

CAMERABEWAKING ALS PRIVATE BEVEILIGINGSMAATREGEL

Situatieschets, toepassingsgebied en krachtlijnen die volgen uit de Wet van 8 december 1992, zoals gewijzigd door de Wet van 11 december 1998 (NWVP)

Dieter VERHAEGHE*

1. Inleiding: private camerabewaking en privacyreglementering

Private beveiliging kan zeer algemeen worden omschreven als het domein waar private actoren¹ maatregelen nemen teneinde de veiligheid van personen en goederen te waarborgen.

Dit reeds van oudsher gekende fenomeen evolueerde sterk onder invloed van de toenemende behoefte aan beveiligingsmaatregelen en de groeiende beveiligingsindustrie die nieuwe mogelijkheden verschafte zoals de camerabewaking.

De overheid diende herhaaldelijk te reageren door reglementering van, controle op of inkapseling van nieuwe (kiem)vormen van private beveiliging. Bij wijze van rechtshistorisch voorbeeld kan hier worden verwezen naar de Wet op de private militias² die het gebruik van geweld door private actoren aan banden wilde leggen. Meer recent kan worden verwezen naar de Wet op de bewakingsondernemingen,³ de Wet op het Politieambt,⁴ de Omzendbrief betreffende de burgerwachtinitiatieven⁵ waar het fenomeen van burgerwachten een halt werd toegeroepen ten voordele van meer gereguleerde vormen van buurttoezicht zoals de stadswachten, en de voetbalwet⁶ die in haar artikelen 12 tot en met 17 een strikte taak- en bevoegdheidsomschrijving van voetbalstewards voorziet.

* Het artikel verkondigt het persoonlijke standpunt van de auteur, met dank aan Paul De Hert, Jan Dhont en Paul Blontrock voor hun opmerkingen en nazicht.

1. Met private actoren worden bedoeld: burgers of ondernemingen zoals handelaars, bewakingsondernemingen, werkgevers, de vereniging van mede-eigenaars en/of de syndicus, organisatoren van massamanifestaties en dergelijke meer.

2. Wet van 29 juli 1934 waarbij de private militias verboden worden, *B.S.* 6-7 augustus 1934.

3. Wet van 10 april 1990 op de bewakingsondernemingen, de beveiligingsondernemingen en de interne bewakingsdiensten, *B.S.* 29 mei 1990.

4. Wet van 5 augustus 1992 op het politieambt, *B.S.* 22 december 1992.

5. Omzendbrief van 13 oktober 1995 betreffende de burgerwachtinitiatieven, *B.S.* 14 november 1995, 31337-31339.

6. Wet van 21 december 1998 betreffende de veiligheid bij voetbalwedstrijden, *B.S.* 3 februari 1999, 3312-3318 (hierna Voetbalwet).

Deze continue overheidsinitiatieven hadden niet alleen tot doel de bevoegdheden van de private actoren te beperken ten opzichte van de overheidsbevoegdheden; ook is een duidelijke toenemende bezorgdheid merkbaar op het gebied van de bescherming van de fundamentele rechten en vrijheden van de burgers,⁷ waaronder vooral de bescherming van de persoonlijke levenssfeer.

Het gebruik van een concreet privaat camerabewakingssysteem kan naargelang de toepassing of context worden bestudeerd in het licht van diverse rechtsbronnen die de persoonlijke levenssfeer naar Belgisch recht beschermen.

Zonder volledig te willen zijn kan worden verwezen naar belangrijke reglementaire bronnen zoals artikel 8 van het Europees Verdrag voor de Bescherming van de Rechten van de Mens, artikel 22 van de Grondwet, het Verdrag nr. 108,⁸ de Wet van 8 december 1992⁹ (hierna WVP) en de recente wijziging hiervan (hierna NWP), artikel 10 van de Auteurswet,¹⁰ de artikelen 35 en 39 van de Wet op het Politieambt, artikel 1 §§ 3 en 4 van de wet op de bewakingsondernemingen, artikel 5 van de Wet op de privé-detectives¹¹ en wat de arbeidsplaats betreft de C.A.O. nr. 68.¹²

Daarnaast kan ook worden verwezen naar de toepassing van de principes uit voormelde reglementaire bronnen op private camerabewakingssystemen in de rechtspraak en de Adviezen van de CBPL terzake, waarvan hierna enkele belangrijke voorbeelden zullen worden aangehaald.¹³ De recente publicaties via internet zijn hierbij vermeldenswaardig, zoals het initiatief van de CBPL om al haar jaarverslagen en adviezen toegankelijk te maken via haar website 'www.privacy.fgov.be'.

Hoewel voorlopig geen sprake is van een bijzondere Belgische 'camerawet', werden recent door diverse instanties verschillende initiatieven genomen ter reglementering van zowel private als publieke camerabewaking.

7. Zie in dit kader de studies die de Belgische overheid over het fenomeen van private justitie heeft uitgevoerd, waarvan schriftelijke neerslag in o.m. L. VAN OUTHRIE, T. DECORTE en W. VAN LAETHEM (eds.), *Private bewaking en opsporing en de grondrechten van de mens*, Brussel, Politeia, 1995 en de recente Parlementaire Vraag nr. 1863 van dhr. Rik Daems aan de minister van Binnenlandse Zaken over de modaliteiten van camerabewaking d.d. 27 januari 1999, Handelingen Kamer.

8. Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, opgemaakt te Straatsburg op 28 januari 1981, goedgekeurd bij Wet van 17 juni 1991, B.S. 30 december 1993.

9. Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, B.S. 18 maart 1993, zoals gewijzigd door de Wet van 11 december 1998 tot omzetting van de Richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, B.S. 3 februari 1999. De inwerkingtreding van deze wijziging wordt ten vroegste verwacht rond eind 2000-begin 2001.

10. Wet van 30 juni 1994 betreffende het auteursrecht en de naburige rechten, B.S. 27 juli 1994.

11. Wet van 19 juli 1991 tot regeling van het beroep van privé-detective, B.S. 2 oktober 1991, *err.* 11 februari 1993.

12. Zie het Koninklijk Besluit 20 september 1998 waarbij algemeen verbindend wordt verklaard de collectieve arbeidsovereenkomst nr. 68 van 16 juni 1998 gesloten in de Nationale Arbeidsraad, betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats, B.S. 2 oktober 1998. Deze C.A.O. wordt o.m. besproken in B. MAGREZ en H. VANOVERSCHelde, *L.c.*, Dossiers, Souriez, vous êtes filmés... La vidéosurveillance en Belgique, *Droit et Nouvelles Technologies*, <http://www.droit-technologie.org/>, 16 maart 1999, 13-17.

13. Voor een algemene inleiding in de materie van het recht op afbeelding: zie M. ISGOUR en B. VINCOTTE, *Le Droit à l'image*, Brussel, Larcier, 1998.

Zo werd in juni 1998 door de sociale partners de reeds aangehaalde C.A.O. nr. 68 afgesloten die het gebruik van private camerabewaking door werkgevers regelt.¹⁴ De juridische hiërarchie der normen zoals ingeschreven in de C.A.O.-wet¹⁵ maakt evenwel dat de principes van de WVP, indien toepasselijk, voorrang zullen genieten op deze van de C.A.O. nr. 68.

In maart 1999 werden vervolgens twee wetsvoorstellen¹⁶ ingediend, waarvan een wetsvoorstel werd hernomen in september 1999.¹⁷ Opmerkelijk is alvast dat beide voorstellen een belangrijke verantwoordelijkheid voorzien voor de plaatselijke gemeentelijke overheid, waarbij een legalisering van private initiatieven niet wordt beoogd, doch wel de bewakingssystemen van diverse overheden of overheidsdiensten zoals steden en gemeenten, politiediensten,... De Commissie voor de bescherming van de persoonlijke levenssfeer (hierna CBPL) heeft zich niet uitgesproken over deze recente voorstellen.

