*Mr. dr. G.-J. Zwenne en mr. dr. L. Mommers**

Wetenschappelijk artikel
Zijn foto's en beeldopnamen 'rasgegevens' in de zin van artikel 126nd Sv en artikel 18 Wbp?

206

Trefwoorden:
foto's en beeldopnamen, rasgegevens, artikel 126nd jo. 126nf Sv, artikel 16 jo. 18 Wbp

In een recent strafrechtelijk arrest heeft de Hoge Raad uitgemaakt dat foto's van identificeerbare natuurlijke personen moeten worden aangemerkt als 'gegevens betreffende iemands ras' in de zin van artikel 126nd Sv en artikel 16 jo. 18 Wbp. Het arrest kwam niet als een verrassing, want was in lijn met eerdere rechtspraak van het hoogste rechtscollege. En de wetgever heeft weinig twijfel laten bestaan over deze en andere 'bijzondere' of 'gevoelige' gegevens. Toch valt er meer over te zeggen. Allereerst omdat onze privacytoezichthouder nog niet zo heel lang geleden een heel andere uitleg verdedigde. En verder omdat er inmiddels meer dan een handvol voorbeelden is van rechtspraak van strafrechters die daarover toch anders denken dan ons hoogste rechtscollege. In deze bijdrage volgt, in samenhang met de visie van het CBP en de parlementaire geschiedenis van de Wbp, een bespreking van de desbetreffende uitspraken.

1 Inleiding

Vallen foto's en beeldopnamen onder de definitie van 'persoonsgegeven betreffende iemands ras'? Het antwoord ligt voor de hand. Als uit die foto's of beeldopnamen de huidskleur blijkt, of de vorm van de ogen of neus, haarkleur enzovoorts, dan kan dat duiden op het ras van de geportretteerde. In zoverre vallen herkenbare foto's en beeldopnamen onder het begrip rasgegevens.

De vraag en het antwoord zijn relevant, niet alleen voor de toepassing van artikel 16 jo. 18 en 23 van de Wet bescherming persoonsgegevens (Wbp), maar ook – in een voorkomend geval – voor de wijze waarop en de mate waarin de officier van justitie (OvJ) zijn bevoegdheid om gegevens te vorderen in het kader van een strafrechtelijk onderzoek kan uitoefenen. Als er sprake is van gegevens betreffende iemands ras, mag de OvJ deze gegevens volgens de wet uitsluitend vorderen na voorafgaande schriftelijke machtiging van de rechter-commissaris. Aldus artikel 126nf jo. 126nd van het Wetboek van Strafvordering (Sv).

Onlangs wees de Hoge Raad[1] een arrest over deze bevoegdheid tot gegevensvordering van de OvJ, en de vraag over de kwalificatie van foto's en beeldopnamen als bijzondere of gevoelige gegevens in de zin van voornoemde bepalingen. Al heel snel na het arrest blijken vonnissen en arresten te zijn gewezen waarin politierechters, meervoudige kamers van rechtbanken en gerechtshoven zich in bochten lijken te wringen om van dit arrest af te wijken en de gevolgen van deze uitspraak te nuanceren.

In deze bijdrage bespreken wij deze uitspraken. We beginnen echter met een korte schets van de relevante parlementaire geschiedenis en wat het College bescherming persoonsgegevens (CBP) daarvan vindt. Vervolgens gaan we in op het arrest van de Hoge Raad en bespreken we de door ons gevonden lagere rechtspraak. We ronden af met enige afsluitende opmerkingen.

2 Achtergrond

De wetgever laat er weinig twijfel over bestaan dat foto's en beeldopnamen van identificeerbare natuurlijke personen moeten worden aangemerkt als 'gegevens betreffende iemands ras' in de zin van artikel 16 jo. 18 Wbp. De memorie van toelichting bij de Wbp stelt dat het begrip 'ras' ruim moet worden uitgelegd en dat het dezelfde betekenis heeft als in artikel 1 Grondwet. Over gevoelige of bijzondere gegevens in het algemeen wordt opgemerkt dat daartoe ook moeten worden gerekend:[2]

'de gegevens die weliswaar als zodanig daarop geen betrekking hebben, maar waaruit wel de aanwezigheid van een gevoelig kenmerk rechtstreeks kan worden afgeleid.'

Over rasgegevens en foto's op toegangspasjes wordt de volgende opmerking gemaakt:[3]

'Aangezien van de foto op het pasje het ras van de werknemer kan worden afgeleid, valt de hier bedoelde verwerking tevens onder de reikwijdte van artikel 8 [betreffende bijzondere gegevens] van de richtlijn […]. Om-

* **Gerrit-Jan Zwenne is advocaat bij Bird & Bird te Den Haag en universitair hoofddocent bij eLaw@Leiden, centrum voor recht in de informatiemaatschappij, van de Universiteit Leiden. Laurens Mommers is consultant bij Legal Intelligence en universitair hoofddocent bij eLaw@Leiden.** **De auteurs danken Eva Riphagen voor haar grondige onderzoekswerk ten behoeve van dit artikel, en Menno Bruning voor zijn waardevolle commentaar op een eerdere versie van deze bijdrage.**

1 HR 23 maart 2010, *LJN* BK6331.
2 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 101.
3 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 105; daarover De Vries 2009 (*T&C Telecomrecht*), art. 18 Wbp, aant. 2.

dat het gaat om een gevoelig gegeven, stelt het eerste lid [van artikel 18 Wbp] wel een harde eis. Verwerking van een rasgegeven is – afgezien van de grenzen die inherent zijn aan de elders in het wetsvoorstel geregelde algemene beginselen van gegevensverwerking – alleen dan geoorloofd als het met het oog op die identificatie onvermijdelijk is.'

Daarmee laat de wetgever weinig ruimte om herkenbare (pas)foto's en beeldopnamen van natuurlijke personen niet als rasgegevens aan te merken. Aanvankelijk volgde het CBP deze uitleg. Zo maakte het college in een informatieblad de opmerking dat voor een intranetsmoelenboek toestemming van de desbetreffende werknemers moet worden verkregen voordat hun foto's daarin zouden worden opgenomen, omdat deze foto's zouden moeten worden aangemerkt als gevoelige of bijzondere gegevens.[4] Ook de handleiding voor gegevensverwerkers, die van de website van de toezichthouder kan worden gedownload, gaat uit van deze wetsuitleg en wetstoepassing.[5]

Eind 2007 is het college met een genuanceerder standpunt gekomen. In zijn Richtsnoeren publicatie van persoonsgegevens op internet[6] introduceert het college een nieuw en aanvullend criterium aan de hand waarvan het sindsdien beoordeelt of foto's of beeldopnamen inderdaad als rasgegevens moeten worden aangemerkt:

'Alleen als een verantwoordelijke foto's of ander beeldmateriaal publiceert met het uitdrukkelijke doel om onderscheid te maken naar ras, is bijzondere oplettendheid geboden. In dat geval acht het CBP het een redelijke wetstoepassing om het beeldmateriaal aan te merken als een bijzonder persoonsgegeven.'

Het college kent dus betekenis toe aan het doel waarvoor de foto's en het beeldmateriaal worden gebruikt. Als dat beeldmateriaal zoals bij de intranetsmoelenboeken niet wordt gebruikt om onderscheid te maken naar ras dan is er, zo moet de toezichthouder kennelijk worden begrepen, géén sprake van gegevens betreffende iemands ras.[7] Met deze wetsuitleg en wetstoepassing komt het college tegemoet aan het breed gevoelde sentiment dat voor smoelenboeken of een socialenetwerksite niet dezelfde beperkingen zouden moeten gelden als voor etnische databanken waarin raskenmerken van individuen worden vastgelegd.[8] Er was dan ook wel waardering voor deze koerswijziging,[9] maar toch vooral ook kritiek (strijd met geldend recht, met name door kennelijk als extra vereiste voor de kwalificatie als bijzonder persoonsgegeven te stellen dat de publicatie als *uitdrukkelijk doel* heeft onderscheid te maken naar ras).[10]

