Veiligheid en privacy

Jonge VAR-reeks
3

Veiligheid en privacy

Preadviezen uitgebracht door

Mr. N.M. Schröder
Mr. M.P.J.M. van Grinsven

Voor de bijeenkomst
van de Jonge VAR
op 5 november 2004

Boom Juridische uitgevers
Den Haag
2005

Aanbevolen citeerwijze: Jonge VAR-reeks 3

ISBN 90 5454 562 3
NUR 823
www.bju.nl

Inhoud

Ten geleide

Op 5 november 2004 is alweer de derde jaarlijkse bijeenkomst van de Jonge VAR gehouden, ditmaal bij de Raad van State in Den Haag. De bijeenkomst was inhoudelijk een groot succes (dat een groter aantal deelnemers zou hebben gerechtvaardigd). De preadviezen waren dit keer geschreven door Nynke Schröder, junior-docent aan de Universiteit Utrecht, en Thijs van Grinsven, jurist bij de Raad van State. Ze betroffen aspecten van het thema Veiligheid en privacy. Over hun standpunten is uitvoerig en geanimeerd van gedachten gewisseld en na deze discussie is gestemd over de stellingen die zij aan het eind van de preadviezen hadden opgenomen.

Dit boekje bevat de twee preadviezen en het verslag van de discussie, inclusief de uitslag van de stemming over de stellingen. Het verslag is beknopt, maar geeft de zakelijke inhoud van het gezegde goed weer. Het is samengesteld door Mathijs Raijmakers, werkzaam bij het ministerie van BZK. Het VAR-bestuur dankt de preadviseurs en de verslaglegger hartelijk voor hun inspanningen.

Lex Michiels,
voorzitter van de VAR

Veiligheid en privacy in de openbare ruimte

Mr. N.M. Schröder[*]

* Mevrouw mr. N.M. Schröder is als junior-docent werkzaam bij de disciplinegroep Staats- en Bestuursrecht van de Universiteit Utrecht.

1 Inleiding

De laatste jaren voelen mensen zich niet langer veilig op straat als gevolg van het toegenomen aantal incidenten van geweld en criminaliteit in de openbare ruimte. Zeven op de tien Nederlanders zijn daarbij, volgens een in 2002 uitgevoerd onderzoek van het Sociaal Cultureel Planbureau, van mening dat de overheid te weinig doet aan de bestrijding hiervan.[1] Volgens datzelfde onderzoek wenst ruim driekwart van de burgers dat de overheid krachtiger optreedt bij het bestrijden van criminaliteit en handhaving van de openbare orde.

Deze maatschappelijke onvrede leidde ertoe dat veiligheid in 2002 tijdens de verkiezingen een van de voornaamste speerpunten werd in de verkiezingscampagnes van veel partijen. In het beleid van het nieuwe kabinet vormt veiligheid dan ook één van de belangrijkste aandachtsgebieden. Met behulp van een omvangrijk veiligheidsprogramma wil het kabinet bereiken dat de (rechts)handhaving uiterlijk in 2006 weer goed functioneert en dat de veiligheid, zowel objectief als subjectief, toeneemt. In het kader van dit nieuwe beleid wil het kabinet gaan handhaven op een manier waarbij het optreden van de overheid meer zichtbaar is voor de burger.[2] Hierbij wordt onder andere gedacht aan het gebruik van bestaande maatregelen als preventief fouilleren en cameratoezicht op openbare plaatsen.[3]

Het (intensiever) gebruik van de bestaande maatregelen alleen is volgens het kabinet echter niet genoeg. Zo wordt de effectiviteit van het optreden van de overheid volgens het kabinet op dit moment ondermijnd doordat burgers zich kunnen onttrekken aan de verantwoordelijkheid voor hun handelen door tegen een opsporingsambtenaar of toezichthouder te liegen over hun identiteit. Om dit tegen te gaan wil het kabinet een uitgebreide identificatieplicht invoeren.[4]

Hoewel deze aandacht voor veiligheid positief is en de doelgerichte aanpak van onveiligheid bij grote delen van de bevolking positief is ontvangen, klinken er ook kritische geluiden. Een veelgehoord punt van kritiek is dat de overheid instrumenten gebruikt waarbij de vergroting van de veiligheid ten koste gaat van de privacy van de

1. Sociaal Cultureel Planbureau, Sociaal en Cultureel Rapport 2002. De kwaliteit van de quartaire sector, hoofdstuk 11, p. 28-29. Beschikbaar op www.scp.nl. Alle in deze bijdrage gebruikte internetbronnen zijn voor het laatste bezocht in de week van 10 tot en met 15 oktober 2004.
2. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Ministerie van Justitie, Naar een veiliger samenleving, Den Haag, oktober 2002, p. 19-20.
3. Bij cameratoezicht op openbare plaatsen zullen, wanneer het in dit preadvies centraal staande wetsvoorstel Cameratoezicht op openbare plaatsen wordt aangenomen, echter wel het gebruik en de voorwaarden voor het gebruik van het instrument veranderen.
4. Kamerstukken II 2003-2004, 29 218, nr. 1 en 2.

burger.[5] Van overheidszijde wordt met lichte irritatie op deze kritiek gereageerd. Privacybescherming wordt door met handhaving van regels belaste instanties veelal gezien als hinderlijk obstakel bij het uitoefenen van de overheidstaak. Zo kan het volgens minister Donner niet zo zijn dat je de veiligheid van velen opoffert aan de behoefte aan privacy van de één.[6] De Groningse korpschef drukte het nog iets sterker uit door het grondrecht op privacy onomwonden de schuilplaats van het kwaad te noemen.[7]

Het is in het kader van deze discussie interessant om te onderzoeken of de toepassing van de (voorgestelde) maatregelen inderdaad een ontoelaatbare inbreuk op het recht op privacy oplevert. In dit preadvies wordt dan ook de vraag besproken of de (voorgestelde) nationale regelgeving ten aanzien van cameratoezicht op openbare plaatsen, preventief fouilleren en de uitgebreide identificatieplicht voldoende waarborgen biedt om hun concrete toepassing te laten voldoen aan de eisen die het recht op privacy stelt.

Teneinde deze vraag te beantwoorden zal ik eerst in hoofdstuk 2 uiteenzetten wat de verschillende maatregelen inhouden en wat de relevante (voorgestelde) regelgeving ten aanzien van deze maatregelen inhoudt. In hoofdstuk 3 zal ik vervolgens nagaan of de toepassing van deze maatregelen leidt tot een beperking van het recht op privacy. Tot slot zal ik in hoofdstuk 4 onderzoeken of de eventuele beperkingen van het recht op privacy als gevolg van de toepassing van de maatregelen rechtmatig zijn in het licht van de eisen die relevante privacy-bepalingen stellen aan een gerechtvaardigde beperking van het recht op privacy.

---

5. CBP, Jaarverslag 2003, p. 11. Beschikbaar op www.CBPweb.nl, R. de Winter, Nieuwe criminaliteitsbestrijding, NJB 2002/36, p. 1806, Het Parool, 5 juli 2004, Nog even en de politie kijkt voortdurend mee, De Volkskrant, 15 mei 2004, 'Ze hebben toch maling aan zo'n camera'; In het gebied rond het station van Amsterdam en op de Wallen hangen sinds vrijdag 26 camera's, De Volkskrant, 9 februari 2004, Verantwoord voyeurisme; 'De publieke meningsvorming over privacy is aan het kantelen. Uit enquêtes blijkt dat veel makkelijker wordt gedacht over de schending van de privé-sfeer.'
6. R. de Winter, Nieuwe criminaliteitsbestrijding, NJB 2002/36, p. 1806.
7. CBP, Jaarverslag 2003, p. 11. Beschikbaar op www.CBPweb.nl.

2 De maatregelen en de relevante regelgeving

In dit hoofdstuk zal ik achtereenvolgens de maatregelen cameratoezicht op openbare plaatsen, preventief fouilleren en de uitgebreide identificatieplicht bespreken. Teneinde een duidelijk beeld te schetsen van deze maatregelen zal ik per maatregel eerst kort uitleggen wat deze inhoudt, vervolgens zal ik ingaan op de achtergrond van de maatregel en tot slot zal ik de relevante wettelijke regeling of het voorstel daartoe schetsen.

2.1 Cameratoezicht op openbare plaatsen

Sinds ongeveer vijf jaar wordt er in een toenemend aantal Nederlandse gemeenten gebruikgemaakt van het instrument cameratoezicht op openbare plaatsen om criminaliteit en overlast in de openbare ruimte terug te dringen en het gevoel van veiligheid te vergroten. Onder cameratoezicht wordt verstaan het gebruik van camera's ten behoeve van toezicht en beveiliging.[8] Dit toezicht wordt bewerkstelligd door het plaatsen van één of meer camera's met behulp waarvan vervolgens gebeurtenissen op straat geobserveerd kunnen worden.[9] De aldus geregistreerde beelden kunnen alleen bekeken worden, maar zij kunnen tevens worden vastgelegd.[10]

Op dit moment bestaat er geen algemeen geldende regeling voor het gemeentelijk cameratoezicht op openbare plaatsen. Teneinde een dergelijke regeling te creëren heeft het kabinet op 23 februari 2004 een voorstel ingediend tot wijziging van de Gemeentewet (Gem.w.) en de Wet Politieregisters (Wet Pol.r.).[11]

2.1.1 Achtergrond cameratoezicht op openbare plaatsen

Cameratoezicht wordt in de praktijk door een aantal gemeenten reeds gebruikt als hulpmiddel bij het handhaven van de openbare orde. De bevoegdheid voor het gebruik van camera's in de openbare ruimte wordt thans ontleend aan de bevoegdheden die de organen van de gemeente hebben op het gebied dat door de camera's wordt bestreken.[12]

---

8. Kamerstukken II 1997-1998, 25 760, nr. 1, p. 3.
9. Registratiekamer, In beeld gebracht, Onderzoeksrapport van 27 januari 1997, beschikbaar op www.CBPweb.nl.
10. Kamerstukken II 1997-1998, 25 760, nr. 1, p. 3.
11. Kamerstukken II 2003-2004, 29 440 nr. 1 en 2.
12. Kamerstukken II 1997-1998, 25 760, nr. 1, p. 24.

Zo is de burgemeester op grond van artikel 172 Gem.w. belast met de handhaving van de openbare orde. Op basis van het tweede lid van dit artikel is hij bevoegd overtredingen van wettelijke voorschriften die betrekking hebben op de openbare orde te beletten of te beëindigen. In het kader van dit preventie aspect, dat eveneens onderdeel uitmaakt van deze taak, kan de burgemeester de onder zijn gezag staande politie opdragen toezicht te houden op openbare plaatsen met behulp van camera's.

Naast de burgemeester is de gemeenteraad op grond van zijn autonome verordeningsbevoegdheid bevoegd om op eigen initiatief en naar eigen inzicht regelgeving vast te stellen die hij nodig acht in het belang van de huishouding van de gemeente.[13] Ook handhaving van de openbare orde maakt onderdeel uit van het belang van de eigen huishouding van de gemeente.[14] Wederom kan in het kader van het preventieaspect deze bevoegdheid door de gemeenteraad tevens worden aangewend om cameratoezicht voor dat doel mogelijk te maken.

Deze bevoegdheden van de burgemeester en de gemeenteraad zijn echter niet specifiek in het leven geroepen om het grondrecht op privacy te beperken. Er rezen derhalve al snel vragen omtrent de toelaatbaarheid van dit, volgens velen ingrijpende, instrument. De Registratiekamer[15] concludeerde dat het gebruik van cameratoezicht toelaatbaar is mits voldaan is aan een aantal voorwaarden. Zo dient het gebruik van de camera's in de eerste plaats kenbaar te zijn. Daarnaast moet het doel van het toezicht bepaald zijn en omschreven worden. Ook moet de gebruiker van de camera's bevoegd zijn op het terrein dat door de camera's wordt bestreken. Het gebruik van de camera's dient voorts noodzakelijk te zijn voor de uitoefening van de taak van de gebruiker. Het beoogde doel moet niet op minder ingrijpende wijze kunnen worden gerealiseerd. En tot slot dient eventuele levering van de gemaakte beelden voort te vloeien uit dit doel en mogen de gemaakte beelden niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze gemaakt zijn.[16]

Ook het kabinet-Kok II concludeerde dat het gebruik van cameratoezicht op openbare plaatsen in het kader van de handhaving van de openbare orde geen schending van het recht op privacy van de burgers inhield mits de gebruiker zich houdt aan deze voorwaarden.[17]

De huidige regering betwijfelt of de voormelde bevoegdheden van het lokale bestuur om binnen de gemeente camera's te plaatsen ten behoeve van toezicht toereikend zijn.[18] Ook op openbare plaatsen heeft een burger recht op een zekere eerbiediging van de persoonlijke levenssfeer en het risico bestaat dat, zeker gezien de steeds toenemende technische mogelijkheden bij het gebruik van camera's, cameratoezicht een inbreuk maakt op de persoonlijke levenssfeer. De regering acht het tevens problema-

13. Artikel 127 en 124 Grw en artikel 108, 147 en 149 Gem.w.
14. Met het begrip huishouding van de gemeente worden de gemeentelijke belangen bedoeld die niet door een hogere regeling behartigd worden en waarbij een aspect van het algemeen belang is betrokken. Handhaving van de openbare orde betreft het algemeen belang en behoort derhalve, op terreinen waar dit belang niet door een hogere regeling behartigd wordt, tot de eigen huishouding van de gemeente. Zie hieromtrent M.A.D.W. de Jong, Orde in beweging, Deventer: W.E.J. Tjeenk Willink 2000, p. 27.
15. Thans Collegebescherming Persoonsgegevens (CBP).
16. Registratiekamer, In beeld gebracht, Onderzoeksrapport van 27 januari 1997, beschikbaar op www.CBPweb.nl.
17. Kamerstukken II 1997-1998, 25 760, nr. 1. Zie hierover eveneens H.A. Offens, Cameratoezicht, P&I 2001, nr. 4, p. 148-163.
18. Kamerstukken II 2003-2004, 29 440, nr. 3, p . 3.

tisch dat er door het ontbreken van een algemeen geldende regeling voor het gebruik van cameratoezicht door gemeenten in verschillende gemeenten verschillende regels worden gehanteerd, hetgeen leidt tot uiteenlopende rechtsgevolgen voor de burgers.[19]

Door middel van het voorstel tot wijziging van de Gemeentewet en de Wet Politieregisters (Wet Pol.r.)[20] wil de regering voorzien in een toereikende grondslag voor het gebruik van cameratoezicht. Tevens wil de regering cameratoezicht door gemeenten door middel van dit voorstel normeren en uniformeren door de door het CBP en het kabinet-Kok geformuleerde voorwaarden voor rechtmatig gebruik van cameratoezicht te codificeren en nader uit te werken.