De minister van Binnenlandse Zaken aanvaardde ten slotte het principe van een camerawet,¹⁸ en nam ook op basis van de voetbalwet initiatief m.b.t. camerabewaking. Zo trad op 5 oktober 1999 een Koninklijk Besluit¹⁹ in werking dat de gevallen en de wijze bepaalt waarin organisatoren van bepaalde voetbalwedstrijden worden verplicht²⁰ om bewakingscamera's in een voetbalstadion te plaatsen.

Al deze initiatieven hebben met elkaar gemeen dat ze telkens expliciet of impliciet verwijzen naar enkele basisprincipes, en aldus expliciet of impliciet de WVP als overkoepelende kaderwet erkennen. De reeds vermelde vaststelling dat

14. De toepassing van camera's in de arbeidscontext wordt uitgebreid behandeld in volgend werk: F. HENDRICKX, *Privacy en arbeidsrecht*, Die Keure, 1999, 160-173 (nrs. 262-283).

15. Voor de relatie tussen deze C.A.O. en de Wet van 8 december 1992 dient men rekening te houden met het onderscheiden toepassingsgebied en de hiërarchie der normen zoals geregeld door artikel 51 van de Wet van 5 december 1968 betreffende de collectieve arbeidsovereenkomsten en de paritaire comités.

16. Zie het Wetsvoorstel betreffende het gebruik van camera's, ingediend door de heer Louis Vanvelthoven, 18 maart 1999, *Gedr. St. Kamer*, G.Z., 1998-1999, 2079/1, 1-12.; het Wetsvoorstel betreffende de plaatsing van bewakings- en beveiligingscamera's op de openbare weg, ingediend door de heer Jo Van Overbergh, 25 maart 1999, *Gedr. St. Kamer*, G.Z., 1998-1999, 2101/1.

17. Wetsvoorstel betreffende de plaatsing van bewakings- en beveiligingscamera's op de openbare weg, ingediend door de heer Daniel Vanpoucke, 23 september 1999, *Gedr. St. Kamer*, B.Z., 1999, 104/1.

18. In het kader van een antwoord op een parlementaire vraag stelde de minister van Binnenlandse Zaken reeds: 'Alleszins ben ik overtuigd van de noodzaak van wetgevend werk dienaangaande. Doen wij dat niet, dan voorspel ik dat die initiatieven zeer snel door particulieren of organisaties die zich in de grijze zone tussen overheid en particuliere sector bevinden, zullen worden overgenomen, wat meteen de vraag zal doen rijzen of ze niet de persoonlijke levenssfeer schenden. (...) Tenslotte ga ik graag in op de suggestie om hieraan in commissie een debat te wijden dat uitmondt in wetgevend werk. Mijns inziens is dit een onderwerp voor de gemeenschappelijke commissies voor de Justitie en de Binnenlandse Zaken.' Zie de Vraag. nr. 1863 van dhr. Rik Daems aan de minister van Binnenlandse Zaken omtrent de modaliteiten van camerabewaking d.d. 27 januari 1999, *Handelingen van de Commissie voor Binnenlandse Zaken, Algemene Zaken en het openbaar ambt*. Deze vraag is te raadplegen op volgend internetadres: <http://www.dekamer.be/commissions/acts/hc726n.htm>, kwam ook aan bod in de pers: FVG, 'Van den Bossche en parlement werken aan wet camerabewaking', *De Standaard*, 28 januari 1999; X, 'Vers un 'oui' aux caméras de rue?', *La Libre Belgique*, 28 januari 1999.

19. Koninklijk Besluit van 12 september 1999 betreffende de installatie en de werking van bewakingscamera's in de voetbalstadions, *B.S.* 5 oktober 1999.

20. Artikel 10, 6° van de Voetbalwet.

er geen alomvattende Belgische reglementering bestaat van de camerabewaking, wordt dus wel gecorrigeerd door de ruime toepasselijkheid van fundamentele basisprincipes die we in een wettelijke regeling met ruim toepassingsgebied terugvinden.

Deze bijdrage heeft dan ook tot doel het gebruik van een camerasysteem door private actoren voor bewakings- en beveiligingsdoeleinden te bestuderen in het licht van zowel de WVP als de NWVP.²¹ Camerasystemen die door de overheid voor overheidsdoeleinden (b.v. verkeerscontrole,²² ...) of door particulieren voor andere private doeleinden (journalistiek, artistiek of privé-gebruik, studie van consumentengedrag, ...) worden aangewend, zullen verder niet worden behandeld.

2. Is de WVP toepasselijk op alle private camerabewakingssystemen?

De WVP en NWVP beschermen niet het gehele veld van de persoonlijke levenssfeer of de privacy; enkel de camerasystemen die een verwerking van persoonsgegevens²³ vormen, worden beschermd. Belangrijk is dus dat de bescherming van de persoonlijke levenssfeer of privacy niet samenvalt met de bescherming van een onderdeel van de privacy, met name de dataprotectie, die enkel verwerkingen van persoonsgegevens viseert.

TOEPASSELIJKHEID VAN DE WVP EN HET ADVIES 14/1995

Uit de parlementaire voorbereiding van de WVP²⁴ volgde reeds dat beelden van identificeerbare personen als persoonsgegevens kunnen worden beschouwd, ongeacht het type gegevensdrager zoals de gebruikelijke analoge videoband of nieuwe digitale opslagmedia zoals bijvoorbeeld compact-disc, harddisk of an-

21. Zie voor een diepgaander bespreking van de wijziging van de WVP TH. LEONARD en Y. POULLET 'La protection des données à caractère personnel en pleine (r)évolution. La Loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995', *J.T.* 22 mai 1999, nr. 5928, 377-395.

22. Voor een rapport betreffende het gebruik van onbemande verkeerscamera's door de overheid: zie W. VAN DER SYPT *Onbemande verkeerscamera's, Leefbaarheid in de gemeente, Technische Sectie Rijkswacht* d.d. 4 augustus 1999. Dit rapport kan worden geconsulteerd op volgend internetadres: <http://www.dma.be/p/mrm/info/onbemand.htm>.

23. Zie de definitie in artikel 1 §§ 1 en 2 WVP.

24. Zie het verslag namens de Commissie voor Justitie uitgebracht door de heer VANDENBERGHE op 27 oktober 1992, *Gedr. Sr. Senaat, B.Z.*, 1991-92, nr. 445/2, 57: 'Tot slot bevestigt de Minister, als antwoord op de vraag of gegevens zoals foto's of filmbeelden tot de werkingssfeer van het ontwerp behoren, een interpretatie die gisteren werd gegeven: het gaat ongetwijfeld om gegevens die betrekking hebben op geïdentificeerde of identificeerbare natuurlijke personen. Hetzelfde geldt voor vingerafdrukken of genetische gegevens. Het soort van gegevensdrager speelt hier geen rol; deze maakt het alleen mogelijk een onderscheid te maken tussen het soort verwerking (geautomatiseerd of manueel).'

dere opslagmedia. De rechtsleer²⁵ sloot hierbij aan door herhaaldelijk te stellen dat de WVP toepasselijk kan zijn op video-opnames van natuurlijke personen.

De CBPL²⁶ heeft herhaaldelijk de WVP toepasselijk verklaard op systemen van private en publieke camerabewaking.²⁷ Een eerste belangrijke toelichting werd hier gegeven in het advies nr. 14/95 van 14 juni 1995. De CBPL stelde hier: *'Er is sprake van een verwerking van beelden in de zin van de Wet Verwerking Persoonsgegevens zodra de beelden niet alleen worden opgenomen en onmiddellijk weergegeven, maar ook worden bewaard. Observatiesystemen waarbij de beelden niet worden bewaard, vallen niet onder het toepassingsgebied van de Wet Verwerking Persoonsgegevens.'* De WVP was derhalve volgens de CBPL niet van toepassing op camera-systemen waarbij geen sprake is van een verwerking van persoonsgegevens of – indien men deze begrippen op camera-gebruik toepast – van opname en bewaring van beelden van identificeerbare personen, bijvoorbeeld in de situaties waar een camera enkel als het verlengde van het menselijke oog wordt ingezet. Een effectieve continue opname was evenwel niet vereist; een systeem met een opnamemogelijkheid kan derhalve onder de WVP vallen. Deze laatste stelling was sinds enkele jaren de traditionele opvatting die steunt op het klassieke juridisch begrip van verwerking van persoonsgegevens volgens de WVP.

