoonsgegevens

Camerabeelden die informatie bevatten die tot een individu kan worden herleid vallen onder de wetgeving voor persoonsgegevens. Dat geldt dus uiteraard voor gezichten van personen, maar bijvoorbeeld ook voor kentekens. De eigenaar van bijna elke camera verwerkt dus persoonsgegevens. De verantwoordelijke voor de verwerking van dat soort gegevens moet voldoen aan de Wet bescherming persoonsgegevens. Onder het begrip ‘verwerking’ vallen alle handelingen met persoonsgegevens: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens.

- Als camerabeelden informatie over personen bevatten moet de verwerking voldoen aan de Wet bescherming persoonsgegevens.



Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens houdt toezicht op naleving van de Wet bescherming persoonsgegevens. De Autoriteit Persoonsgegevens kan boetes opleggen voor overtredingen van de wet of voor datalekken. De maximale boete bedraagt €820.000. Op de website van de Autoriteit Persoonsgegevens staan beleidsregels voor cameratoezicht om eigenaren van camera's te helpen bij het voldoen aan de wet- en regelgeving.

- De Autoriteit Persoonsgegevens houdt toezicht op naleving van de Wet bescherming persoonsgegevens.

Onderzoek Autoriteit Persoonsgegevens

Net als de rechters doet de Autoriteit Persoonsgegevens geen algemene uitspraken over cameratoezicht. Elk camerasysteem – of eigenlijk: elke verwerking van persoonsgegevens – wordt afzonderlijk beoordeeld. Het aantal onderzoeken dat is uitgevoerd is zeer beperkt. Een interessant onderzoek is uitgevoerd in 2008. Dat ging over de camera's op een bedrijventerrein in Vianen die op de openbare weg waren gericht. Uit dat onderzoek bleek dat de camera's waren toegestaan, a) omdat er geen openbare orde probleem was en b) omdat de gemeente betrokken was bij het cameraproject. Daarnaast waren c) de camera's noodzakelijk voor het doel en d) waren de opgenomen beelden alleen toegankelijk voor de politie. Verder werden nog zo'n vijftien aspecten beoordeeld wat leidde tot goedkeuring van de verwerking. Maar een algemene uitspraak was het niet. In 2009 schreef het toenmalige College bescherming persoonsgegevens (de oude naam van de Autoriteit Persoonsgegevens) dat de inzet van private bewakingscamera's op de openbare weg nooit op voorhand kan worden goed- of afgekeurd 'omdat het gaat om een kwestie die per geval moet worden bekeken' (Cbp, 2009, Cameratoezicht, z2009-00259).

- Ook de Autoriteit Persoonsgegevens zal nooit een algemene uitspraak doen over de toelaatbaarheid van camerabewaking: dat moet per geval worden bekeken.

Vrijstelling van melding

Elke verwerking van persoonsgegevens moet worden gemeld bij de Autoriteit Persoonsgegevens, tenzij de verwerking in aanmerking komt voor vrijstelling van melding. Dit is geregeld in het Vrijstellingsbesluit. Om te bepalen of een verwerking voor vrijstelling van melding in aanmerking komt, kunt u de Handreiking Vrijstellingsbesluit Wet bescherming persoonsgegevens gebruiken (zie de link hieronder).

- Als een verwerking van persoonsgegevens aan de voorwaarden in het Vrijstellingsbesluit voldoet hoeft deze niet te worden gemeld.



Camerabeelden aan politie verstrekken

Private partijen die over opgenomen camerabeelden beschikken die relevant kunnen zijn voor de politie kunnen die beelden op twee manieren aan de politie verstrekken: spontaan en ongevraagd of na een vordering. Uit de Wet bescherming persoonsgegevens (artikel 43, lid b) volgt dat eigenaren van bewakingscamera's uit eigener beweging en vrijwillig camerabeelden aan politie en justitie mogen verstrekken als dat noodzakelijk is in het belang van de voorkoming, opsporing en vervolging van strafbare feiten. De verstrekking moet wel echt vrijwillig en uit eigener beweging plaatsvinden: een opsporingsambtenaar mag dus niet vragen of iemand op vrijwillige basis beeldmateriaal wil verstrekken. Als de beelden niet spontaan en ongevraagd ter beschikking worden gesteld is sprake van een verzoek tot afgifte van beelden. Daar dient altijd een vordering van de officier van justitie of rechter-commissaris aan ten grondslag te liggen (Wetboek van Strafvordering artikel 126nd). Een vordering is in juridische zin de meest betrouwbare werkwijze. Bij dringende noodzaak kan de vordering mondeling worden gegeven, maar dan moet binnen drie dagen alsnog een schriftelijke vordering worden verstrekt.