3 Rechtspraak

3.1 *OV-chipkaart (Hoge Raad 23 maart 2010, LJN BK6331)*

In zijn arrest van 23 maart 2010 beantwoordt de Hoge Raad de vraag of foto's en beeldopnamen als rasgegevens moeten worden aangemerkt. De Hoge Raad doet dit in het kader van de beoordeling van een vordering van een OvJ op basis van artikel 126nd en 126nf Sv.[11] Het voorgelegde geval betrof een vordering gericht aan het Rotterdamse OV-bedrijf RET voor het verkrijgen van naam- en adresgegevens en foto's van de reizigers die gedurende een bepaalde periode in de metro gebruik hadden gemaakt van hun OV-chipkaart. Als de gevorderde foto's zouden worden aangemerkt als gegevens betreffende iemands ras, betekende dit dat voor de vordering een machtiging van de rechter-commissaris vereist was. En dus dat, als de vordering is gedaan zonder deze rechterlijke machtiging, de verkregen foto's niet als bewijs in deze zaak hadden mogen worden gebruikt.[12]

In het arrest neemt de Hoge Raad tot uitgangspunt de bedoeling van de wetgever zoals deze blijkt uit de parlementaire geschiedenis van artikel 16 en 18 Wbp:[13]

'Uit de wetgeschiedenis volgt dat niet alleen gegevens die direct het ras van een persoon betreffen, maar ook gegevens waaruit informatie over het ras van een persoon kan worden afgeleid, zoals een foto van een persoon, als "gevoelige" informatie moet worden aangemerkt, die door de Officier van Justitie slechts kan worden gevorderd op de voet van de art. 126nd en 126nf Sv, dus na daartoe door de rechter-commissaris verleende machtiging. De Rechtbank heeft dat terecht tot uitgangspunt genomen. Het middel berust op de opvatting dat in een geval als het onderhavige, waarin de vordering uitdrukkelijk ook betrekking had op foto's van personen, toepassing van genoemde bepalingen alleen in aanmerking komt indien met de vordering is beoogd de desbetreffende gevoelige informatie aan die foto's te ontlenen. Die opvatting is onjuist, zodat het middel faalt.'

---

4 CBP Informatieblad, *Verstrekken van personeelsgegevens aan derden*, nr. 2A, september 2004, p. 2.
5 L.B. Sauerwein & J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: april 2002, p. 48-49.
6 CBP Richtsnoeren, *Publicatie van persoonsgegevens op internet*, december 2007, p. 15.
7 Vgl. CBP 25 april 2006, z2005-0846 opgenomen in T.E. van Dijk e.a. (red.), *Uitsprakenbundel. Wet bescherming persoonsgegevens*, Den Haag 2009, nr. 8.39, p. 238-240 – waarin het CBP een oordeel geeft over de verwerking van opnamen gemaakt met een beveiligingscamera, zonder daarbij in te gaan op de criteria van artikel 16 jo. 18 Wbp.
8 Zie Zwenne et al., *Eerste fase evaluatie Wet bescherming persoonsgegevens*, Leiden 2007, p. 75; CBP Brief aan Minister van Justitie 12 juli 2005, z2004-1494.
9 J.M.A. Berkvens, 'Richtsnoeren publicatie persoonsgegevens op internet', *Computerrecht* 2008-133, p. 2-3.
10 J.M. van Essen, 'Richtsnoeren publicaties op internet, een brug te ver?', *P&I* 2008, p. 83-84; N. Wisman, 'Persoonsgegevens: bij twijfel "bijzonder"?', *P&I* 2009, p. 136; N. Wisman, 'Noot bij de uitspraak van Rb. Rotterdam van 2 juni 2008', *Computerrecht* 2009-4, p. 4-7 en toch ook Berkvens, *a.w.*
11 In HR 3 maart 2009, *LJN* BG9218 kwam de Hoge Raad tot een vergelijkbare uitleg van het begrip 'gezondheidsgegeven'.
12 'Rovers vrijuit door uitspraak Hoge Raad', *Telegraaf* 6 april 2010.
13 R.o. 2.6.

Naar het oordeel van de Hoge Raad moeten foto's van personen derhalve wél worden aangemerkt als gevoelige (ras)gegevens waarvoor een machtiging van de rechter-commissaris is vereist, ook als deze foto's niet zijn gevorderd om daaraan rasgegevens te ontlenen. Aldus verwerpt het hoogste rechtscollege de juistheid van de voorgestane rechtsopvatting van het Openbaar Ministerie dat van gevoelige of bijzondere gegevens alleen sprake kan zijn als de foto's zijn gevorderd met het doel om daaruit gegevens betreffende het ras af te leiden.

Het arrest was geen verrassing. De daarin gevolgde redenering sluit aan bij een eerder arrest over een andere categorie van gevoelige of bijzondere gegevens, namelijk gegevens betreffende de gezondheid (zie noot 10). Ook daarin oordeelde de Hoge Raad dat onder het begrip 'gezondheidsgegeven' niet alleen gegevens vallen die de gezondheid van een persoon direct betreffen, maar ook gegevens waaruit informatie over de gezondheid van een persoon kan worden afgeleid.[14]

En, hoewel het arrest daarover geen overwegingen bevat, zijn de daarin neergelegde rechtsopvatting en gegeven wetsinterpretatie ook in lijn met het *Lindqvist*-arrest van het Europees Hof van Justitie. In dit arrest koos het Hof ervoor om bij de uitleg van het begrip 'gegevensdoorgifte', net als de Hoge Raad bij de uitleg van de begrippen 'rasgegevens' en 'gezondheidsgegevens', niet uit te gaan van het oogmerk of bedoelingen van de verantwoordelijke.[15]

Omdat de Hoge Raad uitgaat van de parlementaire geschiedenis van de Wbp, is er geen reden om aan te nemen dat deze uitleg beperkt zou zijn tot informatievorderingen in de context van een strafrechtelijk onderzoek. De uitleg geldt voor alle verwerkingen van foto's en beeldopnamen van herkenbare natuurlijke personen en heeft dus ook betekenis voor de toepassing van de Wbp.[16]

In de lagere rechtspraak lijkt niettemin deze door de Hoge Raad gegeven uitleg van het begrip gevoelige of bijzondere gegevens in veel gevallen niet te worden gevolgd. In openbare bronnen zijn inmiddels meer dan tien uitspraken te vinden waarin lagere rechters ervoor kiezen om beeldopnamen van personen niet aan te merken als 'gegevens betreffende iemands ras'.[17] Al deze uitspraken zijn gedaan in een tijdsbestek van nog geen vier maanden na het arrest van maart 2010, te weten vanaf half april tot begin augustus dit jaar. We bespreken negen van deze uitspraken in chronologische volgorde.[18]

3.2 *Camerabeelden bij Rabobank (Rb. Zutphen 15 april 2010, LJN BM1196)*

Minder dan vier weken na het arrest van ons hoogste rechtscollege wijst de politierechter van de Rechtbank Zutphen vonnis in een zaak over een 'veelpleger'. De politierechter gaat uitgebreid in op het arrest van de Hoge Raad en zoekt nadrukkelijk naar argumenten om daarvan te kunnen afwijken. Daarbij acht zij allereerst van belang dat de opnamen waren gemaakt met beveiligingscamera's bij een vestiging van de Rabobank. Anders dan in het arrest van de Hoge Raad beschikte de bank dus niet over deze beelden in het kader van haar klantrelatie met degenen van wie de opname was gemaakt.

'Het verkrijgen van camerabeelden als op zich zelf staande "losse" informatiebron, levert geen schending op van het hiervoor [door de Wbp en Sv te beschermen, *auteurs*] geschetste privacybelang dat de regeling middels oplopende voorwaarden beoogt te beschermen. In dit geval is immers geen sprake van een (dienstverlenende) relatie tussen de onderhavige bank en verdachte, uit hoofde waarvan de bank over de bewuste gegevens (beeldmateriaal) beschikt. Integendeel, verdachte heeft zich als passant, op straat, binnen het bereik van deze (beveiligings-)camera bevonden.'