EVOLUTIE NAAR EEN RUIMERE TOEPASSELIGHEID ONDER DE NWVP EN DE NIEUWE ADVIEZEN VAN DE CBPL 34/1999 EN 3/2000

Voornoemde traditionele opvatting die een beperkte toepasselijkheid van de WVP inhield, bleek echter aan herziening toe te zijn. Hierbij speelden niet alleen technologische overwegingen een rol, doch ook de nieuwe bepalingen van de NWVP.

De werkelijke betekenis van het criterium 'bewaring' bleek reeds relatief in het licht van de technologische evolutie. Digitale camera-systemen zoals DVD-RAM bieden tal van nieuwe mogelijkheden zoals het werken met een digitale

25. Zie M.H. BOULANGER, C. DE TERWANGNE en TH. LEONARD 'La protection de la vie privée à l'égard des traitements de données à caractère personnel – La loi du 8 décembre 1992', *J.T.* 1993, nr. 5675, 371; H. BRULIN, 'Défense et illustration de la loi sur la protection de la vie privée appliquée à la vidéosurveillance', *La Revue Politique* 1996, nr. 2, 33-64; B. MAGREZ en H. VANOVERSCHELDE, *l.c.*, 4.

26. Zie voor een korte opsomming van de mogelijke rol van de Commissie: B. MAGREZ en H. VANOVERSCHELDE, *l.c.*, 5 en 6.

27. Advies CBPL nr. 10/94 d.d. 22 maart 1994 betreffende het Wetsontwerp tot wijziging van artikel 62 van de Wetten betreffende de politie over het wegverkeer gecoördineerd op 16 maart 1968, en houdende expliciete erkenning van onbemande toestellen voor de controle van verkeersovertradingen; Advies CBPL nr. 14/95 d.d. 7 juni 1995 betreffende de toepasselijkheid van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens op beeldopnamen, en de gevolgen ervan en Advies CBPL nr. 17/99 d.d. 10 mei 1999 over het ontwerp van Koninklijk Besluit betreffende de installatie en de werking van bewakingscamera's in stadions, de oprichting van een bestand der beelden en de modaliteiten waaraan dit bestand dient te voldoen.

geheugenbuffer die weergeeft wat gebeurde voor een alarm het videosysteem activeerde.²⁸

De recente verruiming van het begrip 'verwerking' door artikel 2 van de Wet van 11 december 1998²⁹ (nieuwe art. 1 § 2 NWVP) had daarnaast een ruimere toepassingsmogelijkheid tot gevolg ten aanzien van systemen van private camerabewaking.³⁰ Onder 'verwerking' wordt volgens de NWVP verstaan 'elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens'.

De klassieke vereisten om de WVP toepasselijk te verklaren bij cumulatie van de criteria opname en bewaring van videobeelden gelden dan ook niet langer onder de NWVP; elke afzonderlijke bewerking zoals het opnemen, het bewaren, het gebruiken, ... van videobeelden kan onder de bescherming van deze dataprotectieregeling vallen. De CBPL erkende deze ruimere toepasselijkheid van de NWVP inmiddels in haar recente adviezen met nummers 34/99 van 13 december 1999 en 03/2000 van 10 januari 2000.

Wat indien men ondanks de verruiming van het begrip verwerking toch buiten het toepassingsveld van de NWVP zou vallen? Hiervoor werd reeds gewezen op het verschil tussen privacy en dataprotectie. Indien geen sprake zou zijn van een verwerking van persoonsgegevens, kan men dan ook zich beroepen op de reeds aangehaalde alternatieve regelingen tot bescherming van de persoonlijke levenssfeer.

Onder deze alternatieven is vooral artikel 8 EVRM van belang. De Europese Commissie voor de Rechten van de Mens³¹ hanteerde in een recente zaak van camerabewaking een strikte benadering van het begrip persoonlijke levenssfeer. Uit diverse hoeken wordt evenwel sinds enige tijd duidelijk kritiek geformuleerd ten aanzien van een dergelijk strikt interpreteren van de persoonlijke levenssfeer. Er is de kritiek uit rechtstheoretische hoek van o.m. F. RIGAUX, P. DE HERT en S. GUTWIRTH³² waarbij men stelt dat de enge interpretaties van het begrip persoonlijke levenssfeer de vrijheidsgedachte miskent die eigen is aan een ruimer pri-

28. Zie overigens gelijkaardige toepassingen in de audiobranche (MP3-spelers) en de fotografie (digitale fototoestellen met geheugenmodule).

29. Wet van 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, *B.S.* 3 februari 1999.

30. TH. LEONARD en Y. POULLET, *l.c.*, 378 (randnummer 7).

31. E.C.R.M., 14 januari 1998, P.H. en V.Z.W. Liga voor de rechten van de mens t/België, *J.T.* 1998, 67-68; *A.J.T.* 1997-1998, 501-504.

32. F. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles-Paris, Bruylant, 1990, (zie vooral n° 684). Voor de kritiek op het arrest van de E.C.R.M. 14 januari 1998 en het aldaar gehanteerde begrip van privé-leven: zie de noot bij dit arrest door P. DE HERT en O. DE SCHUTTER, 'Straatsburg, videosurveillance en het vorderingsrecht van verenigingen', *A.J.T.* 1997-1998, 504-511 en P. DE HERT, *Privacy en het gebruik van visuele technieken door burger en politie*, Brussel, Politeia, 1998.

vacyconcept. Auteurs zoals P. DE HERT en S. GUTWIRTH³³ passen dit toe op camera's waar zij spreken van een subtiele en vaak onbewuste gedragsbeïnvloeding die wordt veroorzaakt door de observatie. Opmerkelijk is dat ook de pers het begrip privacy spontaan als een ruimer begrip beschouwt, zoals blijkt uit de commotie die enige tijd geleden ontstond naar aanleiding van de aankondiging van installatie van camera's in het straatbeeld.³⁴

3. Wie is verantwoordelijk voor de naleving van de NWVP?

De volgende casus is in de praktijk niet denkbeeldig: een werkgever wenst voor veiligheidsdoeleinden op de arbeidsplaats camera's in te zetten. Hij doet voor de technische uitvoering van deze veiligheidsmaatregel beroep op een erkende bewakingsonderneming, en het camerasysteem wordt geïnstalleerd door een gespecialiseerde aannemer. De vraag stelt zich dan ook onmiddellijk: wie draagt de verantwoordelijkheid voor het naleven van de onderscheiden verplichtingen van de NWVP?

De voornaamste verplichtingen worden aan de 'verantwoordelijke voor de verwerking' opgelegd. Volgens artikel 1 § 4 NWVP gaat het hier om de natuurlijke persoon of de rechtspersoon, de feitelijke vereniging of het openbaar bestuur die alleen of samen met anderen het doel (of de doeleinden) en de middelen voor de verwerking van persoonsgegevens bepaalt.³⁵ In de praktijk zal er meestal van kunnen worden uitgegaan dat diegene die in concreto de verantwoordelijkheid of de beslissing neemt m.b.t. het gebruik van een camerasysteem voor doeleinden van private beveiliging, zal kunnen worden beschouwd als de verantwoordelijke die de hierna uiteengezette verplichtingen dient na te leven of minstens zorg dient te dragen voor het feit dat deze verplichtingen worden nageleefd.³⁶

Toch beschouwt de NWVP niet steeds enkel de verantwoordelijke voor de verwerking als voornaamste normadressant; van derden kan immers ook worden verwacht dat zij niet meewerken aan een inbreuk op de NWVP.³⁷ De NWVP

33. P. DE HERT, *Privacy en het gebruik van visuele technieken* (reeds aangehaald), 15; S. GUTWIRTH, *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Amsterdam, Cramwinkel, 1998 (Werkdocument Rathenau Instituut, w. 64).