- Camerabeelden mogen vrijwillig en uit eigener beweging beschikbaar worden gesteld aan de politie. Als politie of justitie het initiatief nemen moet er een vordering aan ten grondslag liggen.

Jurisprudentie

Geen algemene uitspraken

Uiteindelijk kan alleen een rechter in een concreet geval bepalen of een camera is toegestaan. Daarom is jurisprudentie van belang om de algemene wet- en regelgeving te interpreteren. Er zijn niet veel rechtszaken gevoerd waar camerabeelden expliciet werden beoordeeld op rechtmatigheid. En die beoordelingen leveren geen conclusies op over de rechtmatigheid van bewakingscamera's in het algemeen, maar slechts over die concrete gevallen. Dat betekent dat u nooit zeker weet of uw camerasysteem is toegestaan totdat een rechter er een oordeel over velt. De jurisprudentie die er wel is levert belangrijke informatie op over specifieke voorbeelden, maar u kunt er dus geen rechten aan ontlenen voor uw eigen camerasysteem.

- Jurisprudentie levert geen uitspraken op over de rechtmatigheid van cameratoezicht in het algemeen, maar alleen over het gebruik van specifieke beelden in een specifieke casus.

Doelbinding breed uitgelegd

De eis van doelbinding is niet absoluut: rechters kunnen per geval een uitzondering maken. Dat blijkt uit een arrest uit 2004 in een zaak tegen een persoon die op straat graffiti aanbracht. Daarbij werd hij gefilmd door een bewakingscamera die was



bevestigd aan een politiebureau. Die camera was niet bedoeld voor gemeentelijk cameratoezicht op straat en daarom betoogde de advocaat van de verdachte dat de beelden niet mochten worden gebruikt als bewijsmateriaal. Maar de Hoge Raad oordeelde anders: er was geen sprake van een inbreuk op de persoonlijke levenssfeer van de verdachte omdat de feiten zich op straat afspeelden. Op straat kan niemand verwachten 'onbevangen zichzelf te zijn' en daarom mochten de beelden worden gebruikt als bewijsmateriaal (ECLI:NL:HR:2004:AL8449). Het feit dat het cameratoezicht zelf op een ontoereikende wettelijke basis steunde, betekende dus niet automatisch dat er een te grote inbreuk op de persoonlijke levenssfeer van de verdachte werd gemaakt.

- De Hoge Raad heeft in een specifiek geval besloten dat camerabeelden toelaatbaar waren als bewijsmateriaal, ook al ging het gebruik verder dan de oorspronkelijke doelstelling.

Heimelijk gemaakte beelden soms acceptabel als bewijs

Uit de jurisprudentie blijkt dat heimelijk gemaakte camerabeelden in bepaalde gevallen wel degelijk worden gebruikt als bewijsmateriaal in een strafzaak. Dat blijkt bijvoorbeeld uit een arrest van de Hoge Raad uit 2003 over een diefstal door een werknemer van een bedrijf (ECLI:NL:HR:2003:AF4321). Een detectivebureau maakte camerabeelden van de werknemer waarop de diefstal te zien was. Toen de werknemer de beelden zag legde hij een bekennende verklaring af. Volgens zijn advocaat waren de camerabeelden niet legaal gemaakt en mocht de bekentenis dus niet worden gebruikt als bewijsmateriaal. De Hoge Raad beoordeelde deze casus en keek of er sprake was van 'stelselmatige observatie'. In dat geval zou een machtiging van de officier van justitie vereist zijn geweest. Maar omdat de camerabeelden geen volledig beeld gaven van het privéleven van de verdachte was de observatie niet stelselmatig en mochten de beelden worden gebruikt.