Voor deze Zutphense politierechter ligt daarin een beslissend verschil tussen de haar voorgelegde zaak en de zaak waarop het arrest van de Hoge Raad betrekking had. We krijgen de indruk, maar erg duidelijk vinden we het niet, dat dit verschil voor de politierechter erin zit dat de verdachte in de dienstverlenende relatie met de bank wellicht bepaalde verwachtingen mag hebben met betrekking tot het gebruik en de verstrekking van de door hem verstrekte gegevens. En dit is anders als het gaat om beeldopnamen die met beveiligingscamera's op straat worden gemaakt. Als, zo lijkt de redenering te zijn geweest, de verdachte op de hoogte is van de aanwezigheid van camera's en hij eveneens weet dat deze worden gebruikt voor beveiligingsdoeleinden, dan heeft hij de mogelijkheid zich daaraan te onttrekken. Doet hij dat niet, dan mag worden aangenomen dat hij zijn persoonsgegevens voor deze beveiligingsdoeleinden ter beschikking heeft gesteld.[19]

Daarnaast, en in verband daarmee, lijkt de Zutphense politierechter betekenis toe te kennen aan het al dan niet inherente of bijkomstige karakter van de te verkrijgen rasgegevens:

---

14 HR 3 maart 2009, *LJN* BG9218, *NJ* 2009, 325 (m.nt. Mevis).

15 Zie HvJ EU 6 november 2010, zaak C 101/01, r.o. 54; daarover G.-J. Zwenne bij HvJ EG 6 november 2003, zaak C 101/01, in T.E. van Dijk e.a. (red.), *Uitsprakenbundel. Wet bescherming persoonsgegevens*, Den Haag 2009, nr. 2.1, p. 43-58.

16 Aldus r.o. 2.4 en 2.5; *Kamerstukken II* 2003/04, 29 441, nr. 3, par. 4.4; *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 100-105; zie echter ook Mevis in zijn noot bij het arrest in *NJ* 2010, 355.

17 Op rechtspraak.nl wordt minder dan twee procent van alle rechtspraak gepubliceerd. Het gaat dus misschien om het spreekwoordelijke 'topje van de ijsberg'. Vgl. L. Mommers & G.-J. Zwenne, 'Publiceer nu eens alle rechterlijke uitspraken', *NRC* 2 juli 2010; L. Mommers, G.-J. Zwenne & B.W. Schermer, 'Het best bewaarde geheim van de raadkamer', *NJB* 2010.

18 Dit zijn alle uitspraken die in relevante Nederlandse jurisprudentie-uitgaven en op rechtspraak.nl konden worden teruggevonden op basis van de trefwoorden '126nd' en 'gevoelige gegevens' in de genoemde periode, met uitzondering van *LJN* BN1730 (verkort vonnis zonder motivering m.b.t. het onderhavige thema) en *LJN* BN1699 (betreft niet de kwalificatie als bijzondere gegevens, maar de 'vrijwilligheid' van de afgifte van de beelden en de al dan niet aanwezige noodzaak van een vordering ex artikel 126nd jo. 126nf Sv). Zie noot 17 voor de beperkingen van het zoeken in rechtspraak.

19 Vgl. *Kamerstukken II* 1997/98, 25 982, nr. 3, p. 156.

'In zoverre verschilt de onderhavige zaak dan ook van het door de Hoge Raad op 23 maart 2010 besliste geval. Daarin werden immers door de officier van justitie van een bedrijf gegevens gevorderd behorend bij een barcode van in een specifieke periode en op bepaalde plaatsen gebruikte OV-chipkaarten, zoals naam, adres en woonplaatsgegevens en een foto. Uit zo'n foto kan de huidskleur van de betreffende kaarthouder worden afgeleid. Dit bedrijf beschikte over die gegevens, omdat die door de betrokken personen waren verstrekt om een OV-chipkaart te kunnen verkrijgen. Het vorderen van die gegevens door de officier van justitie diende een ander doel, namelijk dat van de opsporing. De vordering strekte er dan ook toe om tegelijk met een persoon identificerende gegevens, ook gevoelige gegevens, zoals uit een foto blijkende informatie omtrent huidskleur van de betrokken reizigers, te verkrijgen. Om die reden kon de vordering in die zaak niet op artikel 126nd Sv gebaseerd worden.'

In de zaak waarover de Hoge Raad in zijn arrest oordeelde, werden gegevens opgevraagd die hoe dan ook als rasgegevens moeten worden aangemerkt. In de aan de politierechter voorgelegde zaak was dat, volgens haar, anders. In deze zaak was er geen sprake van dat de OvJ gegevens vorderde met het oog op het achterhalen van de identiteit van de verdachte en daarmee betrekking hebbend op diens ras. De OvJ vorderde gegevens waaruit, als bijkomstigheid, ook het ras van de verdachte bleek:

'Als vervolgens, bij het bekijken van de beelden door de politie, blijkt dat daarop personen voorkomen van wie (bijvoorbeeld) ook de huidskleur zichtbaar is, dan maakt dit in het onderhavige geval de toepassing van de bevoegdheid ex artikel 126nd Sv achteraf niet onrechtmatig en staat niets het gebruik van die beelden en de daarmee verkregen (gevoelige) informatie in de weg.'

De uitspraak is niet helemaal duidelijk. Wij houden het erop dat de Zutphense politierechter een doelcriterium introduceert, vergelijkbaar met het criterium aan de hand waarvan het CBP foto's buiten de begripsomschrijving van rasgegevens leek proberen te brengen: alleen als het de bedoeling is om rasgegevens te verkrijgen, is er sprake van gevoelige rasgegevens, en anders niet. Deze redenering lijkt op gespannen voet te staan met het arrest van de Hoge Raad, omdat daarin is uitgemaakt dat niet kan worden aangenomen dat er alleen sprake is van gevoelige rasgegevens, als de OvJ beoogd heeft de desbetreffende gevoelige rasgegevens aan die foto's te ontlenen.

Wat zich nog wel zou verhouden met de in het arrest neergelegde rechtsopvatting, is de situatie waarin de OvJ beeldopnamen vorderde waarvan hij echt niet kon vermoeden dat daaruit gevoelige gegevens zouden kunnen worden afgeleid. In die situatie kan mogelijk nog worden gezegd dat hij geen gevoelige gegevens vorderde, maar daarover later als 'bijvangst' of 'bijproduct' kon beschikken.[20] Een dergelijke situatie mag echter, omwille van rechtsbescherming en rechtszekerheid (legaliteitsbeginsel), niet te snel worden verondersteld. En daarbij lijkt het, waar het gaat om het vorderen van camerabeelden, niet heel erg waarschijnlijk dat die situatie zich in dit geval voordeed. Zou de OvJ echt niet hebben voorzien dat uit de gevorderde beelden raskenmerken (huidskleur, haartype enz.) zouden kunnen blijken?

3.3 *Pintransactie in casino (Hof Den Haag 6 mei 2010, LJN BM8433)*

Het Gerechtshof Den Haag moest zich uitlaten over camerabeelden betreffende een pintransactie in een casino, die de OvJ had gevorderd zonder machtiging van de rechter-commissaris. Evenals de hiervoor besproken uitspraak van de Zutphense politierechter acht het hof van belang dat de beeldopnamen niet zijn gevorderd om daaruit rasgegevens af te leiden, alsook dat deze camerabeelden zijn gemaakt met het doel opsporing mogelijk te maken en niet door de betrokken verdachte zelf zijn verstrekt:

'… de officier van justitie [heeft] […] afgifte van de beelden gevorderd om informatie te verkrijgen over een transactie die is gepleegd met een bankpas ten aanzien waarvan eerder aangifte van diefstal was gedaan. Het is hierbij niet op voorhand de bedoeling geweest om gegevens te vorderen om daaraan gevoelige informatie te ontlenen. De beelden zijn niet door de personen die daarop staan afgebeeld afgegeven, en zijn niet gekoppeld aan (door dezen in vertrouwen aan een instantie afgegeven) personalia. Het gaat bij dit type cameratoezicht enkel om de vastlegging van het beeld van degene die komt pinnen. Beoogd wordt hiermee de opsporing mogelijk te maken van diegenen die op onrechtmatige wijze gebruik maken van pinpassen.'

Het hof introduceert nog als een ander criterium of degene van wie beeldopnamen werden gemaakt daarmee al dan niet bekend mag worden verondersteld:

'Het is een feit van algemene bekendheid dat bij pinautomaten camerabeelden worden opgenomen, juist ter bescherming van de belangen van degenen die van de mogelijkheid om te pinnen op rechtmatige wijze gebruik willen maken. Voor beelden, opgenomen in winkels en casino's ter bestrijding en voorkoming van winkeldiefstallen en andere criminaliteit, geldt mutatis mutandis hetzelfde. Gelet hierop kan niet gezegd worden dat de afgifte van de beelden in de onderhavige zaak inbreuk maakt op een rechtens te beschermen belang.'