34. Zie o.m. S. DE FOER, 'Heel Nederland eist camera's rond cafés. Dood onschuldige tienermeisjes vraagt om harde aanpak', *Het Nieuwsblad*, 16 januari 1999; R. FALTER, 'Bewakingscamera's zijn niet meer weg te denken. Het privé-gebruik is de tendens van de jongste jaren', *Het Nieuwsblad*, 22 januari 1999; B. VANDORMAEL, 'Camera's in Leuven: ja/nee?', *Knack*, 27 januari 1999, nr. 4, 10; P. STAUDT, 'Standpunt Tobback over camera's zorgt voor polemiek in Leuven', *Gazet Van Antwerpen*, 30-31 januari 1999; P. DE BACKER, 'SP'ers leggen camera-idee van Tobback aan banden', *De Standaard*, 12 maart 1999; P. MARTENS, 'SP wil heimelijk filmen met strenge boetes aanpakken', *Het Nieuwsblad*, 12 maart 1999.

35. Merk het verschil op met de oorspronkelijke versie van de WVP waar geen sprake was van de cumulatie van de criteria door de vermelding van 'of' in plaats van 'en': 'houder van het bestand', gedefinieerd als 'de natuurlijke persoon of de rechtspersoon of de feitelijke vereniging die bevoegd is om te beslissen over het doel van de verwerking of over de soorten gegevens die erin moeten voorkomen.'; TH. LEONARD en Y. POULLET, *l.c.*, 379 (randnummer 6).

36. Zie artikel 4 § 2 m.b.t. de toepassing van het finaliteitsprincipe.

37. De strafrechtelijke afdwingbaarheid kan ook ten opzichte van derden gelden gezien de figuur van strafbare deelneming (artikelen 66 tot en met 69 Strafwetboek).

omschrijft de derde op negatieve wijze in artikel 1 § 6 als ‘*de natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of het openbaar bestuur, niet zijnde de betrokkene, noch de verantwoordelijke voor de verwerking, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verantwoordelijke of de verwerker gemachtigd zijn om de gegevens te verwerken.*’ Naargelang de situatie zouden bijvoorbeeld de politiediensten kunnen worden beschouwd als hetzij derden, of anderzijds als ontvangers³⁸ in de zin van de NWVP.

In ons voorbeeld zal dus vaak de werkgever verantwoordelijk zijn voor de naleving van bijzondere verplichtingen zoals informatieplicht, de plicht tot beveiliging van de beeldopnames en de aangifteplicht. Gezien de overtredingen van de verplichtingen van de (N)WVP strafbaar werden gesteld en de strafrechter zich niet steeds dient gebonden te achten door juridische constructies uit bijvoorbeeld het burgerlijk recht,³⁹ kan worden aangenomen dat van de definitie van ‘voor de verwerking verantwoordelijke’ niet kan worden afgeweken door het voorzien van een contractuele clausule in een overeenkomst tussen een werkgever en een bewakingsonderneming. Het afschuiven van verantwoordelijkheid door contractuele technieken is derhalve niet mogelijk.

Wel dient hier onmiddellijk te worden opgemerkt dat de NWVP in de artikelen 9 §§ 1 en 2 en 17 in de mogelijkheid voorziet om bij het vervullen van de informatieplicht en de aangifteplicht een vertegenwoordiger aan te duiden van de verantwoordelijke voor de verwerking. Gezien de WVP nergens verbiedt dat deze vertegenwoordiger een externe instantie zou zijn, zou derhalve in ons voorbeeld kunnen worden aangenomen dat de bewakingsonderneming als vertegenwoordiger van de werkgever de informatieplicht en aangifteplicht mee zou kunnen vervullen. Een taakverdeling op deze twee punten lijkt derhalve wel mogelijk, in tegenstelling tot de hiervoor aangehaalde juridische constructie die een overdracht van de uiteindelijke verantwoordelijkheid voor de verwerking zou beogen.

4. Enkele vuistregels die volgen uit de toepassing van de WVP en NWVP

Kan men als maatregel van private beveiliging een camerasysteem gebruiken zonder de (N)WVP te schenden en zo ja, welke voorwaarden moet men hierbij naleven? Samengevat kunnen uit de (N)WVP drie vuistregels worden afgeleid die een verantwoordelijke dient na te leven bij het gebruik van een camerasysteem dat onder de WVP valt.

38. Merk het verschil met het begrip ontvanger, gedefinieerd in artikel 1 § 7 WVP als de natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of het openbaar bestuur, aan wie de gegevens worden meegedeeld, ongeacht of het al dan niet een derde betreft; administratieve of gerechtelijke instanties aan wie gegevens kunnen worden meegedeeld in het kader van een bijzondere onderzoeksprocedure worden evenwel niet beschouwd als ontvangers.

39. Voor meer uitleg i.v.m. deze zogenaamde ‘autonomie van het strafrecht’: zie L. DUPONT en R. VERSTRAETEN, *Handboek Belgisch Strafrecht*, Leuven, Acco, 1989, 73-77 (nrs. 40-49).

EERSTE VUISTREGEL: GEBRUIK VIDEOPNAMES NIET ALS ENIG BEWIJSMIDDEL

Beleggingsadviseurs raden bij een risicovolle belegging hun klanten vaak aan het risico te spreiden. Het vermijden om alle eieren in dezelfde mand te leggen is een volkswijsheid die installateurs van bewakingssystemen ook aan hun klanten zouden kunnen adviseren.

Het investeren in een camerabewakingssysteem lijkt op het eerste zicht een kordaat en efficiënt middel om veiligheidsproblemen aan te pakken; het lijkt op een belegging waarvoor spectaculaire resultaten worden voorgeschoteld. De euforische houding ten aanzien van dit wondermiddel zou voor de verantwoordelijke wel eens een risicovolle belegging kunnen blijken te zijn, wanneer het vergaarde bewijsmateriaal niet alleen voor de strafrechter op grond van de niet-naleving van de (N)WVP niet zou worden weerhouden, maar ook doordat de verantwoordelijke zelf zou kunnen worden beschuldigd of veroordeeld op grond van niet-naleving van de (N)WVP.⁴⁰

Deze risico's vloeien voort uit strikte verplichtingen van de WVP, zoals de informatieplicht (art. 4 en 9 WVP en 9 NWVP), de plicht tot naleving van het finaliteitsprincipe (art. 5 WVP en 4 NWVP) en het principiële verbod van de verwerking van de zogenaamde 'gevoelige' gegevens. Deze problematiek zal hierna nog verder worden besproken.

TWEEDE VUISTREGEL: ZORG VOOR VOLDOENDE OPENBAARHEID OF KENNISGEVING OMTRENT HET CAMERABEWAKINGSSYSTEEM (HET TRANSPARANTIEBEGINSEL)

Het zogenaamde 'transparantieprincipe' bleek reeds uit de parlementaire voorbereiding van de WVP. In het Verslag Merckx-Van Goey⁴¹ lezen we immers herhaaldelijk dat bewust de klemtoon wordt gelegd op doorzichtigheid of het recht van de particulier om van het bestaan en de modaliteiten van een gegevensverwerking op de hoogte te worden gebracht. Dit principe werd door de wetgever zowel uitgewerkt rechtstreeks naar de betrokkenen toe via de informatieplicht, als onrechtstreeks (via de CBPL) door middel van de aangifteplicht en opname van de aangifte in het openbaar register van de CBPL.