2.1.2 Het wetsvoorstel cameratoezicht op openbare plaatsen

Wanneer een gemeentebestuur wil overgaan tot het gebruik van cameratoezicht, dient de gemeenteraad op grond van het nieuw te introduceren artikel 151c Gem.w. eerst bij verordening de burgemeester de bevoegdheid te verlenen om te besluiten camera's te plaatsen. De burgemeester kan vervolgens op basis van deze bevoegdheid besluiten om in bepaalde gebieden over te gaan tot de plaatsing van camera's en daarna vaststellen wanneer deze camera's daadwerkelijk gebruikt worden.

Het plaatsingsbesluit

Op grond van het eerste lid van het voorgestelde artikel 151c Gem.w. dient de gemeenteraad, zoals gezegd, de burgemeester eerst bij verordening de bevoegdheid te verlenen om te besluiten camera's te plaatsen. In deze verordening kan de gemeenteraad aanwijzingen opnemen omtrent de aan te wijzen gebieden en de duur van de plaatsing van de camera's. De gemeenteraad mag de burgemeester deze bevoegdheid blijkens artikel 151c lid 1 Gem.w. slechts verlenen indien dit in het belang van de openbare orde noodzakelijk is. Uit de motivering van dit besluit dient derhalve te blijken dat er in de gemeente gebieden zijn waar zich met enige regelmaat onveilige situaties voordoen die effectief bestreden kunnen worden met behulp van de inzet van cameratoezicht en waar een minder ingrijpend middel, zoals bijvoorbeeld de inzet van extra agenten, niet zou volstaan.[21]

Op basis van de door de gemeenteraad verleende bevoegdheid kan de burgemeester vervolgens besluiten tot de plaatsing van camera's. Bij het plaatsingsbesluit is de burgemeester blijkens artikel 151c lid 1 Gem.w. aan een aantal voorwaarden gebonden. Bij de keuze van de gebieden dient de burgemeester zich te beperken tot 'openbare plaatsen', deze plaatsen dienen nauwkeurig in het plaatsingsbesluit omschreven te zijn, de duur van de plaatsing moet beperkt zijn en er mag slechts gebruik worden gemaakt van vaste camera's.

Voor de uitleg van het begrip openbare plaats heeft het voorstel blijkens het eerste lid aansluiting gezocht bij artikel 1 van de Wet Openbare Manifestaties (WOM). Volgens

---

19. Kamerstukken II 2003-2004, 29 440, nr. 3, p . 3. Zo is in de ene gemeente de Wet bescherming persoonsgegevens van toepassing op de gegevens die door middel van het cameratoezicht verzameld zijn en in de andere de Wet Pol.r. Er zijn gemeenten die het gebruik van cameratoezicht niet bij het CBP gemeld hebben.
20. Kamerstukken II 2003-2004, 29 440, nr. 1 en 2.
21. Kamerstukken II 2003-2004, 29 440, nr. 3, p. 10.

artikel 1 WOM is een openbare plaats 'een plaats die krachtens bestemming of vast gebruik openstaat voor het publiek'. Het kan daarbij zowel gaan om plaatsen die een typisch onderdeel zijn van het publiek domein, zoals een openbare weg, als om plaatsen die particulier eigendom zijn, zoals bijvoorbeeld een particulier winkelcentrum. Voorwaarde is wel dat het een ieder in beginsel vrij moet staan om op deze plaats te verblijven, te komen en te gaan.[22]

De duur van het cameratoezicht dient ingevolge artikel 151c lid 1 Gem.w. beperkt te zijn en in het besluit tot het plaatsen van de camera's dient aangegeven te zijn gedurende welke periode de camera's geplaatst worden. Het voorstel geeft evenwel geen maximale duur van de plaatsing omdat een geschikte duur per gebied en per gemeente kan verschillen.

Bij het toezicht moet worden gebruikgemaakt van vaste camera's, dat wil zeggen camera's die permanent zijn bevestigd aan bijvoorbeeld gevels, dakranden van gebouwen en palen. Het gebruik van de camera's kan wel dynamisch zijn, dit betekent dat de observatiehoek van de camera's op afstand kan worden aangepast en met de camera's kan worden in- en uitgezoomd.[23]

Het daadwerkelijke toezicht

Nadat de burgemeester heeft besloten tot de plaatsing van de camera's moet hij op grond van het tweede lid in overleg met de officier van justitie vaststellen gedurende welke periode de camera's daadwerkelijk gebruikt worden en dat er in ieder geval rechtstreeks met de gemaakte beelden wordt meegekeken. Uit onderzoek is gebleken dat cameratoezicht het meest effectief is als er rechtstreeks met de beelden wordt meegekeken zodat er, indien zich incidenten voordoen, direct kan worden ingegrepen.[24] Permanent meekijken is echter niet mogelijk gezien de beperkte capaciteit van de politie, die de beelden in de praktijk het eerst gebruikt.[25] De burgemeester zal derhalve periodes moeten vaststellen waarin rechtstreeks met de beelden wordt meegekeken. Dit dient hij in overleg met de officier van justitie te doen omdat, wanneer door middel van cameratoezicht strafbare feiten worden waargenomen en de politie daartegen optreedt, de politie handelt in het kader van strafrechtelijke handhaving van de rechtsorde en dan staat zij onder het gezag van de officier van justitie (artikel 13 Pol.w.).

Wanneer de camera's daadwerkelijk geplaatst zijn, dient hun aanwezigheid voor de burgers voldoende duidelijk te zijn (artikel 151c lid 3 Gem.w.). Dit kan bijvoorbeeld door aan de rand van het door camera's bewaakte gebied borden te plaatsen.[26]

---

22. Het openstaan voor publiek dient gebaseerd te zijn op het karakter dat de rechthebbende aan de plaats heeft toegekend of de plaats dient gedurende een bepaalde tijd te zijn gebruikt alsof deze openstaat voor publiek en de rechthebbende heeft dit gebruik gedoogd. In navolging van het systeem van artikel 1 WOM worden kerken en andere gebouwen die door de rechthebbende zijn bestemd voor het belijden van een geloofsovertuiging uitgesloten van de toepasselijkheid van het voorstel. Kamerstukken II 2003-2004, 29 440, nr. 3, p. 8.
23. Kamerstukken II 2003-2004, 29 440, nr. 3, p. 7.
24. CBP, Cameratoezicht in de openbare ruimte, Rapport 1, november 2003, p. 13-14. Beschikbaar op www.CBPweb.nl.
25. Dit betekent echter niet dat de politie verplicht is het meekijken uitsluitend te laten plaatsvinden door politiefunctionarissen. Op grond van lid 8 mag het bekijken van de beelden worden uitbesteed aan anderen mits dit onder regie van de politie gebeurt en de beslissing tot daadwerkelijk politieoptreden op basis van de beelden voorbehouden blijft aan politiefunctionarissen. Kamerstukken II 2003-2004, 29 440, nr. 3, p. 11.
26. Kamerstukken II 2003-2004, 29 440, nr. 3, p. 17.

De politie mag de met behulp van de camera's gemaakte beelden vastleggen in het belang van de handhaving van de openbare orde (artikel 151c lid 6 Gem.w.). Zij mogen deze beelden echter niet langer dan 7 dagen bewaren. De aldus vastgelegde beelden vormen blijkens artikel 151c lid 7 Gem.w. een politieregister in de zin van de Wet Pol.r.[27] Dit heeft tot gevolg dat de beelden, die in beginsel slechts mogen worden gebruikt in het belang van de handhaving van de openbare orde, op basis van het door het voorstel te introduceren zevende lid van artikel 13 Wet Pol.r. aan de met opsporing van strafbare feiten belaste instanties mogen worden verstrekt indien er concrete aanwijzingen zijn dat deze beelden informatie bevatten die noodzakelijk is voor de opsporing van een gepleegd strafbaar feit.

Op grond van lid 9 van artikel 151c Gem.w. dient de burgemeester tot slot ten minste één maand voor het verstrijken van de geldingsduur van het plaatsingsbesluit een verslag te zenden aan de gemeenteraad waarin het gebruik van de camera's in het desbetreffende gebied wordt geëvalueerd. Daarbij dient te worden bezien of de doelstellingen van het cameratoezicht zijn gerealiseerd en of voortzetting van het cameratoezicht noodzakelijk is.

Rechtsbescherming voor de burger

Tegen de beslissing van de gemeenteraad om de burgemeester bij verordening de bevoegdheid te verlenen om over te gaan tot het plaatsen van camera's ten behoeve van de handhaving van de openbare orde staat geen beroep op de bestuursrechter open.[28] Wel kan de burger zich tot de burgerlijke rechter wenden door te stellen dat de gemeente met het plaatsingsbesluit jegens hem een onrechtmatige daad heeft gepleegd. Of de burger hier in de praktijk veel aan heft, is echter zeer de vraag. Het zal bijzonder lastig zijn om aannemelijk te maken dat wordt voldaan aan een aantal van de voorwaarden van de onrechtmatige daad, zoals bijvoorbeeld schade en causaliteit.

Op de vraag of tegen het plaatsingsbesluit een gang naar de bestuursrechter openstaat, zijn verschillende antwoorden mogelijk. De memorie van toelichting van het wetsvoorstel 'Cameratoezicht op openbare plaatsen' laat zich over deze vraag niet uit. Enerzijds valt te verdedigen dat een aanwijzingsbesluit geen besluit is in de zin van de Awb omdat de beslissing geen rechtsgevolg meebrengt. De beslissing heeft slechts tot gevolg dat er een feitelijke handeling verricht wordt, het plaatsen van camera's. Aan de andere kant kan worden beargumenteerd dat de beslissing wel een verandering in de wereld van het recht met zich mee kan brengen omdat de plaatsing van camera's eventueel een inbreuk op het recht op privacy van de met behulp van de camera's waargenomen burgers vormt. In dat geval zal een burger, indien hij in rechte wil opkomen tegen het besluit om camera's te plaatsen, zich moeten wenden tot de burgerlijke rechter.

Wanneer een burger wil weten of er, en zo ja welke, beelden over hem zijn opgenomen in een politieregister, heeft hij op grond van artikel 20 Wet Pol.r. een recht op kennisneming. Een verzoek tot kennisneming mag door de korpsbeheerder slechts geweigerd worden indien en voorzover dit noodzakelijk is voor de goede uitvoering

---

27. Dit heeft tot gevolg dat niet de normen van de Wet bescherming persoonsgegevens van toepassing zijn op deze gegevensverwerking maar de normen van de Wet Pol.r.
28. De verordening (een algemeen verbindend voorschrift) is ingevolge artikel 8:2 Awb uitgezonderd van de rechtsmacht van de bestuursrechter.

van de politietaak of de bescherming van gewichtige belangen van derden (artikel 21 Wet Pol.r.). Indien er gegevens omtrent de verzoeker in het register opgenomen blijken te zijn, kan de betrokkene de korpsbeheerder schriftelijk verzoeken deze te verbeteren, aan te vullen of te wijzigen als deze feitelijk onjuist zijn, voor het doel van het register onvolledig of niet noodzakelijk zijn of wanneer deze in strijd met een wettelijk voorschrift in het register voorkomen (artikel 22 Wet Pol.r.). Mocht de beheerder niet aan een verzoek als bedoeld in artikel 20 of 22 Wet Pol.r. voldoen, dan staat voor de betrokkene ingevolge artikel 23 Wet Pol.r. een rechtsgang open bij de rechtbank of kan hij zich voor bemiddeling wenden tot het CBP.

2.2 Preventief fouilleren

Sinds september 2002 zijn de bevoegdheden van de politie, in speciale daartoe door de burgemeester aangewezen veiligheidsrisicogebieden, om personen te fouilleren en voertuigen, verpakkingen en bagage op wapens te onderzoeken uitgebreid.[29] Om een persoon aan de kleding en bagage, verpakkingen en voertuigen te onderzoeken is niet langer vereist dat er jegens deze persoon een verdenking bestaat van het plegen van enig strafbaar feit. Het zich bevinden in een veiligheidsrisicogebied is op basis van deze nieuwe regeling voldoende aanleiding om iemand 'preventief te fouilleren'.