De relevantie van 'het feit van algemene bekendheid' ligt daarin, begrijpen we, dat dan kan worden verondersteld dat degenen van wie beeldopnamen worden gemaakt daarmee bekend zijn. En dat betekent dan, in de redenering van het hof, dat deze personen ten aanzien

20 Aldus nr. 3.6 van de conclusie van A-G Machielse; zie ook Mevis *a.w.*

van die opnamen geen verwachtingen mogen hebben. Ze hebben er maar rekening mee te houden dat deze gegevens op enig moment door de OvJ kunnen worden gevorderd.

Het bezwaar tegen deze redenering is dat het toch ook een feit van algemene bekendheid is dat uit camerabeelden van herkenbare natuurlijke personen in veel gevallen reeds zonder meer de rasgegevens zijn af te leiden, alsmede dat, zoals de Hoge Raad benadrukte, dergelijke gegevens moeten worden aangemerkt als gevoelige gegevens in de zin van artikel 126nd lid 2 Sv. En daaraan doet niet af dat het mogelijk een feit van algemene bekendheid is dat deze beeldopnamen worden gemaakt. Als uit de beeldopnamen huidskleur en andere raskenmerken blijken, dan gaat het om rasgegevens, ongeacht de bekendheid met de mogelijkheid dat die opnamen worden gemaakt.

3.4 *Nog een pintransactie (Rb. Rotterdam 19 mei 2010, LJN BM5003)*

Ook de Rechtbank Rotterdam moest zich uitlaten over de vraag of de camerabeelden, gemaakt bij een geldautomaat in het kader van een pintransactie, moeten worden aangemerkt als rasgegevens. Evenals het Hof Den Haag in de hiervoor besproken zaak (*LJN* BM8433) kent de rechtbank betekenis toe aan de omstandigheid dat het een feit van algemene bekendheid is, en dus voor de desbetreffende gebruiker van de pinautomaat duidelijk moet zijn geweest, dat er van hem opnamen werden gemaakt:

'De camerabeelden die de officier van justitie wenst te verkrijgen zijn gemaakt tijdens één (of meerdere) pintransactie(s). Feit van algemene bekendheid is dat pintransacties uit oogpunt van beveiliging/veiligheid door beveiligingscamera's worden opgenomen. Dat er opnames plaatsvinden wordt tijdens de pintransactie ook kenbaar gemaakt op de pinautomaat. Voor de gebruiker van een pinautomaat is derhalve volstrekt helder dat opnamen worden gemaakt en is voorts ook duidelijk met welk doel dat wordt gedaan.'

Vervolgens geeft de rechtbank een eigen toepassing van dit criterium van algemene bekendheid. Aan de hand daarvan beredeneert de rechtbank dat voor deze bekend veronderstelde opnamen impliciet toestemming is gegeven. Vanwege de aldus veronderstelde toestemming meent de rechtbank dat de gevoeligheid van het gegeven is 'prijsgegeven', zodat er geen sprake is van een 'indringende inbreuk op de persoonlijke levenssfeer' van de gebruiker van de betaalautomaat. Omdat de betrokkene bekend wordt met de mogelijkheid dat er opnamen van hem worden gemaakt:

'[…] kan niet worden volgehouden dat wanneer deze gegevens voor de opsporing worden gevorderd en gebruikt sprake is van gegevens die vanwege hun aard een indringende inbreuk kunnen maken op de persoonlijke levenssfeer van de betrokkenen. Immers, door de impliciete toestemming van de betrokkene tot de opname van het camerabeeld, in het kader van het voor de betrokkenen kenbare doel, is de gevoeligheid van het gegeven prijsgegeven. Derhalve zijn deze gegevens niet (meer) te beschouwen als gevoelige gegevens in de zin van artikel 126nd lid 2, derde volzin Sv die met de in artikel 126nf Sv voorgeschreven waarborgen moeten worden beschermd.'

Deze redenering is onnavolgbaar. Of een foto of beeldopname heeft te gelden als 'bijzonder' of 'gevoelig' gegeven in de zin van artikel 126nd lid 2 Sv en artikel 16 en 18 Wbp, is niet afhankelijk van door wie dan ook gegeven toestemming. Als uit beeldopnamen het ras van de gefotografeerde blijkt, dan betreft het een gegeven van het ras en niet valt in te zien waarom toestemming voor het maken van de beeldopnamen daaraan iets zou kunnen veranderen.

Evenmin valt trouwens in te zien dat het gebruik van de beeldopname, vanwege de veronderstelde toestemming, geen indringende inbreuk meer zou kunnen maken op de persoonlijke levenssfeer van de betrokkene. Er kan hooguit worden gezegd dat deze inbreuk, vanwege de gegeven toestemming, is toegestaan. Trouwens, als er sprake is van uitdrukkelijke toestemming van de betrokkene[21] is wellicht niet eens een informatievordering in de zin van artikel 126nd of 126nf Sv nodig.

3.5 *En nog een pintransactie (Hof Arnhem 3 juni 2010, LJN BM6941)*

Ook het Gerechtshof Arnhem moest zich uitlaten over beeldopnamen gemaakt door een bank bij pintransacties. Evenals de Rechtbank Rotterdam in de hiervoor besproken zaak, kent het gerechtshof beslissende betekenis toe aan de algemene bekendheid met aanwezigheid van videocamera's bij betaalautomaten:

'Deze zaak verschilt op essentiële punten van de kwestie die aan de orde was in het zo-even genoemde arrest van de Hoge Raad. Het gaat immers om beelden die (anders dan in het geval van de Hoge Raad) niet aan [de bank] waren toevertrouwd, maar om een opname van een beveiligingscamera waarvan de aanwezigheid op allerlei plekken in de publieke ruimte en in het bijzonder bij pinautomaten van algemene bekendheid is.'

In aanvulling daarop gaat het gerechtshof uit van enkele eigen criteria. Zo acht het hof van belang de wijze waarop de gegevens zijn verkregen en zijn verwerkt:

'Om meer of anders dan een foto- of videoregistratie van de (bij een duidelijke opname voor het bewijs bruikbare) fysionomie van degene die voor een bepaalde geldtransactie van de pinautomaat in kwestie gebruik heeft gemaakt, gaat het hier niet. Van een (aan de beelden of de

21 Vgl. artikel 23 lid 1 onder a Wbp.

opnamen daarvan) voorafgegane verwerking van gevoelige persoonsgegevens als bedoeld in artikel 16 Wet bescherming persoonsgegevens, is bij deze registratie geen sprake geweest.'

Het gerechtshof lijkt te erkennen dat in deze zaak de persoon die gebruikmaakte van een pinautomaat herkenbaar in beeld is gebracht, want op zodanige wijze dat dit voor bewijs bruikbaar is. Op zichzelf duidt dit erop dat er, uitgaande van het arrest van de Hoge Raad, sprake is van gevoelige rasgegevens. Echter, dan stelt het hof dat er bij de videoregistratie, of daaraan voorafgaand, geen sprake is of is geweest van verwerking van gevoelige persoonsgegevens.

Het lijkt erop dat het hof bedoelt te zeggen dat er wél sprake is van verwerking van persoonsgegevens, maar niet van gevoelige persoonsgegevens. Dit omdat bij de videoregistratie alleen sprake is van beeldopnamen waaruit de fysionomie[22] van de betrokken persoon blijkt. Echter, uitgaand van de rechtsopvatting van de Hoge Raad in zijn arrest, valt niet in te zien waarom gegevens waaruit de fysionomie van die persoon blijkt, niet als gevoelige gegevens zouden moeten worden aangemerkt. Onduidelijk is hoe uit de gelaatstrekken van een herkenbare persoon geen raskenmerken zouden blijken (een silhouet misschien?).