40. Zo veroordeelde de Correctionele Rechtbank te Dendermonde op 22 juni 1999 een persoon die 'ter beveiliging van zijn woning' een camerasysteem had opgesteld met volledig uitzicht op de openbare weg en diverse private woningen. De rechter hechtte hier belang aan het feit dat de buurtbewoners door betrokkene 24 uur op 24 konden worden gevolgd. Betrokkene werd veroordeeld wegens diverse inbreuken op de WVP (niet naleven van de informatieplicht en de aangifteplicht, disproportionaliteit). De rechter verwees hier expliciet naar het voormelde advies 14/95 van de Commissie. De opgelegde sanctie betrof een totale geldsom van meer dan 125.000 frank, waaronder 10.000 frank bij wijze van schadevergoeding aan acht burgerlijke partijen. Zie Corr. Dendermonde (16° Kamer), 22 juni 1999, A.R. 53.71.1463/96/3, onuitg.

41. Verslag namens de Commissie voor Justitie uitgebracht door mevr. Merckx-Van Goey op 2 juli 1992, *Gedr. St. Kamer*, B.Z., 1991-1992, nr. 413/12, 6 en 10.

Naar de betrokkenen toe legt de NWVP in haar artikel 9 §§ 1 en 2 de verantwoordelijke voor de verwerking of zijn vertegenwoordiger de plicht op om toelichting te verschaffen rond de modaliteiten van de verwerking, dit uiterlijk op het ogenblik van het verkrijgen of de eerste mededeling van de gegevens. De 'private' verantwoordelijke kan zich overigens niet beroepen op de vrijstellingen op de informatieplicht die worden voorzien in de artikelen 4 § 1 en 11 WVP of 3 § 5 NWVP voor opdrachten van bestuurlijke of gerechtelijke politie, gezien deze enkel geldt voor verwerkingen die worden beheerd door openbare overheden met het oog op de uitvoering van hun opdrachten van bestuurlijke of gerechtelijke politie.

De informatieplicht heeft inhoudelijk vooral betrekking op de naam en het adres van de verantwoordelijke of diens vertegenwoordiger en de doeleinden van de verwerking. De WVP voegt hieraan toe dat in functie van een eerlijke verwerking van persoonsgegevens desgevallend bijkomende informatie zal moeten worden verstrekt zoals het bestaan van de rechten van toegang en verbetering van de betrokkenen en de ontvangers of categorieën ontvangers van de gegevens (bijvoorbeeld politiediensten).

Waar de (N)WVP wel de inhoud van de informatieplicht verduidelijkt, regelt zij evenwel niet onmiddellijk de wijze waarop de betrokkenen dienen te worden geïnformeerd. Uit het eerlijkheidsprincipe (art. 4 § 1 1° NWVP) kan evenwel worden afgeleid dat een duidelijke informatievorm moet worden gekozen, zoals een informatiebord waardoor de betrokkene uiterlijk op het moment dat hij wordt gefilmd, geïnformeerd wordt.

Aangifteplicht

Volgens artikel 17 (N)WVP dient de verantwoordelijke voor de verwerking of zijn vertegenwoordiger de verwerking aan te geven⁴², teneinde de CBPL toe te laten een externe controle te voeren op de verwerking.⁴³ Van belang is hierbij te benadrukken dat de aangifte van een camerasysteem bij de CBPL neerkomt op het voldoen aan een wettelijke plicht die de verantwoordelijke helemaal niet ontlast van de naleving van zijn overige plichten. Een aangifte bij de CBPL houdt dus geen loutere formaliteit tot goedkeuring van een camerasysteem in en houdt evenmin in dat een vergunning wordt afgeleverd voor het camerasysteem.

Vallen alle camerasystemen die volgens de CBPL onder de (N)WVP vallen ook onder de aangifteplicht? Volgens artikel 17 geldt de aangifteplicht slechts indien een camerasysteem kan worden beschouwd als een gehele of een gedeeltelijke geautomatiseerde verwerking. Dergelijke geautomatiseerde verwerking betreft elke op zichzelf staande bewerking of elk geheel van dergelijke bewer-

42. De Commissie stelt aangiftepakketten ter beschikking van het publiek die op eenvoudig verzoek kunnen worden bekomen bij het Secretariaat van de Commissie per schrijven gericht per adres Hallepoortlaan 5-8 te 1060 Brussel (kantooradres) of Waterlooilaan 115 te 1000 Brussel (postadres), evenals per fax 02/542.72.12, tel. 02/542.72.00.

43. TH. LEONARD en Y. POULLET, *L.c.*, 379 (randnummer 4) aangaande de controle op de verwerkingen.

kingen met betrekking tot persoonsgegevens, die met behulp van geautomatiseerde procédés wordt uitgevoerd. Onder bewerking verstaat de wet o.m. het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens (art. 1 § 2 NWVP).

Nieuw element ingevolge de Wet van 11 december 1998 is derhalve dat door de vermelding van 'elke bewerking' in artikel 1 § 2 ook een individuele en dus eenmalige geautomatiseerde bewerking duidelijk onder de toepassing van de NWVP valt. Derhalve zou er van kunnen worden uitgegaan dat, gezien het doorzenden van videobeelden doorheen een camera als een geautomatiseerd verwerkingsprocédé kan worden beschouwd, de aangifteplicht toepasselijk zal zijn.

De wet preciseert dat de aangifte dient te gebeuren vooraleer wordt overgegaan tot een verwerking van persoonsgegevens, dit op straffe van een geldboete van honderd tot honderdduizend frank, aldus artikel 39 7° (N)WVP. Persoonsgegevens verwerken zonder de verwerking (tijdig) te hebben aangegeven is derhalve een strafbaar feit. Betekent dit dat het bewijsmateriaal dat verkregen werd met behulp van een niet-aangegeven camerasysteem niet kan worden gereguleerd door het verrichten van een latere aangifte bij de CBPL? Op dit vlak dient te worden verwezen naar de rechtspraak van het Hof van Cassatie m.b.t. het bewijs in strafzaken. Het Hof van Cassatie hanteert reeds sinds 1923⁴⁴ het principe dat onwettelijk verkregen bewijsmateriaal niet tot het bewijs van een inbreuk mag meewerken. Zo overwoog het Hof⁴⁵ nog recent dat 'de rechter niet vermag een misdrijf bewezen te verklaren, wanneer het daartoe aangevoerde bewijs, hetzij door de overheid die met de opsporing, de vaststelling of de vervolging ervan is belast, hetzij door de aangever van dat misdrijf door een strafbaar feit of op een andere wijze onrechtmatig is verkregen'.

Volgens de bewoordingen van artikel 17 (N)WVP dient een aangifte bij de CBPL slechts te worden verricht per (doelstelling van de) verwerking. Dit zogenaamde criterium van de 'generieke finaliteit'⁴⁶ staat dan ook los van andere factoren zoals de eventuele territoriale organisatie van een bedrijf of het aantal camera's dat in een bedrijf is geïnstalleerd. De aangifteplicht dient met andere woorden niet zoveel maal te worden verricht als er filialen van een bedrijf of geïnstalleerde camera's zijn, doch wel zoveel maal als er verwerkingen zijn, gefundeerd op eventueel verschillende niet-verenigbare toepassingen van het private camerasysteem.⁴⁷

44. Cass. 12 maart 1923, *Pas.* 1923, I, 233-234, aangehaald door P. TRAEST, *Het Bewijs in Strafzaken*, Gent, Mys & Breesch, 1992, 347 (nr. 664).

45. Zie o.m. Cass. 9 december 1997, *R.W.* 1997-1998, nr. 40, 1441.

46. Zie dienaangaande het reeds aangehaalde Verslag Merckx-Van Goey, pagina 80 en het advies CBPL nr. 10/92 d.d. 20 augustus 1992 betreffende het wetsontwerp tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals dit door de Kamer van Volksvertegenwoordigers werd overgemaakt aan de Senaat.