- Beelden kunnen soms worden gebruikt als bewijsmateriaal, ondanks het feit dat ze met heimelijke camera's zijn gemaakt.

Heimelijke camera's niet toegestaan

Er is ook jurisprudentie waaruit blijkt dat heimelijke camera's in principe niet zijn toegestaan. Een werkgever installeerde verborgen camera's op de werkplek omdat er geld uit de kassa verdween en gereedschap uit de werkplaats. Toen werknemers de camera's ontdekten vroegen ze de directie om opheldering. Drie werknemers werden ontslagen omdat ze bezwaar maakten tegen de camera's. De kantonrechter concludeerde dat de camera's van de werkgever aan vrijwel geen enkele wettelijke eis voldeden en dat de ontslagen werknemers daarom recht hadden op een drie keer zo hoge ontslagvergoeding als onder normale omstandigheden.

- Het is alleen onder uitzonderlijke omstandigheden toegestaan verborgen camera's in te zetten.



Eisen aan camera's op de werkplek

De Rechtbank Noord Nederland heeft een casus beoordeeld van verborgen camera's op de werkplek (ECLI:NL:RBNNE:2016:713). De werkgever mag cameratoezicht op de werkvloer houden, mits wordt voldaan aan de Wet bescherming persoonsgegevens, de Wet op de ondernemingsraden, het Wetboek van Strafrecht (de artikelen 139f en 441b) en de algemene normstelling van goed werkgeverschap (artikel 7:611 Burgerlijk Wetboek).

Dat betekent:

- De werkgever moet een gerechtvaardigd belang hebben voor het cameratoezicht
- Het cameratoezicht moet noodzakelijk zijn, bijvoorbeeld voor het stoppen van schadetoebrengend handelen, maar alleen onder de voorwaarde dat het bedrijfsbelang is afgewogen tegen het privacybelang van medewerkers en klanten
- De inbreuk op de privacy moet zo klein mogelijk zijn
- De beelden mogen niet langer worden bewaard dan noodzakelijk is (met als uitgangspunt niet langer dan vier weken, tenzij daar een goede reden voor is)
- De ondernemingsraad heeft instemmingsrecht over een besluit om personeelsvolgsystemen (waaronder camera's) te plaatsen
- De aanwezigheid van camera's dient op duidelijke wijze kenbaar te zijn gemaakt

Voor verborgen camera's geldt bovendien:

- Verborgen camera's mogen alleen worden ingezet als uiterste redmiddel en alleen tijdelijk
- De werknemers moeten vooraf op duidelijke wijze in kennis zijn gesteld van de mogelijkheid dat een verborgen camera zou kunnen worden gebruikt
- De werkgever moet de werknemers achteraf informeren over het gebruik van de verborgen camera's
- De werkgever moet het verborgen cameratoezicht vooraf melden bij de Autoriteit Persoonsgegevens en een voorafgaand onderzoek aanvragen. De Autoriteit toetst of het gebruik van de verborgen camera voldoet aan de wettelijke vereisten.

Nieuwe ontwikkelingen

Convenanten

Vaak worden convenanten opgesteld om de uitwisseling van camerabeelden tussen verschillende instanties mogelijk te maken. Bijvoorbeeld voor de doorgifte van beelden van private bewakingscamera's aan de politie. Een convenant kan echter nooit iets mogelijk maken wat bij wet verboden is. De wet- en regelgeving omtrent privacy, persoonsgegevens en politiegegevens blijft onverminderd van kracht – wat er ook in een convenant staat. Een convenant is eigenlijk alleen maar geschikt om de intentie tot samenwerking vast te leggen en afspraken te maken over wederzijdse verplichtingen in die samenwerking.



- Een convenant is wel geschikt voor het vastleggen van de intentie tot samenwerking, maar kan iets wat bij wet verboden is niet alsnog mogelijk maken.

Wetsvoorstellen

Op het moment van schrijven zijn diverse wetsvoorstellen over cameratoezicht in behandeling.