2.2.1 Achtergrond preventief fouilleren

De wetswijziging die deze bevoegdheid tot preventief fouilleren heeft geïntroduceerd, is totstandgekomen tegen de achtergrond van de toegenomen gevoelens van onveiligheid in het publieke domein als gevolg een forse toename van de geweldscriminaliteit. Uit onderzoek bleek dat deze geweldsproblematiek sterk in bepaalde gebieden en rond bepaalde tijden geconcentreerd is.[30] De met opsporing van (vuur)wapens belaste instanties constateerden echter dat de bevoegdheden die zij bezaten om wapenbezit in deze gebieden tegen te gaan in de praktijk niet toereikend waren.[31] Teneinde vuurwapencriminaliteit beter te kunnen bestrijden stelden zij voor de bevoegdheden om personen te fouilleren en bagage, verpakkingen en vervoermiddelen op wapens te controleren uit te breiden zodat in bepaalde gebieden met een bijzondere gevaarzetting preventief gefouilleerd zou kunnen worden.[32]

Hoewel het toenmalige kabinet niet negatief stond tegenover preventief fouilleren, meende het dat, alvorens tot uitbreiding van de bestaande bevoegdheden zou kunnen worden besloten, eerst diende te worden onderzocht of de bestaande wettelijke

29. Stb. 2002, 420 en Stb. 2002, 459.
30. WODC en CBS, Criminaliteit en rechtshandhaving, 1999, p. 163.
31. Kamerstukken II 1999-2000, 26 586, nr. 2 (Raad van Hoofdcommissarissen, Eindrapport landelijke project aanpak illegale vuurwapens).
32. Regiokorps Rotterdam-Rijnmond, Aanpak Vuurwapengeweld (1998), Raad van Hoofdcommissarissen, Eindrapport landelijke project aanpak illegale vuurwapens (Kamerstukken II 1999-2000, 26 586, nr. 2) en de brief van de Vereniging van Nederlandse Gemeenten aan de Vaste commissie voor Justitie van 20 oktober 1999 (commentaar op de justitiebegroting 2000).

bevoegdheden ter bestrijding van vuurwapencriminaliteit toereikend waren.[33] Ter uitvoering van dit voornemen werden er enkele gebieden geselecteerd voor een proefproject, inhoudende dat gedurende enige tijd in gebieden met een bijzondere gevaarzetting een geïntensiveerde inzet van de politie zou plaatsvinden. Hierbij zou optimaal gebruik worden gemaakt van alle preventieve en repressieve bevoegdheden die de wet op dat moment bood ter bestrijding van illegaal wapenbezit en wapengebruik.[34]

Op 26 november 1999 werd in het kader van dit proefproject in de Rotterdamse Millinxbuurt een actie gehouden waarbij alle zich in het afgesloten gebied bevindende personen en rijdende voertuigen werden onderzocht op de aanwezigheid van wapens. De juridische grondslag voor deze actie was gelegen in artikel 50 lid 2, 51 lid 2 en 52 lid 2 Wet wapens en munitie (WWM). Volgens de officier van justitie vormde het feit dat zich in de afgelopen vijf jaar 424 geweldsincidenten hadden voorgedaan in de Millinxbuurt, waarbij 38 vuurwapens waren aangetroffen een voldoende grond om eenieder die zich in die buurt na 20:00 uur op de openbare weg bevond aan te merken als een verdachte tegen wie ernstige bezwaren bestonden zoals bedoeld in artikel 52 lid 2 WWM.[35]

In de naar aanleiding van deze actie aanhangig gemaakte strafzaken oordeelde de rechtbank echter dat de gekozen grondslag niet toereikend was.[36] Artikel 52 lid 2 WWM eist voor een onderzoek aan de kleding ten minste een geïndividualiseerde verdenking, aldus de rechtbank. Gegevens over toegenomen wapenbezit en -gebruik in een beperkt gebied en een bepaald tijdvak zijn niet voldoende doordat zij niet direct tot concrete personen te herleiden zijn.[37] Dientengevolge kunnen de artikelen 50 lid 2, 51 lid 2 en 52 lid 2 WWM niet fungeren als rechtmatige grondslag voor een actie preventief fouilleren.

Om preventief fouilleren mogelijk te maken maakte het CDA Tweede-Kamerlid Van de Camp een initiatiefvoorstel aanhangig bij de Tweede Kamer.[38] Deze wijziging van de Gemeentewet en de Wet wapens en munitie is in werking getreden op 15 september 2002.[39]

2.2.2 Relevante regelgeving ten aanzien van preventief fouilleren

Op basis van het nieuwe artikel 151b Gem.w. kan de gemeenteraad de burgemeester bij verordening de bevoegdheid geven om een gebied aan te wijzen als veiligheidsrisicogebied. Na aanwijzing van een dergelijk veiligheidsrisicogebied door de burgemeester kan de politie in dit gebied vervolgens, op uitdrukkelijk bevel van de officier van justitie, gebruikmaken van de bevoegdheden van de nieuwe artikel 50 lid 3, 51 lid 3 en 52 lid 3 WWM.

---

33. Kamerstukken II 1998-1999, 26 494, nr. 1, p. 6.
34. Kamerstukken II 1998-1999, 26 494, nr. 1, p. 4.
35. Rb. Rotterdam 4 januari 2000, LJN AA4046.
36. Rb. Rotterdam 4 januari 2000, LJN AA4046.
37. Kamerstukken II 1999-2000, 26 800 VI, nr. 50.
38. Kamerstukken II 1999-2000, 26 865, nr. 1 en 2 (Initiatiefvoorstel Van de Camp). Ook de regering heeft een voorstel ingediend bij de Tweede Kamer (Kamerstukken II 2000-2001, 27 605, nr. 1 en 2), Het regeringsvoorstel is echter, nadat het voorstel Van de Camp door de Kamers is aangenomen en door de Kroon is bekrachtigd, ingetrokken.
39. Stb. 2002, 420 en Stb. 2002, 459.

De aanwijzing van het veiligheidsrisicogebied

Alvorens de politie daadwerkelijk kan overgaan tot een actie preventief fouilleren dient de gemeenteraad derhalve eerst de burgermeester bij verordening de bevoegdheid te verlenen om een gebied aan te merken als veiligheidsrisicogebied. Bij het gebruik van deze bevoegdheid is de burgemeester gebonden aan een aantal voorwaarden.

Allereerst dient er op grond van artikel 151b lid 1 Gem.w. sprake te zijn van verstoring van de openbare orde door de aanwezigheid van wapens dan wel bij ernstige vrees daarvoor. Van verstoring van de openbare orde is sprake wanneer de normale gang van zaken en rust in het openbare leven wordt verstoord.[40] Met het gebruik van het subjectieve begrip vrees wordt blijkens de memorie van toelichting aansluiting gezocht bij artikel 175 en 176 Gem.w.[41] Hoewel het begrip vrees een subjectief begrip is, dient dit wel objectiveerbaar te zijn. Van vrees moet in redelijkheid sprake zijn, dit betekent dat de rechter op basis van concrete feiten en omstandigheden moet kunnen toetsen of deze vrees gerechtvaardigd is.[42] De rechter zal het bestaan van deze vrees echter niet indringend kunnen toetsen, de rechter zal slechts kunnen beoordelen of het bestuursorgaan gezien de feiten en omstandigheden in redelijkheid heeft kunnen komen tot het oordeel dat er ernstige vrees bestond voor verstoring van de openbare orde als gevolg van de aanwezigheid van wapens.

Ten tweede is de burgemeester op basis van het tweede lid bij de aanwijzing van een veiligheidsrisicogebied verplicht overleg te voeren met de officier van justitie. Deze voorwaarde is opgenomen omdat fouillering een handeling is die, bij ontdekking van een wapen, aanleiding geeft tot een beslissing omtrent gerechtelijke afdoening en dus de medewerking van het OM vereist. Het uitoefenen van de aanwijzingsbevoegdheid zonder overleg met de officier van justitie is daarom onwenselijk.[43]

In het derde lid van artikel 151b Gem.w. wordt vervolgens de eis gesteld dat de aanwijzing voor een bepaalde duur gegeven wordt, deze duur dient niet langer te zijn dan noodzakelijk is ten behoeve van de handhaving van de openbare orde. Van een concrete maximum tijdsduur heeft de wetgever afgezien omdat een geschikte tijdsduur sterk afhankelijk is van de omstandigheden die tot de aanwijzing van het gebied hebben geleid. Wel dient het besluit zo nauwkeurig mogelijk begrensd te zijn, bij voorkeur door een aanduiding van een begin- en einddatum. Ook de omvang van het gebied mag niet groter zijn dan noodzakelijk is voor de handhaving van de openbare orde en moet zo nauwkeurig mogelijk worden afgebakend in het aanwijzingsbesluit (artikel 151c lid 3 Gem.w.).

Tot slot dient de aanwijzing op schrift te worden gesteld en zo spoedig mogelijk ter kennis van de gemeenteraad en de officier van justitie te worden gebracht. Indien de (ernstige vrees voor) verstoring van de openbare orde door de aanwezigheid van wapens niet langer bestaat, dient de burgemeester de gebiedsaanwijzing ingevolge artikel 151b lid 6 Gem.w. in te trekken.

---

40. M.A.D.W. de Jong, Orde in beweging, Deventer: Kluwer 2000, p. 18.
41. Kamerstukken II 1999-2000, 26 865, nr. 5, p. 5.
42. Ministerie van Justitie, Tussen-evaluatie preventief fouilleren 2003, Den Haag 2003, p. 7.
43. Kamerstukken II 2000-2001, 26 865, nr. 7, p. 5. Deze voorwaarde was niet in het oorspronkelijke voorstel van Van de Camp opgenomen. Zij is geïntroduceerd met het invoegen van een aantal bepalingen uit het meer strafvorderlijk getinte regeringsvoorstel (Kamerstukken 2000-2001, 27 605, nr. 2).

Bevoegdheden in een veiligheidsrisicogebied

In een door de burgemeester aangewezen veiligheidsrisicogebied kan ingevolge artikel 151b lid 1 Gem.w. gebruik worden gemaakt van de bevoegdheden van artikel 50 lid 3, 51 lid 3 en 52 lid 3 WWM. Alvorens tot de daadwerkelijke uitoefening van deze bevoegdheden kan worden overgegaan dient de officier van justitie op grond van artikel 50 lid 3, 51 lid 3 en 52 lid 3 WWM door middel van een bevel de toepassing van deze bevoegdheden te gelasten. Dit bevel dient een omschrijving van het aangewezen gebied te bevatten en een specifieke geldigheidsduur. Deze geldigheidsduur mag niet langer zijn dan 12 uur. Op basis van dit bevel mag vervolgens gebruik worden gemaakt van de genoemde bevoegdheden uit de WWM.

Op basis van het nieuwe artikel 52 lid 3 WWM mogen personen binnen veiligheidsrisicogebieden aan de kleding onderzocht worden op de aanwezigheid van wapens zonder dat ten aanzien van hen 'uit feiten en omstandigheden een redelijk vermoeden van schuld aan eenig strafbaar feit voortvloeit'.[44] Daar wapens tevens kunnen worden meegebracht in bagage of verpakkingen die een persoon bij zich draagt en het vervoermiddel waarin iemand zich vervoert, omvat de wetswijziging naast het 'preventief fouilleren' in de letterlijke zin van het woord tevens de mogelijkheid verpakkingen, bagage en vervoermiddelen te onderzoeken op de aanwezigheid van wapens. Het vereiste dat slechts mag worden overgegaan tot het doorzoeken van vervoermiddelen en het onderzoeken van bagage en verpakkingen indien daartoe redelijkerwijs een aanleiding bestaat op grond van een gepleegd of toekomstig strafbaar feit waarbij wapens zijn of naar verwachting zullen worden gebruikt, zoals dat gesteld wordt in artikel 50 lid 2 en 51 lid 2 WWM, is in de nieuwe artikelen 50 lid 3 en 51 lid 3 WWM losgelaten.[45]

In de praktijk worden voor de daadwerkelijke actie van preventief fouilleren verschillende middelen en methoden gebruikt. In verschillende gemeenten wordt het onderzoek aan de kleding handmatig verricht terwijl andere gemeenten gebruik maken van metaaldetectoren (handscans). Om personen en voertuigen te selecteren wordt gebruikgemaakt van verschillende methoden. In sommige gemeenten wordt er een heel gebied afgesloten en worden zo veel mogelijk van de in het gebied aanwezige personen en/of voertuigen op wapens onderzocht, de zogenaamde gebiedsafsluiting en de statische voertuigencontrole. Een aantal gemeenten laat agenten surveilleren of rondrijden die passanten of passerende voertuigen aanhouden en onderzoeken op de aanwezigheid van wapens. Hier spreekt men van gebiedssurveillance, passantencontrole en dynamische voertuigcontrole. Ook maakt een aantal gemeenten gebruik van zogenaamde lokaliteiten- of horecacontroles waarbij iedereen die in een lokaliteit of horecagelegenheid aanwezig is in een wachtruimte wordt gezet en vervolgens onderzocht wordt op de aanwezigheid van wapens.[46]

Rechtsbescherming voor de burger

Indien een burger bezwaren heeft tegen de aanwijzing van een gebied als veiligheidsrisicogebied kan hij zich volgens de memorie van toelichting met zijn bezwaarschrift

---

44. Artikel 27 Sv, Kamerstukken II 2000-2001, 27 605, nr. 3 p. 13-16.
45. Kamerstukken II 1999-2000, 26 865, nr. 5, p. 3.
46. Ministerie van Justitie, Tussen-evaluatie preventief fouilleren 2003, Den Haag 2003, p. 54-55.

richten tot de burgemeester en kan hij zich daarna met een eventueel beroepschrift wenden tot de bestuursrechter. Rechtbank Alkmaar heeft echter geoordeeld dat een burger die beroep instelt bij de bestuursrechter tegen een aanwijzingsbesluit niet-ontvankelijk is in zijn beroep omdat hij geen belanghebbende is bij dit besluit. Het belang van de burger is niet voldoende rechtstreeks bij het besluit betrokken indien de burger pas met de rechtsgevolgen van het besluit geconfronteerd wanneer de officier van justitie ook daadwerkelijk een last tot preventief fouilleren heeft doen uitgaan. Een burger voldoet dus niet aan het door artikel 8:1 juncto 1:2 lid 1 Awb gestelde belanghebbendevereiste.[47]

De burger kan de rechtmatigheid van het plaatsingsbesluit en ook de rechtmatigheid van de verordening waarin de gemeenteraad de bevoegdheid om een gebied aan te wijzen als veiligheidsrisicogebied aan de burgemeester verleent wel aanvechten in het kader van een onrechtmatigedaadsactie bij de burgerlijke rechter. Het is waarschijnlijk echter, evenals bij cameratoezicht, moeilijk om aannemelijk te maken dat voldaan is aan de voorwaarden voor een onrechtmatige daad.