47. De preventie van diefstal van tentoongestelde goederen en controle van het productieproces zijn voorbeelden van niet-verenigbare doelstellingen. Dergelijke niet-verenigbare doelstellingen vormen volgens de WVP een aparte verwerking. Verbonden doelstellingen kunnen daarentegen door de ver-

DERDE VUISTREGEL: HET DOEL HEILIGT NIET HET MIDDEL DAT HIERTOE WORDT AANGEWEND OF CAMERABEWAKING ALS ULTIEME REMEDIE

De eis van finaliteitsafbakening en gerechtvaardigd doel: artikel 5 WVP en artikel 4 § 1 2° NWVP

Camerabewaking dient te kunnen steunen op een doelstelling die rechtvaardig dient te zijn. Het gaat hierbij niet zozeer om een concrete juridische basis zoals bijvoorbeeld het eigendomsrecht, maar bijvoorbeeld ook om een redelijk belang of vrijheid van de verantwoordelijke die in evenwicht is met de persoonlijke levenssfeer van de betrokkenen. Een legitiem doel impliceert dus een belangenafweging.⁴⁸ Onder de eerste vuistregel werd reeds gesteld dat de verantwoordelijke te allen tijde voldoende doorzichtigheid of duidelijkheid moet verschaffen aangaande zijn verwerking. Dit transparantieprincipe is door de wetgever in het bijzonder uitgewerkt op het gebied van het belang dat de verantwoordelijke dient te kunnen aanvoeren als rechtvaardiging voor het inzetten van zijn camerasysteem, en toont het problematisch karakter aan van (zeer) algemene of 'multi-aanwendbare' doelstellingen zoals 'veiligheid'. Beter is de doelstelling zo duidelijk en concreet mogelijk af te bakenen. Als mogelijk voorbeelden van dergelijke concrete doelomschrijvingen in het veld van de private beveiliging kunnen worden aangehaald: de toegangscontrole voor gebouwen (bijvoorbeeld appartementen) en de preventie van diefstal van koopwaren.

De vereiste van verenigbaar gebruik: artikel 5 WVP en artikel 4 § 1 2° NWVP

Beeldopnames mogen niet worden gebruikt voor andere doeleinden dan diegene die de verantwoordelijke dient op te geven. Van belang is er op te wijzen dat niet alleen de krachtens de eerste vuistregel geopenbaarde of 'papieren' doelstelling kan worden nagegaan door de CBPL of bevoegde rechter, doch ook het gebruik. Het verbod van doelafwending kan niet alleen worden toegepast in gevallen van duidelijk misbruik zoals het bespioneren van burens onder de noemer 'veiligheid', maar ook in situaties waar ondoordacht van de officiële doelstelling wordt afgeweken, zoals een handelszaak die officieel een camerasysteem gebruikt om diefstal door klanten te voorkomen, doch met hetzelfde systeem werknemers zou controleren die plots van hetzelfde feit verdacht worden. Een oplossing is hier wellicht om reeds bij het ogenblik van aangifte voldoende duidelijk en vooruitziend te zijn in het licht van mogelijke toepassingen in de toekomst, dit teneinde mogelijke problemen te vermijden.

→ antwoordelijke voor de verwerking wel onder de noemer van een enkele verwerking worden gebracht. Zie in dit kader TH. LEONARD en Y. POULLET, *L.c.*, 379 (randnummer 4).

48. zie Y. POULLET en TH. LEONARD, 'Les Libertés comme fondement de la protection des données nominatives' in F. RIGAUX (e.a.), *La vie privée: une liberté parmi les autres*, 229-277, waaronder vooral 263 en 264.

Een concreet camerabewakingssysteem dient een toetsing aan het zogenaamde 'proportionaliteitsprincipe' te kunnen doorstaan. Dit houdt in dat het systeem allereerst niet alleen nuttig, doch ook noodzakelijk dient te zijn in functie van het beoogde doel. Bovendien betekent dit principe vooral dat er geen sprake mag zijn van een verstoring van de belangenverhouding⁴⁹ doordat het camerasysteem als een te zware maatregel voor de concrete situatie zou uitvallen. Deze elementen worden hierna verder toegelicht.

Het aspect 'nuttigheid' betekent o.m. dat de niet-relevante opnames dienen te worden geweerd. O.m. kan hier worden gewezen naar camera's die tot doel hebben een handelszaak te beschermen, doch die eveneens gericht zouden zijn op de openbare weg⁵⁰ of plaatsen die hiertoe kunnen behoren zoals parkeerplaatsen.

Het element 'noodzakelijkheid' impliceert dat de verantwoordelijke moet kunnen aantonen dat hij voor het bereiken van zijn te beschermen belang over werkelijk geen andere afdoende alternatieven meer beschikt, aantoonbaar door bijvoorbeeld ervaringen uit het verleden zoals het aanhouden van ernstige inbreuken nadat alternatieve beveiligingstechnieken hebben gefaald. De noodzakelijkheid kan verder afhangen van het risico dat bepaalde situaties met zich brengen zoals de manipulaties met geld of waardevolle goederen, de frequentie waarmee inbreuken zijn te verwachten en het risico op letsel voor personen.

Tenslotte mag de belangenverhouding tussen de betrokkene en de verantwoordelijke niet worden verstoord door gebruik of de technische kenmerken van een camerasysteem.

Het beoordelen van dit laatste element vergt uiteraard een zeer concrete beoordeling; men dient zich dus de vraag te stellen of het plaatsen van een camerasysteem en de technische kenmerken hiervan niet verder gaan dan wat strikt genomen nodig is om het nagestreefde doel te bereiken.

In gevallen die als 'te zwaar' worden beoordeeld, zal helemaal geen camerasysteem kunnen worden geplaatst, zoals bijvoorbeeld een school die haar schoolreglement zou wensen te controleren met behulp van een camera of een verhuurder die het naleven van zijn huurreglement door de huurders zou willen controleren met behulp van camera's.

In andere gevallen zal wel een camerasysteem kunnen worden geïnstalleerd, waarbij de strikte noodzakelijkheid eventueel een performanter technisch systeem en dus verdergaand ingrijpen in de persoonlijke levenssfeer zal kunnen rechtvaardigen. Dit ingrijpen in de persoonlijke levenssfeer zal variëren naargelang de toepassing en de diverse technische kenmerken van het camerasysteem.

Qua gebruik kunnen camerabeelden al dan niet worden opgenomen en/of bewaard, camera's kunnen verborgen opgesteld staan en de duur van het bewaren

49. Artikel 2 WVP bepaalt: 'Iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, inzonderheid op bescherming van zijn persoonlijke levenssfeer.' Uit dit artikel kan het principe van belangenafweging worden afgeleid.

50. Corr. Dendermonde (16° Kamer), 22 juni 1999, A.R. 53.71.1463/96/3, onuitg.

van de opnames kan variëren. De concrete technische kenmerken en mogelijkheden van het camerasysteem zijn uiteraard ook van belang, zoals het analoog of digitaal karakter van de opnames, de beeldresolutie, evenals de mogelijkheden qua bediening op afstand, zoom, helderheid of actieradius. Verder kan worden gewezen op nieuwe digitale toepassingen die de detectiemogelijkheden van camera-systemen hebben verbeterd, bijvoorbeeld bij gebruik van 'intelligente' systemen die enkel reageren door opname en/of alarmsignaal indien zich 'ongewone' gebeurtenissen voortdoen (de zgn. Video-motion detection⁵¹). Camera-systemen kunnen nu echter ook worden gekoppeld aan databanken van bijvoorbeeld gezochte personen.⁵²

5. Bijzondere problemen bij private camerabewaking

MOGEN 'GEVOELIGE' GEGEVENS HET VOORWERP UITMAKEN VAN CAMERABEWAKING?

Gevoelige gegevens worden door de (N)WVP gedefinieerd in de artikelen 6 (o.m. raciale, godsdienstige en seksuele gegevens), 7 (medische gegevens) en 8 (gerechtelijke gegevens).