Het zou ook kunnen dat het hof bedoeld heeft te zeggen dat er geen sprake is van 'verwerking'. Maar dat zou evident een onjuiste rechtsopvatting zijn. Volgens de definitie van artikel 1 onder b Wbp valt daaronder alles (jazeker: alles[23]) wat met persoonsgegevens kan worden gedaan. Oftewel: het verzamelen, vastleggen, ordenen, bewaren, opvragen, raadplegen, enzovoorts, en alle andere handelingen met betrekking tot persoonsgegevens die denkbaar zijn. Ook het vastleggen en bewaren van de beeldopnamen zijn verwerkingshandelingen in de zin van de Wbp.[24]

3.6 *In een Rotterdams metrostation (Rb. Haarlem 11 juni 2010, LJN BM7440)*

De politierechter van de Rechtbank Haarlem moest oordelen over een zaak waarin de OvJ met een beveiligingscamera gemaakte opnamen had gevorderd die in twee metrostations in Rotterdam waren gemaakt. Evenals de hiervoor besproken zaken ziet deze politierechter essentiële verschillen met de zaak waarop het arrest van de Hoge Raad betrekking had. Van belang acht hij allereerst de doeleinden waarvoor de gegevens zijn vastgelegd en opgevraagd.

'Er blijken in die zaak [waar het arrest van de Hoge Raad op zag] dus gegevens opgevraagd te zijn die door een betrokkene aan een instelling of instantie zijn afgestaan met een ander doel dan waarvoor zij door de officier van justitie in die zaak werden gevorderd.'

De politierechter lijkt hier, evenals de Zutphense politierechter in het hiervoor besproken vonnis (*LJN* BM1196), te willen zeggen, dat anders dan bij het arrest van de Hoge Raad, de beeldopnamen in de haar voorgelegde zaak worden gebruikt voor het doel waarvoor deze zijn gemaakt. In de zaak waarover de Hoge Raad oordeelde waren de foto's door de gefotografeerden aan het OV-bedrijf verstrekt om een OV-chipkaart te verkrijgen, terwijl het in de aan deze politierechter voorgelegde zaak ging om opnamen van beveiligingscamera's. Maar, evenals in de Zutphense zaak, is het doel waarvoor de gegevens zijn verstrekt of gevorderd niet bepalend voor de kwalificatie daarvan als gevoelige gegevens. Of het gebruik van de opnamen al dan niet onverenigbaar is met het verzameldoel[25] doet niet af aan het bijzondere, gevoelige karakter ervan. Zowel bij verenigbaar als bij onverenigbaar gebruik kunnen huidskleur, haartype en andere raskenmerken uit de beeldopnamen blijken.

Ook acht de Haarlemse politierechter het van belang dat er in het geval van het arrest van de Hoge Raad niet alleen beeldopnamen werden opgevraagd, maar ook naam- en adresgegevens:

'Bovendien waren door het opvragen van de naam en adresgegevens met de daarbij behorende foto gevoelige gegevens zoals ras direct te koppelen aan een betrokkene.'

Het belang daarvan houdt verband met de identificeerbaarheid. De politierechter kent betekenis toe aan de wijze waarop en het doel waarvoor de beeldopnamen worden gemaakt. Een en ander leidt ertoe dat er, volgens de politierechter, niet kan worden uitgegaan van identificerende gegevens. Er is dan, zo begrijpen wij de politierechter, geen sprake van persoonsgegevens en al helemaal niet van bijzondere, gevoelige gegevens.

'Er wordt niet vanuit gegaan dat uit camerabeelden zonder meer gevoelige gegevens als ras kunnen worden afgeleid, ook al niet omdat vooraf onbekend is van welke personen beelden worden gemaakt. Daarmee zijn ze niet op voorhand te beschouwen als gevoelige gegevens. Vaak zal pas achteraf blijken wat uit de beelden valt af te leiden, of wat daarop al dan niet zichtbaar is. De kwaliteit is bovendien wisselend, de beelden zijn ook niet zelden zwart-wit. In dat opzicht kan de vergelijking gemaakt worden met het opvragen van de in de memorie van toelichting als voorbeeld genoemde financiële gegevens. Hiervan is ook pas achteraf vast te stellen dat zich tussen de gevraagde gegevens gevoelige gegevens (bijvoorbeeld betreffende schenkingen aan een levensbeschouwelijke organisatie) bevinden.'

---

22 Van Dale Hedendaags Nederlands (versie 2.0): *fy-sio-no-mie* (zie ook: fysiognomie): de fysionomie (vrouwelijk), de fysionomieën: gelaatsuitdrukking.
23 Vgl. artikel 1 onder b Wbp.
24 Vgl. Rb. Amsterdam (vzr.) 26 augustus 2004, *LJN* AQ7877.
25 Vgl. artikel 9 lid 1 en 2 Wbp.

Deze rechtsoverweging is – en dat is eigenlijk voor het eerst in dit overzicht van uitspraken – goed te volgen. Zolang het niet zonder onevenredige inspanning mogelijk is om aan de hand van de beeldopnamen de identiteit te achterhalen van desbetreffende personen, is er geen sprake van persoonsgegevens[26] en al helemaal niet van bijzondere, gevoelige persoonsgegevens. De vraag is echter of daarvan in het onderhavige geval kan worden uitgegaan. Niet alleen zal de bedoeling van beveiligingscamera's waarschijnlijk wel zijn om, als dat nodig is, de personen aan de hand van de opnamen te identificeren, maar ook is de technologie om beeldopnamen geautomatiseerd te herkennen algemeen, en zeker voor opsporingsdiensten, al beschikbaar.[27] Interessant is trouwens ook dat deze uitleg van het begrip persoonsgegevens ingaat tegen de door sommige toezichthouders (in een andere context) verdedigde opvatting dat identificeerbaarheid al heel snel moet worden verondersteld.[28]

In aanvulling daarop introduceert de politierechter nog nieuwe, eigen criteria, zoals met betrekking tot wat zij noemt de 'Schutznorm':

'Daar komt bij dat deelname aan het maatschappelijk verkeer een zekere inbreuk op de privacy met zich mee brengt, waarbij niet altijd sprake is van schending van een "Schutznorm". Naar het oordeel van de politierechter is daarvan sprake bij beelden van een camera door een bedrijf ter beveiliging van dat bedrijf geplaatst. De filmbeelden zijn immers niet door de verdachte afgegeven om op een zorgvuldige wijze in een of ander systeem op te laten slaan conform de Wet bescherming persoonsgegevens. Hierin verschilt de onderhavige zaak dan ook wezenlijk van het door de Hoge Raad bij arrest van 23 maart 2010 beslechte geschil.'

Deze overwegingen kunnen we niet goed plaatsen. Zowel artikel 126nd en 126nf Sv als artikel 16 en 18 Wbp beogen een waarborg te bieden tegen het te lichtzinnig gebruik van gegevens waaraan, in termen van privacy, bijzondere risico's zijn verbonden, zoals gegevens betreffende iemands ras. En de Hoge Raad zag in elk geval nadrukkelijk geen aanleiding om de in de beide wetten gehanteerde begrippen verschillend uit te leggen. Integendeel, voor de uitleg van het in artikel 126nf Sv gebruikte begrip ging de Hoge Raad juist uit van de parlementaire geschiedenis van artikel 16 en 18 Wbp. En dat duidt er toch op dat de in beide wetten gebruikte begrippen op eenzelfde wijze moeten worden uitgelegd en tegen de achtergrond van wetten met eenzelfde bedoeling.

Maar het gaat de politierechter in deze overweging wellicht niet zozeer om de bescherming die de beide wetten beogen te bieden, maar veeleer om de verschillende doeleinden waarvoor de gegevens in de beide zaken zijn verkregen. Ook voor deze Haarlemse politierechter – evenals voor haar collega uit Zutphen en voor het Hof Den Haag – is dan beslissend dat in de zaak van de Hoge Raad de gegevens door de betrokkenen zelf waren verstrekt om een OV-kaart te verkrijgen, terwijl het in de haar voorgelegde zaak ging om beelden gemaakt met beveiligingscamera's. Echter, zoals gezegd, dat is niet relevant voor de uitleg van het begrip 'rasgegevens'. Waar het om gaat is of uit de beeldopnamen gegevens betreffende iemands ras kunnen worden afgeleid, niet om welke redenen deze opnamen zijn gemaakt.