Wanneer een burger zich wil beklagen over de uitoefening van de bevoegdheden in het kader van een actie van preventief fouilleren, kan hij in de eerste plaats gebruikmaken van de klachtprocedure van hoofdstuk 9 Awb, nader gepreciseerd voor de politie in hoofdstuk X Pol.w. Op basis van deze klachtprocedure kan de burger zich met zijn klacht wenden tot de korpsbeheerder. Daarnaast kan de burger zich op grond van artikel 12 e.v. Wet Nationale Ombudsman met een klacht over de behoorlijkheid van de gedraging van de politieagent wenden tot de Nationale ombudsman.[48] Indien er bij de burger verboden wapens worden aangetroffen en de burger vervolgd wordt wegens overtreding van artikel 13 en 26 WWM, kan hij de rechtmatigheid van de vordering tevens aan de orde stellen in de strafrechtelijke procedure.

2.3 Uitgebreide identificatieplicht

Op 24 juni 2004 is de wet op de uitgebreide identificatieplicht vastgesteld.[49] De wet beoogt de bestaande, beperkte identificatieplichten uit te breiden en houdt in dat een ieder die de leeftijd van veertien jaar heeft bereikt verplicht is om op vordering van een (buitengewoon) opsporingsambtenaar of een toezichthoudend ambtenaar een identificatiebewijs ter inzage aan te bieden.[50]

---

47. Rb. Alkmaar 28 juni 2004, LJN AP5618. Zie ook Rb. Alkmaar 16 juni 2003, AB 2003, 419 en Gst. 2003, nr. 7192/150. Zie hieromtrent I. Tappeiner, J. de Visser en A. Woltjer, Preventief fouilleren: op zoek naar rechtsbescherming, NJB 2003/36, p. 1903-1904; P.R. Rodriguez, Bezwaar tegen aanwijzing veiligheidsrisicogebied, P&I, nr. 5, oktober 2003, p. 216-218.
48. Gezien het feit dat de oordelen van de Nationale ombudsman geen formele rechtskracht hebben, wordt deze vorm van rechtsbescherming echter niet gezien als een *effective remedy* in de zin van artikel 13 EVRM, EHRM 26 maart 1987, Series A 116, p. 31 (Leander tegen Zweden).
49. Stb. 2004, 300.
50. M. Duker, M.E. de Meijer en B.J. Schmitz, Commentaar op de voorgestelde uitbreiding van de identificatieplicht, NJCM-Bulletin, jrg. 29 (2004), nr. 4a, p. 528.

2.3.1 Achtergrond van de uitgebreide identificatieplicht

Op dit moment kennen wij op basis van de huidige wet op de identificatieplicht een systeem van beperkte identificatieplichten. Het gaat hierbij om een zogenoemde bewijsplicht waarbij burgers in ieder geval dienen te beschikken over een geldig identificatiebewijs en dit in bepaalde situaties moeten tonen. De situaties waarin burgers verplicht zijn een identificatiebewijs te tonen zijn opgenomen in verschillende specifieke wetten.[51]

Een opsporingsambtenaar heeft thans slechts de bevoegdheid om inzage in een identiteitsbewijs te vragen in het kader van de strafrechtelijke handhaving. Op grond van artikel 55b Wetboek van Strafvordering (Sv) kan de politie een verdachte die is staande gehouden of aangehouden vragen om zijn identiteitsbewijs. Op het terrein van de andere taken van de politie, handhaving van de openbare orde en de hulpverlening aan burgers, heeft de politie op dit moment niet de bevoegdheid om burgers om een identiteitsbewijs te vragen. Zij is daar slechts toe bevoegd indien er tevens sprake is van een strafbaar feit. In de praktijk komt het volgens de regering echter voor dat er, bijvoorbeeld bij dreigende wanordelijkheden, behoefte bestaat om de identiteit van de betrokkenen vast te stellen zonder dat er sprake is van verdenking van een strafbaar feit.

Ambtenaren belast met het houden van toezicht op de naleving van wettelijke voorschriften (artikel 5:11 Awb), zijn thans op grond van artikel 5:17 Awb bevoegd tot het vorderen van inzage in zakelijke gegevens en bescheiden. De bevoegdheid om inzage te vorderen in zakelijke gegevens en bescheiden omvat onder omstandigheden tevens de bevoegdheid tot het inzien van identificatiebewijzen.[52] Daar de bevoegdheden van toezichthoudend ambtenaren worden begrensd door het in artikel 5:13 Awb neergelegde evenredigheidsbeginsel mag een toezichthoudend ambtenaar slechts inzage in een identificatiebewijs vorderen voorzover dit redelijkerwijs noodzakelijk is voor de uitoefening van zijn taak.

De regering is echter van mening dat de huidige beperkte identificatieplichten niet langer toereikend zijn als het gaat om de bevoegdheden die (buitengewoon) opsporingsambtenaren en toezichthouders hebben om inzage te vragen in identiteitsbewijzen. Om de taken die primair aan de overheid zijn opgedragen, de politietaak en het toezicht op de naleving van wetten goed te kunnen uitvoeren is het volgens de regering noodzakelijk dat de bevoegdheden van (buitengewoon) opsporingsambtenaren en toezichthouders om inzage te vragen in identiteitsbewijzen worden uitgebreid.[53] Het is voor deze ambtenaren, willen zij hun taak effectief kunnen uitoefenen, in bepaalde situaties noodzakelijk dat zij weten met wie ze van doen hebben. Daar de bevoegdheid om burgers om inzage in een identiteitsbewijs te vragen in een aantal situaties ontbreekt, is het mogelijk dat burgers zich onttrekken aan de verantwoordelijkheid voor hun optreden door zich te verschuilen achter de anonimiteit in de openbare ruimte.[54] Wat de regering hier precies mee bedoelt, wordt niet uitgelegd. Zij lijkt hier-

---

51. Kamerstukken II 2001-2002, 28 069, nr. 1, p. 5. Bijvoorbeeld artikel 65 Algemene bijstandswet, artikel 50 en 111 Wegenverkeerswet, artikel 151a Gem.w., artikel 50 Vreemdelingenwet.
52. Kamerstukken II 1996-1997, 25 280, nr. 3, p. 40 en Rb. Den Haag 25 februari 2000, AB 2000, 271, r.o. 8.
53. Kamerstukken II 2003-2004, 29 218, nr. 3, p. 4.
54. Kamerstukken II 2003-2004, 29 218, nr. 3, p.1.

bij te denken aan situaties waar bijvoorbeeld bekeuringen wegens overtreding van de plaatselijke verordening (denk bijvoorbeeld aan wildplassen) worden uitgeschreven aan niet bestaande of onjuiste personen doordat de overtreder een valse naam opgeeft.

Of deze vrees gerechtvaardigd is, wordt niet onderbouwd met gegevens over het soort en aantal gevallen waarin regelgeving om deze reden niet gehandhaafd kan worden.[55] Ook wordt de bewering van de regering dat een uitgebreide identificatieplicht zou bijdragen aan meer effectieve handhaving en bestrijding van criminaliteit niet nader onderbouwd met argumenten en cijfers.[56] De regering toont evenmin overtuigend aan hoe de vermeende tekorten in de (criminaliteits)handhaving kunnen worden opgelost met behulp van een uitbreiding van de identificatieplicht.[57] Ten slotte laat de regering na toe te lichten waarom een intensiever gebruik van het huidige bestaande systeem van beperkte identificatieplichten, zoals het kabinet-Kok II amper twee jaar geleden nog concludeerde,[58] niet zou volstaan bij de bestrijding van deze vermeende tekorten.[59]

2.3.2 De nieuwe wet op de identificatieplicht

Op grond van de door de wet te introduceren artikelen 8a Politiewet en 5:16a Awb krijgen politieambtenaren, buitengewoon opsporingsambtenaren en toezichthouders de bevoegdheid om van een ieder die de leeftijd van veertien jaar heeft bereikt inzage in een identiteitsbewijs te vorderen.[60] Bij de uitoefening van deze bevoegdheid is de ambtenaar gebonden aan de voorwaarde dat dit redelijkerwijs noodzakelijk is voor de uitoefening van zijn taak. Door deze uitbreiding krijgen de betreffende ambtenaren de zelfstandige bevoegdheid om naar een identiteitsbewijs te vragen. Het is echter niet de bedoeling dat de identiteitscontrole een doel op zich wordt, wil een ambtenaar een burger om een identiteitsbewijs kunnen vragen, dan dient daarvoor een concrete aanleiding te zijn.[61]

De burger wordt op grond van het nieuwe artikel 2 Wet op de identificatieplicht verplicht gevolg te geven aan de vordering van de opsporings- of toezichthoudend ambtenaar. Indien de burger niet in staat of bereid is aan de vordering van de ambte-

---

55. M. Duker, M.E. Meijer en B.J. Schmitz, NJCM-commentaar op de voorgestelde uitbreiding van de wet identificatieplicht, NJCM-Bulletin, jrg. 29 (2004), p. 536-537; P. Mendelts en I. Sewandono, De voorgestelde identificatieplicht moet veel beter worden genormeerd, NJB 2003/19, p. 973-974; NOVA, Advies inzake het wetsvoorstel uitbreiding identificatieplicht van 23 januari 2003, beschikbaar op www.advocatenorde.nl.
56. Kamerstukken II 2003-2004, 29 218, nr. 10, p. 2; M. Duker, M.E. Meijer en B.J. Schmitz, NJCM-commentaar op de voorgestelde uitbreiding van de wet identificatieplicht, NJCM-Bulletin, jrg. 29 (2004), p. 528-543.
57. M. Duker, M.E. Meijer en B.J. Schmitz, NJCM-commentaar op de voorgestelde uitbreiding van de wet identificatieplicht, NJCM-Bulletin, jrg. 29 (2004), p. 536-537; P. Mendelts en I. Sewandono, De voorgestelde identificatieplicht moet veel beter worden genormeerd, NJB 2003/19, p. 973-974; NOVA, Advies inzake het wetsvoorstel uitbreiding identificatieplicht van 23 januari 2003, beschikbaar op www.advocatenorde.nl.
58. Kamerstukken II 2001-2002, 28 069, nr. 1.
59. CBP, Advies wetsvoorstel uitbreiding identificatieplicht, beschikbaar op www.CBPweb.nl; NVvR, Advies inzake het conceptwetsvoorstel inzake uitbreiding van de identificatieplicht van 20 februari 2003, beschikbaar op www.verenigingvoorrechtspraak.nl.
60. Deze leeftijd was in het conceptvoorstel op twaalf jaar gesteld. Om tegemoet te komen aan de bezwaren van onder andere de NOVA en de NVvR omtrent de disproportionaliteit van deze leeftijd is deze verhoogd naar veertien. NOVA, Advies inzake het wetsvoorstel uitbreiding identificatieplicht van 23 januari 2003, beschikbaar op www.advocatenorde.nl.; NVvR, Advies inzake het conceptwetsvoorstel inzake uitbreiding van de identificatieplicht van 20 februari 2003, beschikbaar op www.verenigingvoorrechtspraak.nl.
61. Kamerstukken II 2003-2004, 29 218, nr. 10, p. 4.

naar te voldoen, kan hij worden aangemerkt als verdachte van een strafbaar feit, het overtreden van het eveneens nieuw te introduceren artikel 447e Sr. Hij kan dan worden gestraft met een geldboete van de tweede categorie, maximaal € 2250. De opsporingsambtenaar kan de verdachte vervolgens meenemen naar het politiebureau en onderwerpen aan identificatiemaatregelen.

Is het een toezichthouder die constateert dat niet wordt voldaan aan zijn vordering, dan is hij niet bevoegd om daar een proces-verbaal van op te maken. Een toezichthoudend ambtenaar die niet tevens is aangesteld als buitengewoon opsporingsambtenaar, dient daartoe de bijstand van een opsporingsambtenaar in te roepen.

Alleen de controles waarvan een proces-verbaal wordt opgemaakt, worden geregistreerd. Dit is niet vastgelegd in de wet maar berust op de toezegging van de regering dat dit niet zal gebeuren.[62] Het is de vraag of de regering deze toezegging gestand zal doen.

Rechtsbescherming voor de burger

Wanneer een burger wil opkomen tegen de wijze van uitoefening van de bevoegdheid om inzage in een identiteitsbewijs te vorderen, kan hij gebruikmaken van de bestaande klachtprocedures. Is de vordering gedaan door een opsporingsambtenaar, dan kan de burger zich op basis van de klachtprocedure wenden tot de korpsbeheerder.[63] Deed een toezichthouder de vordering, dan kan de burger zich met zijn klacht op grond van hoofdstuk 9 van de Awb wenden tot het bevoegde bestuursorgaan. Daarnaast kan de burger zich op grond van artikel 12 e.v. Wet Nationale Ombudsman met een klacht over de behoorlijkheid van de gedraging van de opsporingsambtenaar of de toezichthouder wenden tot de Nationale ombudsman. Indien de burger vervolgd wordt wegens overtreding van artikel 447e Sr, kan hij de rechtmatigheid van de vordering tevens aan de orde stellen in een strafrechtelijke procedure.