In het kader van deze bijdrage lijkt vooral de definitie van artikel 8 § 1 (N)WVP van belang, waar gerechtelijke gegevens worden gedefinieerd als 'persoonsgegevens inzake geschillen voorgelegd aan hoven en rechtbanken alsook aan administratieve gerechten inzake verdenkingen, vervolgingen of veroordelingen met betrekking tot misdrijven, of inzake administratieve sancties of veiligheidsmaatregelen'.

Opvallend is dat de private verwerking van dergelijke gerechtelijke gegevens door dit artikel 8 wordt verboden. Volgens de NWVP zou zelfs de toestemming van de gefilmde personen (bijvoorbeeld werknemers) geen uitzondering toelaten op het verwerkingsverbod voor gerechtelijke gegevens. De overige uitzonderingsmogelijkheden zoals de noodzaak voor de verwezenlijking van een wettelijk doel of het beheer van de eigen geschillen lijken immers geen afdoende duidelijke en zekere basis te bieden om als private instantie geldig videobeelden te verwerken voor voormelde gerechtelijke doeleinden.

Betekent dit dat een van de belangrijkste praktische toepassingen van camerabewaking een strafrechtelijke inbreuk op artikel 8 (N)WVP vormt en aldus bewijsmateriaal produceert dat niet bruikbaar is in juridische zin, zelfs indien de verantwoordelijke voor de verwerking reeds alle hiervoor aangehaalde fundamentele principes naleefde? Recente rechtspraak op basis van artikel 8 WVP (aangaande de mogelijke uitzonderingen op het verbod tot verwerking van 'gerechtelijke' gegevens) leek alvast in die richting te gaan door de vrijspraak toe kennen op basis van het onrechtmatig karakter van het verkregen bewijsmateri-

51. M. THIENPONT, 'Video-Motion Detection. Of hoe de camera een alarminstallatie werd', *Private Veiligheid* 1999, nr. 2, 32-38.

52. P. DE HERT, *Privacy en het gebruik van visuele technieken* (reeds aangehaald), 13.

aal. Zo sprak de Correctionele rechter te Antwerpen⁵³ reeds herhaaldelijk verschillende beklaagden vrij van de tenlastelegging van loondiefstal, die uitsluitend gebaseerd was op een video-opname. De rechter steunde hierbij op artikel 8 WVP en het niet-naleven van de aangifteplicht (art. 17 WVP). De rechter overwoog bovendien dat een werkgever die zelf een camera plaatste een strafbare inbreuk pleegde in de zin van het artikel 39 3° WVP. Een boomerang-effect is dus niet uitgesloten.

Het valt zeker te betreuren dat de wetgever tot op heden geen duidelijkheid heeft verschaft ten aanzien van alle private verantwoordelijken die wettelijk in orde willen zijn met hun systeem. In de huidige situatie waar massaal camera's in het maatschappelijke leven zijn opgedoken als private veiligheidsmaatregel, blijft men dus zitten met een versnipperde en onduidelijke reglementering die eenzijdig het gebruik van camera's door de overheid wenst te regelen en onvoldoende duidelijkheid biedt voor een van de voornaamste doelstellingen van privaat cameragebruik, met name het voorkomen van misdrijven op een bepaalde plaats.

Het probleem van onvoldoende basis voor de verwerking van gerechtelijke gegevens is nochtans niet nieuw. Dienaangaande overwoog de CBPL reeds in het voormelde advies nr. 14/95: *'Visuele beelden bevatten regelmatig onvermijdelijke informatie over het ras, de etnische afstamming, de religieuze of politieke overtuiging, of zelfs het seksueel gedrag. Ook kunnen beelden bijvoorbeeld informatie bevatten m.b.t. de verdenking van misdrijven.'* In dat kader drong de CBPL dan ook aan op het voorzien van een bijzondere machtigingsgrond voor de verwerking van dergelijke gegevens. Dezelfde vraag werd ook op 20 december 1995 gesteld door dhr. Borin⁵⁴ aan de toenmalige minister van Justitie.

Nu wettelijk initiatief op dit punt uitbleef, is het lovenswaardig dat de CBPL op dit punt inmiddels gebruik maakte van haar bevoegdheid tot interpretatie van de WVP. In haar recente advies nr. 34/99 van 13 december 1999 (punt IV) stelt de CBPL dat bij de problematiek van de gevoelige gegevens rekening moet worden gehouden met de context van het gebruik van de camera's en de nagestreefde doeleinden. Volgens de CBPL is niet alle informatie op zich gevoelig, zoals bijvoorbeeld de huidskleur van een persoon. De informatie kan echter gevoelig worden indien bijvoorbeeld de doelstelling van de beeldopname ligt in het identificeren van personen op basis van hun huidskleur. De CBPL erkent wel een verhoogd risico tot misbruik bij verwerking van gevoelige informatie en concludeert vervolgens op basis van het proportionaliteitsbeginsel dat de identificatiemogelijkheden van de camera's moeten worden beperkt.

Ondanks deze korte toelichting is het echter de vraag hoe de rechtspraak zal reageren op de private camerabewaking. De onduidelijkheid rond het (il)legaal karakter van de private camerabewaking is dus nog niet verdwenen.

53. Corr. Antwerpen (Kamer 3C), 21 november 1997, A.R. 4027, onuitg.; Corr. Antwerpen (Kamer 3C), 2 juni 1999, A.R. 2193, onuitg.

54. Zie Vraag nr. 172 van dhr. Borin over de bewaking met infraroodcamera's in de kamers van gespecialiseerde instellingen, beknopt Verslag Kamer, G.Z., 1995-1996, COM 20 december 1995, C 52 - 4 t.e.m. 6.

KUNNEN DE BEELDEN WORDEN BEWAARD EN WAT IS DE BEWARINGSTERMIJN?

In haar advies nr. 34/99 van 13 december 1999 had de CBPL ook aandacht voor de vraag naar de mogelijkheid tot het bewaren van opgenomen beelden, en de tijd gedurende dewelke opgenomen beelden kunnen worden bewaard.

Het bewaren van de opnames dient volgens de CBPL op basis van het proportionaliteitsbeginsel de uitzondering te zijn op de regel dat beelden niet worden opgenomen.

Indien wel wordt opgenomen kan dit opnieuw slechts voor een beperkte duur. De WVP voorziet overigens nergens een algemene duur voor het bewaren van opnames, zodat in concreto een afweging zal moeten worden gemaakt in functie van zowel de doelstelling als de technische kenmerken van het systeem.

Vanuit technisch opzicht overwoog de CBPL dat de bewaringstermijn afhankelijk is van de bewaringscapaciteiten van een concreet systeem. Zo zal een digitale opslag minder ruimte vergen en grotere kwaliteitswaarborgen kunnen bieden in vergelijking met analoge registraties, zodat digitale opslag een groter risico inhoudt voor de persoonlijke levenssfeer. Wat de doelstelling betreft moeten de beelden in elk geval worden gewist indien voor het nog langer bewaren van de beelden geen verantwoorde reden meer is aan te tonen doordat bijvoorbeeld geen incidenten hebben plaatsgevonden.

Tenslotte kan nog worden gesteld dat voor private camerabewaking een kortere bewaringstermijn is toegestaan in vergelijking met het gebruik van camera's dat door een overheid is voorzien en geregeld. In het camerabesluit m.b.t. voetbal werd bijvoorbeeld aanvankelijk een bewaringstermijn van vijf jaar ingeschreven. Deze termijn werd evenwel door zowel de CBPL bij advies nr. 17/99 van 10 mei 1999 als de Raad van State⁵⁵ als disproportioneel bevonden in functie van het beoogde doel, zodat de termijn werd herleid tot één jaar behoudens het geval van inbeslagname van de beelden.