Ten slotte gaat de politierechter nog in op de wijze waarop de gegevens zijn verkregen en de voorzienbaarheid daarvan, alsmede de afweging van privacy- en opsporingsbelangen:

'Eén en ander kan anders zijn indien voorzienbaar is dat er gevoelige gegevens zijn geregistreerd. Gelet op het voorgaande gaat het echter te ver er op voorhand vanuit te gaan dat camerabeelden, zoals hiervoor bedoeld, gevoelige gegevens bevatten en dus onder het regime van artikel 126nf Wetboek van Strafvordering vallen. Daarmee zou ook het evenwicht tussen de diverse belangen, zoals het individuele belang bij bescherming van de persoonlijke levenssfeer en het algemene belang bij opsporing van strafbare feiten, verstoord zijn.'

Deze rechtsoverwegingen over de voorzienbaarheid van de vastlegging van gevoelige gegevens lijken tegemoet te komen aan de mogelijke en niet-denkbeeldige situatie dat de OvJ niet had kunnen vermoeden dat uit de gevorderde beeldopnamen rasgegevens zouden kunnen blijken. En dan kan mogelijk worden betoogd dat die vordering geen betrekking had op gegevens betreffende iemands ras. Echter, zoals hiervoor opgemerkt bij de bespreking van het vonnis van de Zutphense politierechter (*LJN* BM1196) is het niet zonder meer geloofwaardig dat daarvan sprake is als er beelden van een beveiligingscamera worden gevorderd.

Ook mogelijk is dat deze overwegingen aansluiten bij de door het Hof Den Haag en de Rechtbank Rotterdam (*LJN* BM8433 resp. *LJN* BM5003) geïntroduceerde nieuwe criteria die uitgaan van het feit van algemene bekendheid dat er in voorkomende gevallen beeldopnamen worden gemaakt. Zoals bij de bespreking van deze zaken al aangegeven, valt niet in te zien dat die criteria betekenis hebben voor de kwalificatie van de beeldopnamen als gegevens betreffende iemands ras. Als uit de opnamen huidskleur, vorm van de ogen of neus, of anderszins

26 *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 15, 47-49; zie ook annotatie van M. Voulon bij ABRvS 8 maart 2006, *LJN* AV3911, in T.E. van Dijk e.a. (red.), *Uitsprakenbundel. Wet bescherming persoonsgegevens*, Den Haag 2009, nr. 1.1.

27 Inmiddels blijkt RET al gezichtsherkenningsprogrammatuur op de trams in te zetten, zie 'Gezichtsherkenning op tram om criminelen te weren omstreden', *Trouw* 20 augustus 2010. Overigens worden veel consumentencomputers (o.a. Apple iMac) en digitale fototoestellen (o.a. Canon Ixus) standaard geleverd met gezichtsherkenningsprogrammatuur. Deze leggen een verband tussen dezelfde personen die op verschillende foto's te zien zijn. Daarmee is al snel sprake van identificeerbaarheid.

28 Artikel 29 WG, Opinion 4/2007 on the concept of personal data, (WP136) 20 november 2007; Artikel 29 WG, Opinion 1/2008 on data protection issues related to search engines, (WP148) 4 april 2008; daarover G.-J. Zwenne, 'Over persoonsgegevens en IP-adressen, en de toekomst van privacywetgeving', in: Mommers et al. (red.), *Het binnenste buiten*, liber amicorum prof. Aernout Schmidt, Leiden 2010, p. 321-341.

rasgegevens blijken met betrekking tot identificeerbare natuurlijke personen, dan zijn het bijzondere en gevoelige gegevens, ongeacht of die beeldopnamen voorzienbaar waren. Verder komt het ons voor dat artikel 126nd en 126nf Sv überhaupt geen belangenafweging toelaten.

3.7 *In het café (Rb. Amsterdam 5 juli 2010, LJN BN1025)*

De Rechtbank Amsterdam heeft recent uitspraak gedaan in een zaak over een zware mishandeling, waarin in een café gemaakte camerabeelden waren opgevraagd zonder machtiging van de rechter-commissaris. Ook deze rechtbank komt tot de conclusie dat in het hem voorgelegde geval uit de gevorderde opnamen géén rasgegevens *kunnen* worden afgeleid. Hij overweegt daartoe allereerst dat alleen deze opnamen zijn gevorderd, en niet ook naam- en adresgegevens:

'Daarbij is allereerst van belang dat hier, anders dan in het hiervoor genoemde arrest van de Hoge Raad, geen samenstel van gegevens is gevorderd waaruit, door de gestructureerd verwerkte combinatie van "naw-gegevens" met bijbehorende afbeelding, het ras van een door de verstrekte gegevens te identificeren persoon kan worden afgeleid. De vordering ziet immers slechts op de met een camera in café [naam] opgenomen beelden, waarop niet meer is te zien dan een weergave van een bepaalde stand van zaken die zich op enig moment in die voor het publiek toegankelijke ruimte heeft voorgedaan. Meer in het bijzonder geldt daarbij dat de beelden niet meer of andere informatie bevatten dan hetgeen door iedere willekeurige op dat moment in het café aanwezige omstander ook had kunnen worden waargenomen, terwijl de beelden ook niet meer of andere informatie bevatten omtrent een van de daarop waar te nemen personen. […]

Het achterliggende doel voor het plaatsen van dergelijke camera's is beveiliging, niet identificatie op zich. Er worden ook geen namen gekoppeld aan de beelden. Daarmee vindt de verwerking – dat wil zeggen opslag – tegen een geheel andere achtergrond plaats dan wanneer het gaat om foto's in een leden- of personeelsadministratie dan wel een registratiesysteem voor houders van bepaalde passen, zoals in de wetsgeschiedenis ten voorbeeld gesteld. Vooraf is onbekend van welke personen beelden worden gemaakt.'

Voor zover het gaat om de identificeerbaarheid is dit nog te volgen. Als het gaat om alleen beeldopnamen is het denkbaar dat het niet, althans niet zonder onevenredige inspanning, mogelijk is om de cafébezoekers aan de hand daarvan te identificeren. Maar zoals gezegd kan daar, gelet op de toenemende mogelijkheden om beeldopnamen geautomatiseerd te herkennen, niet al te gemakkelijk van uit worden gegaan.[29]

De enkele omstandigheid dat het om een publieke ruimte gaat, is niet relevant als het gaat om de kwalificatie van de gegevens. Hetzelfde geldt met betrekking tot de omstandigheid dat iedere willekeurig in deze ruimte aanwezige omstander heeft kunnen waarnemen wat op de beeldopnamen is vastgelegd. Er kan ook sprake zijn van gevoelige rasgegevens als de opnamen zijn gemaakt in een voor het publiek toegankelijke ruimte of als anderen daarvan kennis kunnen nemen.

Interessant is nog wel de verwijzing van de rechtbank naar de antwoorden van de Minister van Justitie op kamervragen[30] naar aanleiding van het arrest van de Hoge Raad:

'Op de [kamer]vraag of deze uitspraak gevolgen kan hebben voor de werkwijze van de politie bij het opvragen van camerabeelden, en de rechter-commissaris niet onnodig en belemmerend moet worden ingeschakeld, heeft de minister het volgende geantwoord: "Ik sta op het standpunt dat deze uitspraak niet de in de vraag bedoelde gevolgen heeft. Beelden van particuliere bewakingscamera's zijn naar mijn oordeel van een andere aard dan een bestand met pasfoto's en daaraan gekoppelde andere persoonsgegevens. […] In geval van bewakingscamera's is vooraf onbekend of en van welke personen beelden worden gemaakt en wat daarop wel of niet zichtbaar zal zijn. Ook zijn daarbij geen andere persoonsgegevens bekend. Dergelijke camerabeelden worden om die reden bij de toepassing van de Wet bescherming persoonsgegevens niet als bijzondere (de rechtbank begrijpt: gevoelige) persoonsgegevens gezien."'

Dit autoriteitsargument overtuigt niet. De minister ontkent niet dat de camerabeelden persoonsgegevens zijn, maar stelt alleen dat het geen *bijzondere* of *gevoelige* gegevens zijn. Er zou dan dus wel sprake zijn van identificeerbaarheid, maar niet van gegevens betreffende iemands ras. Dat lijkt moeilijk houdbaar in het licht van de bedoeling van de wetgever zoals deze blijkt uit de parlementaire geschiedenis. Er valt niet in te zien dat iemand aan de hand van camerabeelden wel kan worden geïdentificeerd, zonder dat daarmee ook rasgegevens duidelijk worden. Het standpunt van de minister lijkt dan ook niet zozeer te zijn gebaseerd op een analyse van het arrest van de Hoge Raad en de relevante wettelijke bepalingen, maar veeleer te zijn ingegeven door de gedachte dat het wel heel ongelukkig zou zijn als de foto's en beeldopnamen inderdaad worden aangemerkt als gevoelige en bijzondere gegevens, zoals de Hoge Raad doet.