- Wetsvoorstel flexibel gemeentelijk cameratoezicht

Artikel 151c Gemeentewet wordt aangepast door het woord 'vaste' te schrappen. Hierdoor wordt het mogelijk camera's eenvoudiger te verplaatsen als het probleem zich verplaatst. Hierdoor worden ook rijdende, varende en vliegende camera's (drones) mogelijk. De Tweede Kamer is in 2014 akkoord gegaan en het wetsvoorstel ligt nu bij de Eerste Kamer.

- Wetsvoorstel publicatie door particulieren van camerabeelden van diefstal of vernieling

Dit wetsvoorstel verandert de Wet bescherming persoonsgegevens en maakt het mogelijk dat burgers en bedrijven camerabeelden van misdrijven mogen publiceren ter ondersteuning van de opsporing, mits het gaat om diefstal of vernieling. Daarnaast gelden nog vier andere eisen, onder andere dat er ook aangifte van het incident moet zijn gedaan en de beelden aan de politie moeten zijn verstrekt. De internetconsultatie is in 2015 afgerond en het wetsvoorstel gaat naar de Tweede Kamer.

- Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie

Dit wetsvoorstel stelt de politie in staat automatisch kentekens te scannen en de gegevens te verwerken. Tot op heden mochten alleen de 'hits' worden bewaard, maar als dit wetsvoorstel wordt goedgekeurd kunnen ook de 'no hits' worden bewaard. Het wetsvoorstel is 2013 ingediend en is in behandeling bij de Tweede Kamer.



Vragen en antwoorden

Kan ik 100% zekerheid krijgen dat mijn camera's aan de wet voldoen?

Nee, die garantie heeft u alleen als u geen camera's ophangt. Zodra u een camera gebruikt, is er altijd een risico dat uw afweging van de noodzakelijkheid door een rechter anders zal worden geïnterpreteerd.

Welk risico loop ik als ik camera's ophang die niet aan de wet voldoen?

U kunt een boete krijgen van de Autoriteit Persoonsgegevens als u niet aan de Wet bescherming persoonsgegevens voldoet. Belanghebbenden (zoals bewoners en werknemers) kunnen bezwaar tegen uw camera's maken en dat kan uiteindelijk tot een rechtszaak leiden. Ook loopt u het risico dat opgenomen beelden onbruikbaar zijn als bewijsmateriaal omdat ze onrechtmatig zijn verkregen.

Ben ik verplicht een cameraprotocol op te stellen?

Nee, maar het is wel sterk aan te raden. U moet als verantwoordelijke namelijk de afweging maken of de camera's noodzakelijk zijn. Die afweging kunt u het beste schriftelijk vastleggen, zodat u kunt aantonen dat u al het nodige hebt gedaan om aan de wet te voldoen. Een cameraprotocol helpt ook bij de zorgvuldige omgang met de gegevens.

Mag ik werknemers filmen met camera's?

Ja, maar alleen als het noodzakelijk is voor een gerechtvaardigd doel en als u de camera's duidelijk kenbaar maakt. De noodzakelijkheid hangt af van de proportionaliteit (de camera's moeten in verhouding staan tot het doel en niet verder gaan dan het doel) en subsidiariteit (er zijn geen lichtere instrumenten waarmee u hetzelfde doel kunt bereiken).

Mag ik werknemers filmen met verborgen camera's?

Nee, alleen bij hoge uitzondering. In elk geval moet de ondernemingsraad er vooraf mee akkoord gaan en alle werknemers moeten vooraf op de hoogte worden gebracht dat er mogelijk verborgen camera's worden ingezet. En u moet vooraf toestemming vragen aan de Autoriteit Persoonsgegevens.

Mag ik de straat filmen?

Ja, maar alleen als het voor uw doel noodzakelijk is en als uw verantwoordelijkheid zich uitstrekt tot het deel van de openbare weg dat u in beeld wilt brengen. Als u kunt aantonen dat de camera's op straat noodzakelijk zijn (dus wederom: proportioneel en subsidiair) én als u zeer zorgvuldig met de gegevens omgaat, kan het toegestaan zijn. Let op: alleen een gemeente kan camera's inzetten voor handhaving van de openbare orde; private partijen mogen alleen camera's inzetten voor beveiliging.

Hoe lang mag ik de beelden bewaren?

Zo lang als noodzakelijk is voor het doel. Meestal wordt een bewaartermijn van maximaal 28 dagen gekozen, omdat de verwerking dan in aanmerking kan komen voor vrijstelling van melding bij de Autoriteit Persoonsgegevens.