62. Kamerstukken II 2003-2004, 29 218, nr. 3, p. 13.
63. Hoofdstuk 9 Awb, voor de politie nader gepreciseerd in hoofdstuk X Pol.w.

3 Privacy in het geding

Cameratoezicht, preventief fouilleren en de plicht zich te identificeren wordt door menig burger ervaren als een inbreuk op zijn privacy. Kenmerkend aan deze controlemaatregelen is dat zij veelal (zullen) worden toegepast in voor publiek toegankelijke, openbare ruimten. In dit hoofdstuk staat de vraag centraal of de toepassing van deze controlemaatregelen een beperking van het recht op privacy vormen. Om deze vraag te beantwoorden zal ik eerst ingaan op de vraag of het recht op privacy, zoals dat voor Nederland beschermd wordt in nationale en internationale bepalingen, zich tevens uitstrekt tot de openbare ruimte. Vervolgens zal ik onderzoeken of de (voorgestelde) maatregelen die in dit preadvies centraal staan een beperking van dit recht vormen.

3.1 Privacy op openbare plaatsen

Het recht op privacy is in Nederland in algemene zin vastgelegd in de Grondwet (Grw), artikel 10 lid 1, en in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM).[64]

Ingevolge artikel 10 lid 1 Grw heeft een ieder het recht op eerbiediging van zijn persoonlijke levenssfeer. Naar blijkt uit de memorie van toelichting en jurisprudentie over dit artikel kan de inhoud van het begrip persoonlijke levenssfeer niet in één alomvattende definitie worden beschreven. Het begrip persoonlijke levenssfeer strekt zich uit tot verschillende aspecten van het persoonlijk leven. Zo omvat zij de woning (ruimtelijke privacy), het familie- en gezinsleven, de seksuele identiteit, het aangaan en onderhouden van relaties met anderen (relationele privacy), het uitoefenen van invloed op de verwerking van hem betreffende persoonsgegevens (informationele privacy) en lichamelijke integriteit.[65] De wetgever, en later de rechter, hebben de inhoud van het begrip persoonlijke levenssfeer bewust gedeeltelijk open gelaten. Onder invloed van nieuwe ontwikkelingen en veranderende (rechts)opvattingen doen zich steeds nieuwe privacykwesties voor. Door de inhoud van het begrip gedeeltelijk open te laten worden deze nieuwe privacykwesties niet bij voorbaat uitgesloten van de door artikel 10 lid 1 Grw geboden bescherming.

---

64. Ook in artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR) wordt het recht op privacy beschermd. Dit artikel voegt echter weinig toe aan de door artikel 10 lid Grw en artikel 8 EVRM geboden bescherming. Om deze reden zal ik dit artikel in dit preadvies buiten beschouwing laten.
65. Kamerstukken II 1975-1976, 13 872, nr. 3, p. 40-41. Zie ook het rapport van de Commissie grondrechten in het digitale tijdperk, p. 116.

Volgens de memorie van toelichting inzake artikel 10 lid 1 Grw ziet het recht op eerbiediging van de persoonlijke levenssfeer op 'de reeks van situaties waarin de mens onbevangen zichzelf wil zijn'.[66] Deze situaties laten zich niet ruimtelijk begrenzen en het recht op eerbiediging van de persoonlijke levenssfeer kan derhalve ook in de openbare ruimte in het geding zijn.[67] Gezien de in de openbare ruimte heersende betrekkelijke anonimiteit heeft de burger ook daar recht op een zekere mate van privacybescherming.[68] Wel is het recht op privacy minder snel in het geding naarmate een situatie zich meer in het openbaar voordoet.

Artikel 8 EVRM beschermt, naar blijkt uit het eerste lid, het recht van een ieder op respect voor zijn privé-leven, familie- en gezinsleven, woning en correspondentie. Het Europees Hof voor de Rechten van de Mens (EHRM) heeft aangegeven het mogelijk noch noodzakelijk te achten een uitputtende definitie te geven van de reikwijdte van dit artikel,[69] het verdrag is volgens het EHRM een levend instrument dat dient te worden uitgelegd in het licht van de omstandigheden die op dat moment gelden.[70] Dit brengt met zich mee dat de in het eerste lid opgesomde categorieën ruim moeten worden geïnterpreteerd en een breed scala aan belangen bestrijken. Zo kan het privacybegrip ook relevant zijn ten aanzien van handelingen in het publieke domein. Of een concrete situatie valt onder de bescherming van artikel 8 EVRM wordt daarbij mede bepaald door de redelijke verwachting die de betreffende persoon koestert omtrent de bescherming van zijn privacy. Deze verwachting is echter niet allesbepalend.[71]

Concluderend kan worden gesteld dat de burger ook in de openbare ruimte recht heeft op een zekere eerbiediging van zijn privacy. Niet ieder handelen van de overheid waardoor de aanwezigheid of het handelen van de burger in de openbare ruimte wordt opgemerkt, vormt echter een beperking op het door artikel 10 lid 1 Grw en artikel 8 EVRM beschermde recht op privacy. Voor elk van de in dit preadvies behandelde controlemaatregelen zal derhalve moeten worden bezien of hun toepassing een beperking op het recht op privacy van de burger kan opleveren.

3.2 De maatregelen en het recht op privacy

3.2.1 Cameratoezicht op openbare plaatsen

Observatie, in welke vorm dan ook, van wat er in het openbaar gebeurt, maakt niet per definitie een inbreuk op het recht op privacy van de betrokkenen.[72] Bij het bepalen of cameratoezicht een beperking op het recht op privacy van de betrokkenen vormt, dient te worden gekeken naar een aantal factoren. In de eerste plaats vormt cameratoezicht

66. Kamerstukken II 1975-1976, 13 872, nr. 3, p. 41.
67. Kamerstukken II 1975-1976, 13 872, nr. 3, p. 41; zie ook HR 19 februari 1991, NJ 1992, 50 (Journalistieke filmopname demonstranten).
68. Registratiekamer, In beeld gebracht, Onderzoeksrapport van 27 januari 1997, p. 18, beschikbaar op www.CBPweb.nl.
69. EHRM 16 december 1992, Series A, 251-B (Niemietz tegen Duitsland), § 29.
70. EHRM 25 april 1978, Series A, 26 (Tyrer), § 31.
71. EHRM 15 juni 1992, Series A, 238 (Lüdi) en EHRM 25 september 2001, appl. 44787/98 (P.G. en J.H. tegen Verenigd Koninkrijk) § 56-57.
72. Zie onder andere HR 18 mei 1999, NJ 2000, 104 (4 M–zaak); HR 20 april 2004, LJN AL8449.

slechts een beperking op het recht op privacy van de betrokkene als zij betrekking heeft op een situatie waarin de betrokkene onbevangen zichzelf wil zijn of, zoals het EHRM het uitdrukt, waar de burger een reasonable expectation of privacy heeft.[73] Deze verwachting is echter niet doorslaggevend en er moet tevens worden gekeken naar factoren als het doel van het toezicht, de duur en frequentie, de kenbaarheid, het soort camera's dat voor het toezicht gebruikt wordt en het gebruik van de vergaarde beelden.[74]

Of een burger in een bepaalde situatie onbevangen zichzelf wil zijn is, gezien de subjectiviteit van dit criterium, moeilijk vast te stellen. De rechter heeft dit subjectieve criterium in een aantal uitspraken getracht te objectiveren door voor het bestaan van deze wens aanwijzingen te zoeken in de aard en intimiteit van de geobserveerde situatie en gedragingen[75] en te kijken naar de redelijke verwachting omtrent de bescherming van de persoonlijke levenssfeer die de betrokkene in een geobserveerde situatie kan hebben.[76] Deze laatste objectivering sluit aan bij het door het EHRM gehanteerde criterium van de reasonable expectation of privacy, waarbij wordt gekeken naar de mate van privacy die een burger redelijkerwijs mag verwachten in een bepaalde situatie.

Het cameratoezicht dat het wetsvoorstel beoogt te normeren ziet op openbare plaatsen in de zin van artikel 1 WOM. Hoewel algemeen aanvaard is dat een burger op een openbare plaats een minder grote verwachting van privacy mag hebben, kunnen zich ook hier situaties voordoen waarin burgers zich onbespied wanen en onbevangen zichzelf willen zijn, zeker als er niemand in de buurt is. Ook deze situaties kunnen onder de bescherming van het recht op privacy vallen.[77]

Zoals gezegd is de verwachting van de betrokkenen niet doorslaggevend. Er moet ook worden gekeken naar de genoemde andere factoren. Zo zal cameratoezicht minder snel een beperking van het recht op privacy zijn indien het toezicht noodzakelijk is in het belang van een legitiem doel dat in verband staat met de verantwoordelijkheid die het gemeentebestuur heeft ten aanzien van de ruimte.[78] Het toezicht waar artikel 151c lid 1 Gem.w. in voorziet, dient noodzakelijk te zijn in het belang van de handhaving van de openbare orde, één van de kerntaken van het gemeentebestuur. Indien een gemeentebestuur gemotiveerd aangeeft dat cameratoezicht in de betreffende gemeente noodzakelijk is in het belang van de openbare orde, zal er derhalve minder snel sprake zijn van een beperking.

Ook naar de duur en de frequentie van het toezicht moet worden gekeken. Naarmate toezicht langer duurt en er meer gebruikgemaakt wordt van de camera's zal er eerder sprake zijn van een situatie die onder de bescherming van het recht op privacy valt.[79] Het door het voorstel beoogde toezicht scoort op dit punt hoog omdat het hier doorgaans zal gaan om langdurig en stelselmatig toezicht. Het wetsvoorstel schrijft weliswaar voor dat de duur van het toezicht beperkt moet zijn maar het voorstel

---

73. EHRM 15 juni 1995, Series A, 238 (Lüdi); EHRM 25 september 2001, appl. 44787/98 (P.G. en J.H. tegen Verenigd Koninkrijk) en EHRM 28 januari 2003, appl. 44647/98 (Peck tegen Verenigd Koninkrijk).
74. HR 20 april 2004, LJN AL8449; HR 18 mei 1999, NJ 2000, 104 (4 M-zaak) en Kamerstukken II 1997-1998, 25 760, nr. 1, p. 6-9.
75. Hof Amsterdam 24 maart 1994, NJ 1994, 478 (video-observatie kleedruimte).
76. HR 19 december 1995, NJ 1996, 249 (Zwolsman).
77. EHRM 28 januari 2003, appl. 44647/98 (Peck tegen Verenigd Koninkrijk) en HR 19 december 1995, NJ 1996, 249 (Zwolsman).
78. HR 24 april 2004, LJN AL8449.
79. HR 19 december 1995, NJ 1996, 249 (Zwolsman).

schrijft geen maximum duur voor. Ook kan de duur van de plaatsing na afloop van de duur van het plaatsingsbesluit verlengd worden. Aan het daadwerkelijk gebruik van de camera's stelt het voorstel slechts de voorwaarde dat dit noodzakelijk is in het belang van de handhaving van de openbare orde. Het is dus mogelijk dat de camera's permanent gebruikt worden.

Voorts zal er minder snel sprake zijn van een beperking indien de burger weet of redelijkerwijs had kunnen weten dat de mogelijkheid bestaat dat hij op beelden voorkomt zodra hij een gebied betreedt waar door middel van camera's toezicht wordt gehouden. Ingevolge artikel 151c lid 4 van het voorstel dient de burger hiervan bij het betreden en verlaten van het gebied in kennis worden gesteld. Dit kan volgens de toelichting met behulp van borden aan de grenzen van het geobserveerde gebied.[80]

Tot slot dient te worden gekeken naar het soort camera's dat voor het toezicht gebruikt wordt en het gebruik van de beelden. Naarmate de camera's meer mogelijkheden hebben, als zij bijvoorbeeld verplaatsbaar zijn, kunnen zwenken en in en uit kunnen zoomen, spitst het toezicht zich meer toe op een individueel persoon en dringt daardoor dieper in in de persoonlijke levenssfeer van deze persoon. Dan zal eerder sprake zijn van een beperking. Ook het gebruik van de beelden kan in meer of mindere mate indringend zijn. Indien er slechts met de beelden wordt meegekeken en deze niet worden vastgelegd, is er doorgaans slechts sprake van een dermate beperkte inmenging dat niet kan worden gesproken van een beperking omdat de waarnemingen ook door een aanwezige persoon hadden kunnen worden gedaan.[81] Legt de politie de beelden echter vast, dan zal er eerder sprake zijn van een beperking,[82] evenals wanneer zij met behulp van bepaalde bewerkingstechnieken uit de beelden meer persoonsgegevens kan afleiden, de vergaarde gegevens koppelt aan andere bestanden en de beelden voor andere doelen kan gebruiken en aan derden kan doorgeven.[83]

Het hier behandelde voorstel voorziet blijkens artikel 151 c lid 1 in het gebruik van vaste camera's. Deze camera's kunnen blijkens de MvT echter wel dynamisch zijn in de zin dat het mogelijk is dat de camera's kunnen zwenken en er met de camera's in- en uitgezoomd kan worden.