3.8 *Weer in een metrostation (Rb. Rotterdam 22 juli 2010, LJN BN3338 en BN3336)*

In het voorgaande is al een uitspraak van de Rechtbank Rotterdam (*LJN* BM5003) besproken waarin beeldopnamen niet werden aangemerkt als gegevens betreffende ras, onder andere omdat het een feit van algemene bekendheid was dat deze opnamen worden gemaakt. Iets

29 Zie voetnoot 25 van deze bijdrage.

30 *Aanhangsel Handelingen II* 2009/10, nr. 2724: antwoord van Minister van Justitie d.d. 24 juni 2010 op kamervragen betreffende de uitleg van het arrest van de Hoge Raad van 23 maart 2010.

meer dan twee maanden later komt deze rechtbank weer met een andere redenering die, voor wie bekend is met de Wbp, heel bijzonder is omdat daarin een nieuwe betekenis wordt toegekend aan het Vrijstellingsbesluit.[31] De rechtbank zegt het zo:

'Zogenaamde bijzondere persoonsgegevens mogen op grond van artikel 16 van de Wbp in beginsel niet worden verwerkt. Op grond van artikel 38 van het Vrijstellingsbesluit Wbp is de RET bevoegd om geautomatiseerde video-opnamen te maken van haar stations en deze beelden vast te leggen. Gesteld noch gebleken is dat vastlegging niet voldoet aan de eisen die het Vrijstellingsbesluit daaraan stelt. Anders dan door de raadsman is betoogd is er dan ook een wettelijke basis voor het maken van de camerabeelden.

Uit artikel 29 Wbp gelezen in samenhang met artikel 38 van het Vrijstellingsbesluit Wbp volgt dat beelden verkregen door middel van videocameratoezichtbeelden zonder verdere persoonsgegevens geen persoonsgegevens zijn als bedoeld in artikel 16 van de Wbp.

Nu deze beelden geen gevoelige gegevens bevatten als bedoeld in artikel 126nf van het Wetboek van Strafvordering, hadden deze beelden op grond van artikel 126nd van deze wet door de officier gevorderd kunnen worden, zonder voorafgaande machtiging van de rechter-commissaris.'

Deze rechtsoverweging berust op een paar misverstanden. Allereerst biedt het Vrijstellingsbesluit geen wettelijke basis voor het maken van camerabeelden, maar geeft dit besluit alleen een opsomming van de verwerkingen die zijn uitgezonderd van de meldplicht van artikel 27 Wbp. Verder doet deze vrijstelling uiteraard niet af aan de toepassing van de wet als zodanig en van de andere verplichtingen die daaruit voortvloeien. En al helemaal brengt deze vrijstelling niet mee dat er *geen* sprake zou (kunnen) zijn van gevoelige gegevens als bedoeld in artikel 126nf Sv, die alleen met machtiging van de rechter-commissaris mogen worden gevorderd.

In aanvulling daarop, wellicht als overweging ten overvloede, merkt de rechtbank op dat in dit geval de beelden vrijwillig zijn afgegeven en dus niet op basis van een vordering van de OvJ:

'In dit geval zijn de beelden niet gevorderd maar op grond van een overeenkomst tussen de RET en de politie verstrekt, zodat van een vrijwillige afgifte sprake is. De door de RET afgegeven beelden kunnen voor het bewijs worden gebruikt, evenals de resultaten van het onderzoek die uit het gebruik van deze beelden voortkomen.'

Ook dit argument overtuigt niet. Als er sprake is van wettelijke gegevensvorderingsbevoegdheden (i.c. artikel 126nd en 126nf Sv) kan en mag de OvJ daaraan niet zomaar voorbijgaan door deze gegevens op vrijwillige basis aan zich te doen verstrekken en/of door een overeenkomst aan te gaan met degene die kan beschikken over deze gegevens.[32] Overigens duidt deze 'vrijwillige verstrekking' erop dat de RET mogelijk in strijd heeft gehandeld met de Wbp, omdat deze wet slechts onder heel beperkte voorwaarden verstrekking van dergelijke persoonsgegevens toestaat.[33]

3.9 *In de supermarkt (Rb. Arnhem 3 augustus 2010, LJN BN2280)*

Ook de Rechtbank Arnhem moest zich een oordeel vormen over opnamen gemaakt met beveiligingscamera's. De rechtbank volgt, in taalgebruik en overwegingen, het al besproken arrest Gerechtshof Arnhem 3 juni 2010 (*LJN* BM6941). We volstaan met het aanhalen van de overwegingen, waarin vooral belang wordt gehecht aan achtereenvolgens: het doel waarvoor de opnamen zijn gemaakt, de omstandigheid dat dit in de publieke ruimte is gedaan en dat het een feit van algemene bekendheid is dat dergelijke opnamen worden gemaakt.

Anders dan in het arrest van de Hoge Raad ging het, volgens deze rechtbank, in dit geval om opnamen:

'…van beveiligingscamera's waarvan de aanwezigheid op allerlei plekken in de publieke ruimte en in het bijzonder bij pinautomaten en supermarkten van algemene bekendheid is. Om meer of anders dan een foto- of videoregistratie van de (bij een duidelijke opname voor het bewijs bruikbare) fysionomie van degene die een supermarkt heeft bezocht of voor een bepaalde geldtransactie van een pinautomaat gebruik heeft gemaakt, gaat het hier niet. Van een (aan de beelden of de opnamen daarvan) voorafgegane verwerking van gevoelige persoonsgegevens als bedoeld in artikel 16 Wet bescherming persoonsgegevens, is bij deze registratie geen sprake geweest. Het verbod van artikel 18 van die wet doet zich (daarom) evenmin gelden.'

We kunnen hier kort over zijn. Onder verwijzing naar wat we bij het voornoemde arrest van het Gerechtshof Arnhem al opmerkten, komt ons ook dit oordeel onbegrijpelijk voor.

3.10 *Bij een tankstation (Rb. Alkmaar 5 augustus 2010, LJN BN3312)*

De meest recente door ons gevonden uitspraak is van de Rechtbank Alkmaar en betrof ook opnamen van beveiligingscamera's. De rechtbank kent, net als de Haarlemse politierechter en het Gerechtshof Den Haag, betekenis toe aan de omstandigheid dat, anders dan in de zaak

31 *Stb*. 2001, 250.

32 Aanwijzing opsporingsbevoegdheden van het College van Procureurs-Generaal, 11 november 2004, § 2.12.6, p. 11; *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 1-3; daarover Mevis in zijn noot bij het arrest in *NJ* 2010, 355 en Wisman in haar noot bij Rb. Rotterdam 2 juni 2008, *Computerrecht* 2009, 4; in dat verband ook Rb. Arnhem 21 juni 2010, *LJN* BM8534, Rb. Amsterdam 5 juli 2010, *LJN* BN1025 en Rb. Breda 29 juli 2010, *LJN* BN3637.

33 Vgl. artikel 16 jo. 18 of 23 Wbp: zie echter Rb. Breda 29 juli 2010, *LJN* BN3637.

waarop het arrest van de Hoge Raad betrekking had, in de hem voorgelegde zaak de gevorderde beeldopnamen niet door de betrokkene zelf waren verstrekt maar waren opgenomen met beveiligingscamera's. Ook acht deze rechtbank van belang dat het een feit van algemene bekendheid is dat de opnamen worden gemaakt:

'Het gaat […] om een beeldopname van een beveiligingscamera in een publieke ruimte waarvan de aanwezigheid in winkels en tankstations een feit van algemene bekendheid is. De beelden betreffen een weergave van hetgeen zich afspeelt in de publieke ruimte. Een ieder die zich daar bevindt weet of kan redelijkerwijs weten dat hij of zij gefilmd kan worden en met welk doel er wordt gefilmd. Er worden ook geen namen gekoppeld aan personen die in beeld gebracht worden. Het achterliggende doel van het maken van dergelijke camerabeelden is immers beveiliging teneinde deze indien nodig te gebruiken ten behoeve van opsporing en vervolging.'