Ter vergelijking kan er ook op worden gewezen dat men in het Franse systeem⁵⁶ heeft gekozen voor een duur van 1 maand, waar de Registratiekamer in Nederland⁵⁷ veel strenger is door een termijn van 24 uur voor te houden als norm, behoudens het geval waar een noodzaak voor het langer bewaren kan

55. Zie het advies van de Raad van State m.b.t. het K.B. van 12 september 1999, *B.S.* 5 oktober 1999, 37407.

56. In haar advies van 10 november 1992 overwoog de CNIL reeds in de SNCF-zaak: 'Considérant qu'en l'espèce, ce délai d'un mois n'est pas excessif'. Dit advies is gepubliceerd en becommentarieerd in *Commission Nationale de l'informatique et des libertés (CNIL)*, 'Vingt Délibérations commentées', Paris, La Documentation française, 1998, 97-104; artikel 10, lid 4 Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (Wet Securité.), *J.O.* 24 janvier 1995, 1249-1263. Zie voor een bespreking van deze laatste wet: P. DE HERT en S. GUTWIRTH, 'Cameratoezicht, veiligheid en de wet persoonsregistraties. Juridische denkoefeningen naar aanleiding van de Franse Wet van 21 januari 1995 inzake veiligheid', *Recht en kritiek* 1995, 218-250.

57. Registratiekamer nr. 97.0.0067 d.d. 27 januari 1997, Privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging, te raadplegen op http://www.registratiekamer.nl/bis/top_1_5_34_10.htm (punt 9). Dit standpunt wordt herhaald in volgend rapport van de Registratiekamer: *In Beeld gebracht, Privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging*, januari 1997, 26.

worden aangetoond doordat de vaststelling van incidenten niet onmiddellijk kan gebeuren.

VORMEN VERBORGEN CAMERA'S EEN INBREUK OP DE (N)WVP?

Camera's worden in de praktijk heel vaak verborgen opgesteld, dat wil zeggen niet of moeilijk met het blote oog detecteerbaar. Een strenge houding ten aanzien van verborgen opgestelde camera's was reeds in de rechtspraak⁵⁸ terug te vinden, zij het vaak op grond van andere overwegingen of rechtsgronden dan de (N)WVP. De vraag stelt zich of het gebruiken van dergelijke verborgen camera's verenigbaar kan zijn met de (N)WVP. Het beantwoorden van deze vraag komt dus neer op een toetsing van voormelde principes op de concrete situatie.

Vooraf de proportionaliteitsafweging en de informatieplicht blijken in dit kader van belang. Twee vragen lijken hierbij aan de orde. Ten eerste: wat is de werkelijke reden voor het verborgen opstellen van een camera? Daarnaast kan men zich afvragen of een verborgen camera verenigbaar is met de informatieplicht.

De werkelijke redenen voor het opstellen van dergelijke camera's lopen in de praktijk uiteen. Zo kan terecht worden geargumenteed dat een verborgen camera een efficiënter middel is dan een zichtbare camera om zwaardere misdrijven zoals een gewapende overval te bestrijden. Bij dergelijke types misdrijven riskeert men immers toenemend geweld om de zichtbare camera's te saboteren. In bedrijfscontext wenst men daarnaast vaak verzet van de werknemers te vermijden door het verborgen opstellen van camera's. Dit doeleinde (vermijden van inspraak van de werknemers) lijkt minder gerechtvaardigd.

Uit de informatieplicht en het eerlijkheidsprincipe volgt minstens het verbod van het heimelijk filmen, waaronder kan worden verstaan het niet aangekondigd plaatsen van verborgen camera's. Indien de verantwoordelijke voor de verwerking niet voorafgaand verwittigt dat hij verborgen camera's plaatst, dreigt hij derhalve zijn informatieplicht te schenden en zijn bewijsmateriaal juridisch onbruikbaar verklaard te zien. Verborgen camera's lijken dus op zich genomen niet altijd strijdig te zijn met de WVP, bijvoorbeeld in het geval waar de verantwoordelijke duidelijk en tijdig de gefilmde personen conform artikel 9 § 1 WVP heeft geïnformeerd rond het feit dat camera's verborgen staan opgesteld.⁵⁹

6. Conclusie

De (N)WVP blijkt zowel qua toepassingsgebied als qua regeling nog elementen te bevatten die voor de argeloze veiligheidsverantwoordelijke die 'geacht wordt de wet te kennen' onaangename verrassingen in petto zou kunnen hebben, zoals

58. Zie bijvoorbeeld Vred. Roeselare, 24 juni 1988, *T. Vred.* 1988, 319; Arbeidshof 23 maart 1993, *T.Gez.* 1995-1996, 296-306 met noot J. STIEVENARD, zoals aangehaald door P. DE HERT, *Privacy en het gebruik van visuele technieken door burger en politie, Belgische regelgeving vandaag en morgen*, Brussel, Politeia, 1998. Het Franse Hof van Cassatie paste deze regel toe in een zaak van diefstal door een werknemer: Cass. Fr. 20 november 1991, Dalloz, 1992, *Jurisprudence* p. 73, te raadplegen op <http://jurisweb.citeweb.net/cass/soc20111991.htm>.

59. Zie ook B. MAGREZ en H. VANOVERSCHELDE, *l.c.*, 7.

de strafrechtelijke vrijspraak van de gefilmde bij gebrek aan alternatieve bewijsmiddelen, de verbeurdverklaring van de videopnames en zelfs het worden aangesproken door de overheid tot naleving van de (N)WVP. Camera's gebruiken lijkt dan ook bijna op het werpen van een boomerang of een belegging in een risicovol bewijsmiddel.

Het is bijgevolg aan de overheid om duidelijkheid te verschaffen door het vastleggen van de voorwaarden of grenzen binnen dewelke private camerabewaking toelaatbaar is. Hierbij kan zowel worden gedacht aan een aanpassing van de NWVP als het opstellen van een bijzondere camerawet. Men kan zich bij dergelijke aanpassingen afvragen of het algemene dataprotectiesysteem van de WVP wel een voldoende en geschikt middel is om een (wettelijke) omkadering te bieden voor alle vormen van private camerabewaking. De vraag stelt zich anderzijds of een bijzondere camerawet wel te verkiezen is boven een aanpassing of verduidelijking van de (N)WVP.

Mocht de wetgever het opstellen van een bijzondere camerawet verkiezen, dan zullen wellicht enkele van de volgende valkuilen moeten worden vermeden.

Een eerste gevaar is dat een te vlug opgestelde bijzondere camerawet de reeds uitgebouwde beschermingsregeling m.b.t. de verwerking van persoonsgegevens formeel of materieel zou kunnen uithollen. Een blijvende onafhankelijke controle op de fundamentele principes die de WVP beschermt (transparantie, finaliteit en het verbod tot verwerking van gevoelige gegevens) lijkt geen overbodige luxe om ontsporingen te kunnen aanpakken.

Een te vlug opgestelde camerawet die een regularisering van de huidige toestand wenst tot stand te brengen, zou juist kunnen zorgen voor een toename van het aantal camera's en een verminderde controlemogelijkheid. Een goedkeuring of vergunning houdt immers het risico in van een gelegaliseerde toename van het aantal camera's. Zullen deze gelegaliseerde systemen ook nog ten volle kunnen worden getoetst door een onafhankelijke instantie aan de fundamentele beginselen van de (N)WVP?

Ten slotte houdt een camerawet ook het risico in van wetsinflatie⁶⁰ door het uitvaardigen van wetsebepalingen die overlappen of zelfs strijdig zijn met de reeds in aanhef vermelde rechtsbronnen. De (N)WVP zal immers als kaderwet naast de camerawet blijven gelden, tenzij de wetgever duidelijk het tegendeel zou voorzien.

Het domein van private beveiliging blijft bijgevolg een sector waar de private actoren dienen rekening te houden met de door de overheid afgebakende grenslijnen.

60. Zie voor een rechtstheoretische uitdieping van deze problematiek J. WINTGENS en J. DHONT, *Wet en Wereldbeeld*, Centrum voor Rechtstheorie/European Academy of Legal Theory, K.U.Brussel, te verschijnen in *Omnilegie*.