Met de gemaakte beelden kan volgens het voorstel direct worden meegekeken, maar zij kunnen tevens worden vastgelegd en gedurende ten hoogste zeven dagen bewaard.[84] Het gebruik van meer verfijnde zoek- en analysemethoden, zoals identificatie van personen, wordt door het voorstel niet uitgesloten.[85] Het voorstel normeert het gebruik van deze methoden niet omdat het hier volgens de regering gaat om een techniek die nog in ontwikkeling is. Hier kan de regering wel op een later moment op

---

80. Kamerstukken II 2003-2004, 29 440, nr. 17.
81. ECRM 14 januari 1998, DR 92-B, p. 92. (Herbecq en de vereniging 'Ligue des droits de l'homme' tegen België).
82. EHRM 25 september 2001, appl. 44787/98 (P.G. en J.H. tegen Verenigd Koninkrijk) § 57; EHRM 16 februari 2000, appl. 27798/95, § 69 and 80 (Amann tegen Zwitserland [GC]); EHRM 4 mei 2000, appl. 28341/95, § 46 (Rotaru tegen Roemenië).
83. Kamerstukken II 1997-1998, 25 760, nr. 1, p. 7-8.
84. In de praktijk worden de gemaakte beelden thans in 42% van de gemeenten die cameratoezicht gebruiken slechts achteraf bekeken, in 36% van de gemeenten wordt 'live' meegekeken op bepaalde vastgestelde tijdstippen en op de overige momenten slechts achteraf, in 19%van de gemeenten wordt slechts 'live' meegekeken. In 90% van de gemeenten worden de beelden vastgelegd, driekwart van deze gemeenten bewaart de beelden langer dan 24 uur en een kwart bewaart deze beelden zelfs langer dan 7 dagen. CBP, Cameratoezicht in de openbare ruimte, Rapport 1, november 2003, p. 9. Beschikbaar op www.CBPweb.nl.
85. Kamerstukken II 2003-2004, 29 440, nr. 3, p. 7.

grond van artikel 151c lid 8 Gem.w., bij algemene maatregel van bestuur (amvb) in voorzien. Gezien het gebruik dat een aantal gemeenten nu al maakt van softwareprogramma's met bijvoorbeeld zoekfuncties en gezichtsherkenning lijkt het mij dat een dergelijke nadere regeling niet lang op zich moet laten wachten.[86]

Het is niet toegestaan om de gemaakte beelden en vergaarde persoonsgegevens aan andere gegevensbestanden te koppelen. Dit gebruik gaat teveel in de richting van toezicht op specifieke personen terwijl het voorstel meer in het algemeen ziet op toezicht in het kader van de handhaving van de openbare orde. De regering meent dat dit gebruik gezien de doelstelling van het voorstel te ver gaat.[87] De vastgelegde beelden kunnen ingevolge en onder de voorwaarden van artikel 13 Wet Pol.r. door politie en justitie worden gebruikt voor de opsporing van een concreet strafbaar feit omdat deze beelden volgens artikel 151c lid 7 Gem.w. een politieregister vormen.

In het verleden zijn het CBP, het toenmalige kabinet en ook de rechter met toepassing van deze criteria tot de conclusie gekomen dat cameratoezicht op openbare plaatsen een dermate beperkte inmenging in het privé-leven van de betrokkene met zich meebrengt dat niet kan worden gesproken van een beperking van het recht op privacy zoals dat beschermd wordt door artikel 10 lid 1 Grw en artikel 8 lid 1 EVRM.[88] Deze conclusie is in een concreet geval wellicht terecht geweest doch dit kan mijns inziens niet in het algemeen worden volgehouden.

Ook cameratoezicht op openbare plaatsen zoals dat is voorzien door het wetsvoorstel kan naar mijn mening een beperking van het recht op privacy met zich meebrengen. Hoewel de gedragingen die met het toezicht waargenomen worden plaatsvinden in de openbare ruimte waar een burger minder de verwachting kan hebben dat wat hij doet onopgemerkt blijft, heeft de burger ook in de openbare ruimte recht op een zekere bescherming van zijn privacy. Een concrete toepassing van de door het voorstel te introduceren regeling kan dan ook een inmenging op het recht op privacy van de burgers met zich meebrengen.

Het toezicht waarin het wetsvoorstel voorziet, is langdurig en stelselmatig van karakter, de camera's worden op een potentieel indringende manier gebruikt en de beelden kunnen worden vastgelegd en gedurende langere tijd worden bewaard. Darnaast kunnen uit de beelden met behulp van geavanceerde technieken meer persoonsgegevens worden afgeleid en kunnen de beelden worden gebruikt voor andere doeleinden dan toezicht ten behoeve van de handhaving van de openbare orde. Dit zijn mijns inziens factoren die, bij elkaar opgeteld, tot de conclusie moeten nopen dat een concrete toepassing van de door het voorstel te introduceren regeling meer dan een beperkte inmenging op het recht op privacy kan vormen. Een inmenging die, wil deze rechtmatig zijn, dient te voldoen aan de eisen die artikel 8 lid 2 EVRM en artikel 10 lid 1 Grw stellen aan een gerechtvaardigde beperking.

---

86. CBP, Cameratoezicht in de openbare ruimte, Rapport 1, november 2003, p. 10. Beschikbaar op www.CBPweb.nl.
87. Kamerstukken II 2003-2004, 29 440, nr. 3, p. 8.
88. Zie hieromtrent onder andere Registratiekamer, In beeld gebracht, Onderzoeksrapport van 27 januari 1997, beschikbaar op www.CBPweb.nl, Kamerstukken II 1997-1998, 25 760, nr. 1, HR 24 april 2004, LJN AL8449, ECRM 14 januari 1998, D&R 92-B (1998) (Herbecq en de vereniging 'Ligue des droits de l'homme' tegen België).

3.2.2 Preventief fouilleren

Op basis van artikel 50 lid 3, 51 lid 3 en 52 lid 3 WWM mogen politieambtenaren in een veiligheidsrisicogebied tijdens een actie waarbij zij overgaan tot preventief fouilleren een drietal bevoegdheden uitoefenen ten aanzien van alle zich in het gebied bevindende personen en voertuigen. Allereerst krijgen zij ten aanzien van personen de bevoegdheid tot het verrichten van een onderzoek aan de kleding. Daarnaast krijgen zij de bevoegdheid bagage en verpakkingen die een persoon bij zich draagt te onderzoeken en mogen zij het vervoersmiddel waarin een persoon zich vervoert onderzoeken. Van de toepassing van deze bevoegdheden zal moeten worden onderzocht of zij een inbreuk op het recht op privacy zoals dat beschermd wordt door de artikelen 10 lid 1 Grw en artikel 8 lid 1 EVRM opleveren.

Het recht op privacy dat deze bepalingen beschermen, is in de eerste plaats een afweerrecht dat de burger beoogt te vrijwaren van ongewenste inmenging van de overheid met zijn privé-leven en daaronder valt ook zijn persoon.[89] De grondwetgever achtte deze persoonlijke of fysieke integriteit zelfs een dermate belangrijk aspect van het recht op eerbiediging van de persoonlijke levenssfeer dat hij een aparte bepaling heeft gewijd aan het recht op onaantastbaarheid van het menselijk lichaam, artikel 11 Grw. De reikwijdte van deze verbijzondering van het recht op eerbiediging van de persoonlijke levenssfeer is ruim, getuige de veelheid van situaties die blijkens de toelichting onder de bescherming van dit recht vallen.[90] In het algemeen heeft artikel 11 Grw betrekking op gevallen waarin het lichaam daadwerkelijk wordt aangeraakt, bijvoorbeeld inentingen en onderzoek aan het lichaam. De situatie waarin het lichaam op minder directe wijze wordt aangeraakt, zoals een onderzoek aan de kleding, valt niet onder de reikwijdte van artikel 11 Grw maar onder het meer algemene artikel 10 Grw.[91]

Ook verpakkingen en bagage die iemand bij zich draagt en het vervoermiddel waarin hij zich vervoert, worden gerekend tot de privé-sfeer die door artikel 10 lid 1 Grw en artikel 8 EVRM beschermd wordt, daar zij behoren tot het domein van het persoonlijk leven waar buitenstaanders in beginsel niets mee te maken hebben. Het aan een onderzoek onderwerpen van deze onderdelen van de privé-sfeer vormt derhalve een beperking van het recht op privacy zoals beschermd door artikel 10 lid 1 Grw en artikel 8 lid 1 EVRM.[92]

3.2.3 De uitgebreide identificatieplicht

Volgens sommigen valt onder het recht op privacy ook het recht van een individu om zelf te bepalen op welke wijze, op welk moment en in welke mate informatie over hem

---

89. Zie omtrent dit recht van persoonlijke of fysieke integriteit voor artikel 10 lid 1 Grw, Kamerstukken II 1975-1976, 138 722, nr. 3, p. 40 en 41 en voor artikel 8 lid 1 EVRM onder meer appl. 8239/78, X. tegen Nederland, D&R 16 (1979), p. 189, appl. 8278/78, X. tegen Oostenrijk, D&R 18 (1980), p. 156.
90. Kamerstukken II 1978-1979, 15 463, nr. 2, p. 4-5.
91. M.A.D.W. de Jong, H.R.B.M. Kummeling en M.C. Burkens, Het gebruik van gemeentelijke noodbevoegdheden, Zwolle: W.E.J. Tjeenk Willink 1994, p. 163. Zie ook Kamerstukken II 1979-1980, 16 086, nr. 3, p. 6 en L.F.M. Verhey, Horizontale werking van grondrechten, in het bijzonder het recht op privacy, Zwolle: W.E.J. Tjeenk Willink 1992, p. 259 en J.J.H. Suyver, Politie in de rechtsorde (Serie: Studiepockets Staats- en Bestuursrecht nr. 7), Zwolle 1994, p. 76.
92. ECRM 30 mei 1974, Yearbook XVII 1974, p. 226 (X. tegen België).

wordt verstrekt, het informationele zelfbeschikkingsrecht.[93] Indien deze opvatting algemeen aanvaard zou zijn, zou de vordering om inzage in een geldig identificatiebewijs zonder twijfel een inmenging in het privé-leven van de burger zijn. Hoewel artikel 10 lid 1 Grw het recht op informationele privacy wel beschermt, volgen de wetgever en de rechter deze zelfbeschikkingsrechtopvatting niet.[94] Hoever de bescherming van de informationele privacy dan wel reikt, is afhankelijk van een aantal factoren.

In de eerste plaats dient te worden gekeken naar de aard en indringendheid van de informatie die van of over iemand gevorderd wordt. Hoe gevoeliger deze gegevens zijn, hoe eerder er sprake zal zijn van een beperking van het recht op privacy.[95] Daar een identiteitsbewijs slechts gegevens als de naam, geboortedatum, geboorteplaats en het sofi-nummer bevat, zal op basis van dit criterium niet snel geconcludeerd worden dat er sprake is van een meer dan beperkte aantasting van de persoonlijke levenssfeer.

De aard en indringendheid van de informatie hoeft echter niet doorslaggevend te zijn. Een aantasting van de privacy kan volgens de grondwetgever ook het gevolg zijn van het gebruik van deze op het oog onschuldige gegevens.[96] Indien gegevens omtrent een persoon met elkaar in verband gebracht worden en de aldus verkregen informatie wordt gebruikt als grondslag van een belangrijke beslissing ten aanzien van deze persoon kan er, ondanks het onschuldige karakter van de gegevens, sprake zijn van een beperking van het recht op privacy.[97] Daar een (buitengewoon) opsporingsambtenaar of een toezichthoudend ambtenaar een vordering tot inzage in een identiteitsbewijs op grond van de nieuwe wet slechts mag doen indien dit redelijkerwijs noodzakelijk is voor de uitoefening van zijn taak, is het niet ondenkbaar dat de informatie wordt gebruikt voor een belangrijke beslissing ten aanzien van deze persoon. Daarbij kan bijvoorbeeld worden gedacht aan het in het kader van de handhavingstaak van een toezichthoudend ambtenaar opleggen van een bestuursrechtelijke sanctie. Dit is ook precies de reden waarom de regering een uitgebreide identificatieplicht wil introduceren; voorkomen dat een burger zich met een beroep op de in het publieke domein heersende anonimiteit onttrekt aan de verantwoordelijkheid van zijn handelen.[98]

Artikel 8 EVRM beschermt eveneens het recht op informationele privacy, ook het door dit artikel beschermde recht gaat echter niet zo ver als een informationeel zelfbeschikkingsrecht. Het EHRM lijkt voor de bescherming van het recht op informationele privacy een lijn te volgen die vergelijkbaar is met die van de Nederlandse grondwetgever en de Nederlandse rechter, waarbij het enerzijds kijkt naar het karakter van de informatie en de situatie waarin zij vergaard is en anderzijds kijkt naar het gebruik van deze informatie. Op basis van het eerste criterium kwam de Europese Commissie voor de Rechten van de Mens[99] in een zaak tegen België nog tot de

---

93. NJCM-commentaar op de notitie identificatieplicht, NJCM 14-1 (1989), p. 111 en NJCM-commentaar op het concept wetsvoorstel identificatieplicht, Privacy en registratie, 1993/3, p. 8. De definitie is ontleend aan A.F. Westin, Privacy and Freedom, New York 1970, p. 7.
94. Kamerstukken II 1986-1987, 19 095, nr. 6, p. 15.
95. Kamerstukken II 1975-1976, 13 872, nr. 3, p. 41 en onder andere HR 9 januari 1987, NJ 1987, 928 (Edamse bijstandsmoeder) en HR 1 juli 1988, NJ 1988, 1000 (Vondelpark).
96. Kamerstukken II 1975-1976, 13 872, nr. 3, p. 41.
97. L.F.M. Verhey, Privacy en lichamelijke integriteit: op zoek naar een evenwicht, in: J.B.J.M. ten Berge, P.J.J. van Buuren, H.R.B.M. Kummeling en B.P. Vermeulen (red.), De Grondwet als voorwerp van aanhoudende zorg (Burkens-bundel), Zwolle: W.E.J. Tjeenk Willink 1995, p. 150.
98. Kamerstukken II 2003-2004, 29 218, nr. 3, p. 1.
99. Met de inwerkingtreding van het elfde protocol van het EVRM op 1 november 1998 is de Europese Commissie voor de Rechten van de Mens afgeschaft. Haar taken zijn overgenomen door het EHRM.

conclusie dat de aldaar geldende uitgebreide identificatieplicht geen beperking van het recht op privacy vormde gezien het onschuldige karakter van de in het identificatiebewijs opgenomen gegevens.[100] Inmiddels lijkt het EHRM, hoewel het zich sindsdien niet heeft uitgesproken over een identificatieplicht in relatie tot artikel 8 EVRM,[101] in andere zaken over gegevensverwerking te hebben aangenomen dat er wel sprake kan zijn van een beperking van het recht op privacy indien de vergaarde gegevens worden gebruikt op een manier die nadelige gevolgen heeft voor de burger.[102]

Als men dit criterium toepast op de uitgebreide identificatieplicht, leiden de mogelijke nadelige gevolgen die een identificatieplicht kan hebben voor een burger mijns inziens tot de conclusie dat deze plicht in een concreet geval een beperking van het recht op privacy kan opleveren. Omdat op voorhand niet kan worden gezegd of een vordering tot inzage in een identiteitsbewijs op basis van dit gebruikscriterium een aantasting van het recht op privacy van de burger meebrengt, dient de regeling omtrent de uitgebreide identificatieplicht naar mijn mening in zijn geheel te worden gezien als beperking van het recht op privacy zoals beschermd door artikel 8 EVRM en artikel 10 lid 1 Grw.