Op basis van een en ander komt ook deze rechtbank tot het oordeel dat er geen sprake was van gevoelige gegevens. Alleen voor zover de rechtbank bedoeld heeft te zeggen dat er geen sprake zou zijn van identificeerbaarheid – niet waarschijnlijk maar misschien niet uit te sluiten – is dit te volgen. Voor de rest is ook deze uitspraak moeilijk te begrijpen.

3.11 *Kernpunten*

Instantie	Datum en LJN	Kerngezichtspunten van de uitspraken
Hoge Raad	23 maart 2010 *LJN* BK6331	Een machtiging van de rechter-commissaris is vereist voor vorderen naw-gegevens en foto's van reizigers aangezien de foto's bijzondere persoonsgegevens (kunnen) bevatten
Rechtbank Zutphen	15 april 2010 *LJN* BM1196	Verzameling van bijzondere persoonsgegevens (i.c. rasgegevens) valt niet binnen het doel van het cameratoezicht, en het als bijkomstigheid achteraf kunnen verwerken van gegevens betreffende ras op basis van camerabeelden doet niet af aan rechtmatige toepassing van artikel 126nd Sv
Hof Den Haag	6 mei 2010 *LJN* BM8433	Algemene bekendheid van aanwezigheid camera's bij geldautomaten maakt dat bij de verwerking van beelden geen sprake is van inbreuk op bescherming persoonsgegevens
Rechtbank Rotterdam	19 mei 2010 *LJN* BM5003	Algemene bekendheid van aanwezigheid camera's bij geldautomaten maakt geen inbreuk op bescherming persoonsgegevens door impliciete toestemming van de betrokkenen
Hof Arnhem	3 juni 2010 *LJN* BM6941	Bij de opname van gelaatstrekken is geen sprake van, of niet noodzakelijkerwijs sprake van, verwerking van gevoelige gegevens
Rechtbank Haarlem	11 juni 2010 *LJN* BM7440	Het doel van de verstrekking van (bijzondere) persoonsgegevens is bepalend voor de rechtmatigheid van de vordering De mate van identificeerbaarheid is bepalend voor de rechtmatigheid van de verwerking Beelden die bijvoorbeeld ter beveiliging van een bedrijfspand zijn gemaakt, vallen niet onder het beschermingsbereik van de Wbp, omdat zij niet initieel op initiatief van de verdachte ter verwerking zijn afgestaan
Rechtbank Amsterdam	5 juli 2010 *LJN* BN1025	Onevenredige inspanning te leveren ter identificatie van degenen die in beeld gebracht zijn, maakt dat geen sprake is van (bijzondere) persoonsgegevens Er is geen samenstel van gegevens gevorderd waaruit ras en identiteit van een persoon kunnen worden afgeleid Het doel van de gegevensverwerking die volgt uit de plaatsing van camera's is beveiliging, niet identificatie
Rechtbank Rotterdam	22 juli 2010 *LJN* BN3338 en BN3336	Beelden verkregen door middel van videocameratoezichtbeelden zonder verdere persoonsgegevens zijn geen persoonsgegevens als bedoeld in artikel 16 Wbp De beelden zijn vrijwillig verstrekt aan de politie, zodat een machtiging op basis van artikel 126nf Sv niet nodig was
Rechtbank Arnhem	3 augustus 2010 *LJN* BN2280	Bij de opname van gelaatstrekken is geen, of niet noodzakelijkerwijs sprake van, verwerking van gevoelige gegevens
Rechtbank Alkmaar	5 augustus 2010 *LJN* BN3312	Beelden verkregen door middel van videocameratoezichtbeelden zonder verdere persoonsgegevens zijn geen persoonsgegevens als bedoeld in artikel 16 Wbp

Tabel. Kernpunten van de behandelde uitspraken

4 Afsluiting

Wat van dit alles te vinden? Er is, zoveel is wel duidelijk, sprake van een serieus te nemen probleem met betrekking tot de kwalificatie van foto's en beeldopnamen als 'gevoelige' of 'bijzondere' gegevens. Er kan niet meer worden gesproken van een enkel bedrijfsongeval of incident als eerst de privacytoezichthouder (CBP) in zijn richtsnoeren en later maar liefst zeven verschillende rechterlijke instanties uitgaan van een begripsbepaling die in niet geringe mate lijkt af te wijken van wat de wetgever volgens ons hoogste rechtscollege heeft bedoeld. De geschetste ontwikkeling in de lagere rechtspraak degradeert een uitspraak van de Hoge Raad bijna tot de uitzondering op de regel.

Het arrest van de Hoge Raad heeft consequenties die kennelijk in veel gevallen maatschappelijk onnodig en ongewenst worden gevonden. Waar het gaat om gegevensverwerkingen met beperkte privacyrisico's kan wellicht begrip worden opgebracht voor de pogingen om deze consequenties 'weg' te redeneren. Het is niet helemaal zonder reden dat het CBP probeert de meest alledaagse en onschuldige verwerkingen van foto's en beeldopnamen buiten het domein van de gevoelige of bijzondere gegevens te brengen. Een socialenetwerksite of een intranetsmoelenboek is niet van dezelfde orde als een etnische registratie en het komt inderdaad overdreven voor om met betrekking tot de eerste toepassingen dezelfde waarborgen te verlangen als voor de laatste. Echter, hoe overdreven ook, dit is het gevolg van een uitdrukkelijke keuze van de wetgever, wiens rechtsvormende taakuitoefening democratisch is gelegitimeerd. In een democratische rechtsstaat als de onze is het niet aan de toezichthouder om daaraan voorbij te gaan, ook niet door wat wordt genoemd een 'redelijke wetstoepassing'.

Eenzelfde opmerking kan worden gemaakt waar het gaat om het door strafrechters 'weg' redeneren van de waarborg van rechterlijke machtiging van artikel 126nd en 126nf Sv. Ook daarvoor valt enig begrip op te brengen, maar toch niet heel veel. Als aan de hand van beeldopnamen is vastgesteld dat een verdachte het ten laste gelegde heeft begaan, wil geen rechter het op zijn geweten hebben dat deze verdachte vrijuit gaat, omdat is nagelaten, of er geen mogelijkheid was, een rechterlijke machtiging te vragen.

Echter, ondanks het begrip dat er misschien is voor de beweegredenen, is het in beginsel niet aan de rechter om voorbij te gaan aan wat duidelijk uit de wet blijkt, namelijk dat voor het vorderen van gegevens betreffende iemands ras extra waarborgen in acht moeten worden genomen. Het gaat, zoals de Hoge Raad zelf wel zegt, de grenzen van de rechtsvormende taak van de rechter te buiten om eigenmachtig deze waarborgen weg te interpreteren. Het wettelijke vormvoorschrift van een rechterlijke machtiging bedoelt de toelaatbaarheid van overheidsingrijpen in iemands privésfeer *vooraf* te laten toetsen. En dat niet voor niets.

Inmiddels zou de praktische 'hinder' die de OvJ ondervindt van deze burgervriendelijke waarborgen beperkt moeten zijn. Als gevolg van de op 1 april 2010 in werking getreden wetgeving[34] is aan artikel 126nf Sv een derde lid toegevoegd, waarin artikel 126l lid 7 Sv van overeenkomstige toepassing wordt verklaard. Dit betekent dat 'bij dringende noodzaak' de machtiging van de rechtercommissaris (niet meer schriftelijk hoeft maar) nu mondeling kan worden verleend en vervolgens binnen drie dagen op schrift moet worden gesteld.

Als er niettemin toch nog sprake is van een maatschappelijk onaanvaardbaar probleem met betrekking tot de kwalificatie van beeldopnamen als bijzondere of gevoelige gegevens, dan is het uiteraard allereerst aan de wetgever om dat op te lossen.[35] En dat moet dan ook maar liever snel gebeuren. Al was het maar omdat het niet heel waarschijnlijk lijkt dat de Hoge Raad, als hem dat wordt gevraagd, de in deze bijdrage besproken lagere rechtspraak in stand laat.

34 *Stb*. 2009, 525 en *Stb*. 2010, 139.
35 In die zin ook Mevis in zijn noot bij het arrest in *NJ* 2010, 355.