Mag ik camera's die bedrijfsprocessen filmen ook gebruiken voor criminaliteitsbestrijding?

Nee, in principe niet. Camerabeelden mogen namelijk alleen worden gebruikt voor het oorspronkelijke doel (doelbinding). Als u toevallig een incident in beeld hebt gebracht met een camera, mogen de beelden wel worden gebruikt voor opsporing en vervolging.

Mag ik opgenomen camerabeelden aan de politie geven?

Ja, maar alleen als u dit ongevraagd en vrijwillig doet. Als de politie u eerst vraagt of u beelden hebt van een incident en u ze daarna verstrekt, is de verstrekking niet meer spontaan en loopt u het risico dat de beelden niet bruikbaar zijn als bewijsmateriaal.

Moet ik beelden aan de politie geven als ze daarom vragen?

Ja, maar alleen als er een vordering aan ten grondslag ligt.

Moet ik de politie laten weten waar mijn camera's hangen?

Nee, maar het kan wel wenselijk zijn. Neem contact op met de lokale politie en wijs ze op het politieproject 'Camera in Beeld'.

Wat is Live View en hoe kom ik er aan?

Live View is de koppeling tussen 'poortwachters' (bijvoorbeeld alle Particuliere Alarm Centrales, maar ook andere toezichtcentrales) en de 112-meldkamers van de politie. Als u wilt dat uw beelden in noodgevallen rechtstreeks naar de meldkamer van de politie kunnen worden doorgestuurd, moet er dus een videoverbinding zijn tussen uw camerasysteem en een poortwachter.



Bronnen

Literatuur

Autoriteit Persoonsgegevens (2016), Beleidsregels cameratoezicht, Den Haag.
N. Baas en C. Cozijn (1996), Toezicht met camera's; toepassing, effectiviteit en juridische aspecten, WODC/Den Haag.

College bescherming persoonsgegevens (2009), Definitieve bevindingen inzake het ambtshalve onderzoek naar cameratoezicht op het bedrijventerrein Vianen, 8 oktober 2009.

S. Flight (2013), Cameratoezicht in Nederland; een schets van het Nederlandse cameralandchap, WODC/Den Haag.

S. Flight (2015a), 'Cameratoezicht', in: J. Schilder, A. van den Berg en J. van der Grinten (red.), Hoofdstukken openbare-orderecht, Ars Aequi/Nijmegen.

S. Flight (2015b), Camerabewaking op bedrijventerreinen; het juridisch kader, Interpolis/Tilburg.

G. Homburg en S. Dekkers (2003), Cameratoezicht in de openbare ruimte. Den Haag: College Bescherming Persoonsgegevens.

B. Meijer (2000), Cameratoezicht in het publieke domein in EU-landen, WODC/Den Haag.

A. Smeets (2004), Camera's in het publieke domein; Privacynormen voor cameratoezicht op de openbare orde, Den Haag: College Bescherming Persoonsgegevens.

Websites

www.overheid.nl (overheidsinformatie > cameratoezicht)

www.politie.nl (thema's > cameratoezicht)

www.autoriteitpersoonsgegevens.nl (onderwerpen > cameratoezicht)

<https://autoriteitpersoonsgegevens.nl/nl/melden/handreiking-vrijstellingsbesluit-wbp>

www.hetccv.nl (themasites > cameratoezicht)

www.cameratoezicht.nl (dossiers > wetgeving)

www.iusmentis.com (lijst a-z > cameratoezicht)

Meer weten?

Brancheorganisatie Federatie Veilig Nederland is met 180 lidbedrijven de autoriteit op het gebied van technische (brand)beveiliging in Nederland. Met haar expertise levert Federatie Veilig Nederland al meer dan 50 jaar een bijdrage aan een veiligere samenleving. Deze whitepaper is opgesteld als een bron van informatie ten einde de veiligheid te verhogen en daarnaast extra meerwaarde voor bedrijven en instellingen te creëren.

Colofon

De White paper 'Wet- en regelgeving camerabewaking' is vervaardigd in opdracht van Federatie Veilig Nederland.