3.3 Tussenconclusie

Kort samengevat kan de toepassing van cameratoezicht in de openbare ruimte, preventief fouilleren en de uitgebreide identificatieplicht derhalve een beperking van het door artikel 10 lid 1 Grw en artikel 8 lid 1 EVRM met zich meebrengen. Cameratoezicht op openbare plaatsen vormt, ondanks dat de waargenomen gedragingen in het openbaar plaatsvinden, een beperking van het recht op privacy omdat de mogelijke aard en intimiteit van de waargenomen gedragingen en de situatie waarin de gedragingen plaats kunnen vinden en het gebruik van de gegevens meebrengen dat er sprake is van meer dan een beperkte inmenging met het recht op privacy. De bevoegdheden die in het kader van preventief fouilleren mogen worden toegepast, vormen een beperking van het recht op privacy omdat zij de burger aantasten in zijn persoonlijke integriteit en de burger raken in de onderdelen van de privé-sfeer waar buitenstaanders niets mee te maken hebben. En tot slot is de nieuwe uitgebreide identificatieplicht een beperking van het recht op privacy, niet zozeer vanwege de aard en intimiteit van de gegevens die gevorderd worden, maar vanwege de ingrijpende gevolgen die het gebruik van deze gegevens kan hebben voor de burger.

---

100. Appl. 16810/90, D&R 73 (1992), p. 152 (Filip Reyntjens tegen België).
101. Het EHRM heeft zich in 2003 in een zaak over artikel 5 EVRM nog wel uitgesproken over Deense identificatieplicht, EHRM 25 september 2003, appl. 52792/99, § 39 (Vasileva tegen Denemarken).
102. EHRM 28 januari 2003, appl. 44647/98, § 60 en 61 (Peck tegen Verenigd Koninkrijk); EHRM 16 februari 2000, appl. 27798/95, § 69 and 80 (Amann tegen Zwitserland [GC]); EHRM 4 mei 2000, appl. 28341/95, § 46 (Rotaru tegen Roemenië).

4 De rechtmatigheid van de beperking van het recht op privacy

Nu is vastgesteld dat de toepassing de controlemaatregelen zoals die voorzien is door de relevante (voorgestelde) regelgeving een beperking van het recht op privacy zoals beschermd door artikel 10 lid 1 Grw en artikel 8 EVRM kan opleveren, dient te worden bezien of deze beperkingen gerechtvaardigd kunnen worden onder de beperkingsclausules van artikel 10 lid 1 Grw en artikel 8 lid 2 EVRM. Daarbij moet vooral worden gekeken naar de vraag of de (voorgestelde) regelingen voldoende waarborgen bieden gezien de eisen die artikel 10 lid 1 Grw en artikel 8 lid 2 EVRM stellen.

Om deze vraag te beantwoorden zal ik eerst in paragraaf 4.1 in algemene zin uiteenzetten onder welke voorwaarden het recht op privacy kan worden beperkt. Vervolgens zal ik in paragraaf 4.2 nagaan of de relevante regelgeving voldoende waarborgen biedt om een concrete toepassing van de maatregel te laten voldoen aan het samenstel van deze voorwaarden.

4.1 Beperking van het recht op privacy

Ingevolge artikel 10 lid 1 Grw heeft een ieder, behoudens bij of krachtens wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. Artikel 10 lid 1 Grw eist voor iedere beperking een formeel wettelijke grondslag.[103] Wel geeft artikel 10 lid 1 Grw de wetgever de bevoegdheid om nadere regelgeving over te laten aan lagere regelgevers. In de jurisprudentie heeft de Hoge Raad de eis van de formeel wettelijke grondslag nader gepreciseerd door te eisen dat deze grondslag specifiek bedoeld moet zijn om het grondrecht te beperken.[104]

Ook artikel 8 EVRM kan onder bepaalde voorwaarden rechtmatig beperkt worden. Op grond van het tweede lid kan het in het eerste lid gegeven recht worden beperkt indien de beperking bij wet is voorzien, noodzakelijk is in een democratische samenleving en deze noodzaak gerelateerd is aan één van de in artikel 8 lid 2 EVRM opgesomde legitieme belangen.

---

103. Wanneer de grondwetgever in de Grondwet de term wet gebruikt bedoelt zij daarmee een wet in formele zin. Zie hieromtrent onder andere C.W. van der Pot en A.M. Donner, Handboek van het Nederlandse staatsrecht, bewerkt door L. Prakke, J.L. de Reede en G.J.M. van Wissen, Zwolle: W.E.J. Tjeenk Willink 2001, p. 251.
104. Zie hieromtrent ABRvS 26 april 1995, AB 1996, 208 (Drugspand Venlo).

Met de voorwaarde 'bij wet voorzien' wordt vereist dat een regeling op basis waarvan het recht beperkt wordt voldoende toegankelijk is (adequately accessible), de burger moet een naar de omstandigheden van het geval toereikende indicatie hebben van de regels die op hem van toepassing zijn. Daarnaast dient de regeling voldoende nauwkeurig te zijn geformuleerd opdat de burger de gevolgen van de niet-naleving van de regeling redelijkerwijs kan voorzien (foreseeability).[105] Het EHRM accepteert daarbij dat het noodzakelijk kan zijn dat een wet een zekere mate van beoordelingsvrijheid (discretion) laat. Het EHRM stelt hieraan echter de voorwaarde dat, indien een wet deze beoordelingsvrijheid laat, zij met een redelijke mate van duidelijkheid moet aangeven wat de reikwijdte van deze beoordelingsvrijheid is.[106]

Vervolgens dient de beperking noodzakelijk te zijn in een democratische samenleving in het belang van de in artikel 8 lid 2 EVRM limitatief opgesomde legitieme doelen. In het kader van de noodzakelijkheidstoets dient de beperking tegemoet te komen aan een dringende maatschappelijke behoefte (pressing social need), moet de beperking in een evenredige verhouding staan tot het met de beperking nagestreefde doel en moeten de voor de beperking aangevoerde redenen relevant en toereikend zijn. In het kader van de in deze voorwaarde aangelegde proportionaliteitstoets gaat het EHRM na of een beperking niet onevenredig groot is gezien het doel dat met de beperking wordt nagestreefd en of het nagestreefde doel niet op een andere, minder ingrijpende manier had kunnen worden gerealiseerd. Daarbij kijkt het EHRM naar factoren als de ernst van de inmenging in het privé-leven, de effectiviteit van de beperkende maatregel (alleen en in combinatie met andere maatregelen) bij het realiseren van het nagestreefde doel en de waarborgen voor de burger.[107] De regeling dient de burger een effectief rechtsmiddel te bieden tegen een beperking van zijn recht op privacy. Dit brengt onder andere met zich mee dat de beoordelende instantie moet kunnen oordelen over de inhoud van de klacht, een toereikende voorziening moet kunnen treffen en een bindend oordeel moet kunnen geven.[108]

Bij het bepalen of een beperking noodzakelijk is in een democratische samenleving in het belang van een van de doelcriteria, heeft de nationale overheid vaak een zekere beoordelingsmarge (*margin of appreciation*). Deze beoordelingsmarge gaat echter hand in hand met Europees toezicht. Het is uiteindelijk het EHRM dat bepaalt of de nationale overheid in een concreet geval een *margin of appreciation* heeft en hoe ver deze reikt.[109] Uit het bestaan van deze beoordelingsmarge kan evenmin worden afgeleid dat de nationale rechter slechts marginaal mag toetsen.

---

105. EHRM 26 april 1979, Series A, 30, § 49 (Sunday Times).
106. EHRM 7 december 1976, Series A, 24, § 48. (Handyside), EHRM 25 maart 1983, Series A, 61, § 22 (Silver tegen Verenigd Koninkrijk); EHRM 2 augustus 1984, Series A, 82, § 66 (Malone tegen Verenigd Koninkrijk). Zie eveneens P. Van Dijk en G.J. van Hoof, Theory and Practice of the European Convention on Human Rights, London/Boston/The Hague: Kluwer Law International 1998 (derde druk), p. 82-93.
107. EHRM 7 december 1976, Series A, 24, § 48. (Handyside).
108. Hierbij is aansluiting gezocht bij artikel 13 EVRM. EHRM 7 juli 1989, Series A, 161, p.27-28 (Soering tegen Verenigd Koninkrijk) en EHRM 25 februari 1997, Reports of judgments and Decisions 1997-I, p, § 95 (Z tegen Finland).
109. EHRM 7 december 1976, Series A, 24, § 48. (Handyside). Zie hieromtrent eveneens P. Van Dijk en G.J. van Hoof (red.), Theory and Practice of the European Convention on Human Rights, London/Boston/The Hague: Kluwer Law International 1998 (derde druk), p. 82-93.

4.2 De rechtmatigheid van de beperkingen als gevolg van de toepassing van de maatregelen

4.2.1 Cameratoezicht op openbare plaatsen

Grondslag in een wet in formele zin en bij wet voorzien

De beperking op het recht op eerbiediging van de persoonlijke levenssfeer die het gebruik van cameratoezicht op openbare plaatsen met zich kan meebrengen, is gebaseerd op artikel 151c Gem.w. Deze bepaling is specifiek met het oog op de beperking van dit grondrecht tot stand gebracht. Daarmee voldoet deze beperking aan de door artikel 10 lid 1 Grw gestelde eis van grondslag in een wet in formele zin. Door het stellen van nadere regels en de uitoefening van deze bevoegdheid aan de burgemeester over te laten maakt het voorstel gebruik van de door artikel 10 lid 1 Grw geboden mogelijkheid tot delegatie.

Artikel 8 EVRM eist dat het gebruik van cameratoezicht bij wet voorzien is. Aan dit vereiste is echter niet noodzakelijk voldaan als voldaan is aan de voorwaarden van artikel 10 lid 1 Grw. De voorwaarde 'bij wet voorzien' eist dat het cameratoezicht kenbaar en voorzienbaar is. Met de publicatie van de verordening waarin de gemeenteraad de burgemeester bevoegdheid verleent tot het plaatsen van camera's en het in het voorgestelde artikel 151c lid 4 Gem.w. gestelde vereiste dat het gebruik van camera's in een bepaald gebied voor de burgers voldoende duidelijk moet zijn, wordt in belangrijke mate aan dit vereiste voldaan.

Op het punt van de voorzienbaarheid van de gevolgen van de regeling vraag ik mij echter af of op basis van het in lid 4 gestelde kenbaarheidvereiste wel voldoende duidelijk is voor de burger gedurende welke tijden er van de camera's gebruik wordt gemaakt en op welke wijze dat gebeurt. Worden de beelden vastgelegd of wordt er rechtstreeks meegekeken? Volgens de toelichting op lid 4 dient op grond van dit lid aan de burgers duidelijk te worden gemaakt dat er in een bepaald gebied gebruik wordt gemaakt van cameratoezicht, niet op welke tijden en op welke wijze.[110] Aan dit bezwaar zou mijns inziens tegemoet gekomen kunnen worden door ook de publicatie van het plaatsingsbesluit van de burgemeester verplicht te stellen. In het licht van het EHRM zal dit punt naar mijn mening evenwel geen problemen opleveren. Het is in ieder geval bekend in welk gebied er gebruik gemaakt kan worden van cameratoezicht en het EVRM laat de nationale overheid op dit punt een beperkte mate van beleidsvrijheid.[111]

Legitiem belang en pressing social need

Vervolgens dient de beperking ingevolge artikel 8 lid 2 EVRM noodzakelijk te zijn in het belang van één van de in dit artikel genoemde doelcriteria en tegemoet te komen aan een zwaarwegend maatschappelijk belang. Het zal niet aan twijfel onderhevig zijn dat het cameratoezicht, dat ingevolge artikel 151c lid 1 Gem.w. noodzakelijk dient te

110. Kamerstukken II 2003-2004, 29 440, nr. 3. p. 17.
111. EHRM 2 augustus 1984, Series A, 82, § 66 (Malone tegen Verenigd Koninkrijk).

zijn in het belang van de handhaving van de openbare orde, in beginsel een legitiem belang dient in de zin van artikel 8 lid 2 EVRM.[112]

Uit de veiligheidsanalyses die aan de bevoegdheidsverlening aan de burgemeester en het plaatsingsbesluit van de burgemeester vooraf dienen te gaan, dient voorts te blijken dat cameratoezicht noodzakelijk is gezien de veiligheidsrisico's die zich met enige regelmaat in de betreffende gemeente en het concrete gebied voordoen. Deze veiligheidsrisico's kunnen een voldoende zwaarwegend belang vormen om tegemoet te komen aan de door het EHRM in het kader van de noodzakelijkstoets gestelde eis van een 'pressing social need'. Of dit in een concrete situatie het geval is, zal in de eerste instantie door het bestuur maar vervolgens door de rechter moeten worden beoordeeld aan de hand van de motivering van het plaatsingsbesluit en de gegevens over de concrete feiten en omstandigheden in het betreffende gebied.

Proportionaliteit

Ten slotte dient de vraag te worden beantwoord of het gebruik van cameratoezicht zoals het wetsvoorstel dit voorziet noodzakelijk is in het belang van de handhaving van de openbare orde. In dit kader dient te worden bezien of het middel wel evenredig is gezien dit doel en het doel niet op een minder ingrijpende wijze kan worden gerealiseerd.

Wanneer er rechtstreeks met de gemaakte beelden wordt meegekeken en cameratoezicht wordt gebruikt in combinatie met andere maatregelen, zodat er daadwerkelijk kan worden ingegrepen als er zich incidenten voordoen, is cameratoezicht in de openbare ruimte, naar mijn mening, een proportioneel middel in verhouding tot het doel dat het met het toezicht gediend wordt. Het gaat in dat geval om een beperkte inmenging met het privé-leven van de betrokkenen waarvan men zich kan afvragen of dit een beperking van het recht op privacy oplevert. Burgers dienen zich in de openbare ruimte immers bewust te zijn van de mogelijkheid dat ze gezien worden en deze waarneming had eveneens door een in het gebied aanwezige politiefunctionaris gedaan kunnen worden.[113] Indien deze beperkte inmenging wel wordt gezien als beperking van het recht op privacy, kan worden gesteld dat deze beperking een belang dient dat waarschijnlijk niet even efficiënt en op minder ingrijpende wijze met andere middelen kan worden gerealiseerd.

Het voorstel voorziet echter niet alleen in het rechtstreeks meekijken met de gemaakte beelden maar tevens in de mogelijkheid dat de beelden worden opgeslagen en gedurende maximaal zeven dagen worden bewaard (artikel 151c lid 7 Gem.w.). Het opslaan en bewaren van gemaakte beelden vormt een zwaardere inmenging in het privé-leven van de betrokkene dan het louter waarnemen van de beelden. Het nationale recht dient dan ook te voorzien in voldoende waarborgen om het recht op respect voor het privé-leven van de betrokkene te beschermen.[114]

Zo dient ook het opslaan en bewaren van de gemaakte beelden te voldoen aan het vereiste van noodzakelijkheid ten behoeve van het door het toezicht gediende legitieme

---

112. Het belang van handhaving van de openbare orde kan worden ondergebracht bij zowel openbare veiligheid of het voorkomen van wanordelijkheden en strafbare feiten als de bescherming van rechten en vrijheden van anderen.
113. ECRM 14 januari 1998, DR 92-B, p. 92 (Herbecq en de vereniging 'Ligue des droits de l'homme' tegen België).
114. EHRM 25 februari 1997, Reports of judgments and Decisions 1997-I, p. 348, § 99 (Z tegen Finland). EHRM 16 februari 2000, appl. 27798/95, § 69 and 80 (Amann tegen Switzerland [GC]); EHRM 4 mei 2000, appl. 28341/95, § 46 (Rotaru tegen Roemenië).

belang. Cameratoezicht wordt in de praktijk ervaren als een waardevol hulpmiddel bij de handhaving van de openbare orde vanwege de extra waarneming die het toezicht biedt waardoor de beperkte politiecapaciteit efficiënter kan worden ingezet. Het gebruik van de gemaakte beelden achteraf daarentegen komt voornamelijk ten goede aan de opsporing en vervolging van strafbare feiten, en dit is juist niet de primaire doelstelling van handhaving van de openbare orde.[115] Indien bevordering van de veiligheid in het kader van de handhaving van de openbare orde de doelstelling van het cameratoezicht in de openbare ruimte is, vraag ik mij af of het in het licht van dit belang wel noodzakelijk is dat gemaakte beelden opgeslagen en bewaard kunnen worden.

Als redenen voor het opslaan en bewaren van de beelden worden genoemd de evaluatie van het eigen optreden, het preventieve effect dat van de mogelijkheid van het achteraf bekijken van de beelden uitgaat en het gevoel van veiligheid dat de aanwezigheid van de camera's oproept.[116] Ten aanzien van de evaluatie van het eigen optreden vraag ik mij af of er nog wel een relevant belang is en of dit belang nog wel in een evenredige verhouding staat tot het belang van de handhaving van de openbare orde. Dit doel kan immers op een minder ingrijpende manier gerealiseerd worden, bijvoorbeeld door incidenteel beelden vast te leggen of waarnemers mee de straat op te sturen.

Voorts is uit verschillende onderzoeken naar de effectiviteit van cameratoezicht gebleken dat het aantal incidenten in de gebieden met cameratoezicht niet noemenswaardig gedaald is.[117] Een preventief effect lijkt dus in de praktijk niet uit te gaan van de aanwezigheid van de camera's en de mogelijkheid dat de beelden achteraf worden bekeken. Het gevoel van veiligheid is volgens dezelfde onderzoeken wel toegenomen, maar het is de vraag of de loutere vergroting van het gevoel van veiligheid onder de burgers wel past binnen de doelcriteria van artikel 8 lid 2 EVRM. De doelcriteria openbare veiligheid en bescherming van rechten en vrijheden van anderen lijken blijkens de jurisprudentie van het EHRM immers voornamelijk te zien op de objectieve veiligheid.[118]

Het belang van het opslaan van bewaren van de beelden bij het realiseren van de doelstelling van het handhaven van de openbare orde is naar mijn mening niet voldoende aannemelijk en de beperking op het recht op privacy zoals beschermd door artikel 8 EVRM die het opslaan en bewaren van de beelden met zich meebrengt staat mijn inziens dan ook niet in een evenredige verhouding tot het nagestreefde doel.

In de laatste plaats dient in het kader van de proportionaliteitstoets te worden gekeken naar de waarborgen die het voorstel biedt voor de burgers. De regeling dient de burger een effectief rechtsmiddel te bieden tegen een beperking van zijn recht op privacy als gevolg van het gebruik van cameratoezicht.

In de eerste plaats heeft de burger, zoals in paragraaf 2.1.3 is beschreven, het recht om de beslissing van de gemeenteraad om de burgemeester de bevoegdheid te verlenen camera's te plaatsen en het plaatsingsbesluit van de burgemeester aan te vechten bij de

---

115. Handelingen Eerste Kamer 13 december 1988, p. 11-370, zie hieromtrent eveneens M.A.D.W. de Jong, Orde in beweging, Deventer: W.E.J. Tjeenk Willink 2000, p. 18-19.
116. CBP, Cameratoezicht in de openbare ruimte, Rapport 1, november 2003, p. 17. Beschikbaar op www.CBPweb.nl.
117. I. Leiden en H.B. Ferwerda, Cameratoezicht goed bekeken?, SEC 2003, nr. 3, S. Flight, Effecten van cameratoezicht, SEC 2003, nr. 5. Beschikbaar via www.justitie.nl.
118. P. Van Dijk en G.J. van Hoof (red.), Theory and Practice of the European Convention on Human Rights, London/Boston/The Hague: Kluwer Law International 1998, p. 771-772.

burgerlijke rechter. Daarnaast is een belangrijke waarborg gelegen in de aanmerking van de met behulp van cameratoezicht gemaakte beelden als politieregister (artikel 151c lid 6 Gem.w.). Dit betekent dat de normen van de Wet Politieregisters inzake inzage, correctie en verwijdering van gegevens, zoals omschreven in paragraaf 2.1.2, van toepassing zijn. De burger heeft tevens de mogelijkheid om beslissingen op zijn verzoeken met betrekking tot over hem in het register opgenomen gegevens aan te vechten bij de bestuursrechter. Hiermee biedt het voorstel naar mijn mening voldoende waarborgen om een burger te beschermen tegen een beperking van zijn recht op privacy als gevolg van het gebruik van cameratoezicht.

4.2.2 Preventief fouilleren

Grondslag in een wet in formele zin en bij wet voorzien
Alvorens de officier van justitie in een bepaald gebied een actie preventief fouilleren kan gelasten, dient de burgemeester dat gebied eerst aan te wijzen als veiligheidsrisicogebied ingevolge een hem daartoe door de gemeenteraad bij verordening verleende bevoegdheid. De gemeenteraad ontleent zijn bevoegdheid om de burgemeester de bevoegdheid tot aanwijzing van een veiligheidsrisicogebied te verlenen op zijn beurt aan, het specifiek met het oog op de beperking van het recht op eerbiediging van de persoonlijke levenssfeer in het leven geroepen, artikel 151b Gem.w. Met deze gelaagde structuur van besluitvorming wordt voldaan aan artikel 10 lid 1 Grw, dat voor een beperking een grondslag in een wet in formele zin eist maar delegatie aan lagere regelgevers toelaat.

Artikel 8 EVRM eist dat een actie preventief fouilleren bij wet voorzien is. Wederom is aan dit vereiste niet noodzakelijk voldaan als voldaan is aan de voorwaarden van artikel 10 lid 1 Grw. De actie dient volgens het EVRM kenbaar en voorzienbaar te zijn. Zowel de verordening waarin de gemeenteraad de burgemeester de aanwijzingsbevoegdheid verleent als het daadwerkelijke aanwijzingsbesluit dienen ingevolge artikel 3:42 Awb door middel van publicatie bekend te worden gemaakt. Alleen het bevel van de officier van justitie wordt niet altijd vooraf bekendgemaakt, dit mede omdat het deels repressieve doel van de maatregel gefrustreerd zou kunnen worden door voortijdige bekendheid van de actie.

Door publicatie van de verordening en de gebiedsaanwijzing is het voor de burger in ieder geval voldoende duidelijk in welke gebieden en gedurende welke periode hij rekening moet houden met de mogelijkheid van een actie preventief fouilleren. Het aanwijzingsbesluit dient ingevolge artikel 151b lid 4 Gem.w. immers een nauwkeurige omschrijving van het gebied en een specifieke aanduiding van de geldigheidsduur van het besluit te bevatten. Het ontbreken van specifieke informatie omtrent de dagen en tijden waarop specifieke acties plaatsvinden, doet mijns inziens geen afbreuk aan de kenbaarheid en de voorzienbaarheid van de acties.

Legitiem belang en pressing social need
Vervolgens dient ook een actie preventief fouilleren ingevolge artikel 8 lid 2 EVRM noodzakelijk te zijn in het belang van een van de in dit artikel genoemde doelcriteria en tegemoet te komen aan een zwaarwegend maatschappelijk belang. De verlening van de bevoegdheid om een gebied aan te wijzen als veiligheidsrisicogebied, het aanwijzingsbesluit en het bevel van de officier van justitie om over te gaan tot een actie

preventief fouilleren dienen alle noodzakelijk te zijn om de verstoring van de openbare orde door de aanwezigheid van wapens of de ernstige vrees daarvoor tegen te gaan. Door deze doelbinding komt de beperking tegemoet aan verschillende van de in artikel 8 lid 2 opgesomde legitieme belangen, waaronder openbare veiligheid, voorkomen van wanordelijkheden, bescherming van de openbare orde en de bescherming van rechten en vrijheden van anderen.

Bij iedere beslissing in de keten van besluitvorming die voorafgaat aan een actie preventief fouilleren dient voorts aannemelijk te worden gemaakt dat er in de gemeente of in het aan te wijzen gebied sprake is van een dermate onveilige situatie als gevolg van de aanwezigheid van wapens dat de betreffende beslissing noodzakelijk is om effectief op te kunnen treden tegen deze onveilige situatie. Uit het bestaan van een dermate onveilige situatie kan mijns inziens een voldoende zwaarwegend maatschappelijk belang worden afgeleid om te voldoen aan het door het EHRM gestelde vereiste van een 'pressing social need'. Of dit in een concrete situatie inderdaad het geval is, zal wederom in de eerste instantie door het bestuur en vervolgens door de rechter moeten worden beoordeeld aan de hand van de motivering van het besluit en de gegevens over de concrete feiten en omstandigheden in het betreffende gebied.

Proportionaliteit

Tot slot dient de vraag te worden gesteld of een aanwijzing als veiligheidsrisicogebied, een bevel tot een actie preventief fouilleren en de concrete actie preventief fouilleren wel in een evenredige verhouding staan tot het met het preventief fouilleren gediende belang. Een onderzoek aan de kleding, een onderzoek van bagage en verpakkingen die iemand bij zich draagt en een onderzoek van het vervoermiddel waarin iemand zich vervoert grijpen behoorlijk diep in in het privé-leven van de burger. In het kader van een beoordeling van de proportionaliteit van een actie waarbij tot dergelijke onderzoeken kan worden overgegaan, zullen dan ook strenge eisen worden gesteld aan de proportionaliteit van de maatregel.[119]

Daarbij dient in de eerste plaats te worden gekeken naar de effectiviteit van preventief fouilleren. Er zijn inmiddels verschillende onderzoeken verricht naar de effectiviteit van preventief fouilleren.[120] Uit deze onderzoeken blijkt dat het moeilijk is om de effecten van preventief fouilleren te meten. Hier worden verschillende oorzaken voor aangevoerd. In de eerste plaats is de meting van de effecten afhankelijk van de concrete doelen die een gemeente gesteld heeft. Indien preventief fouilleren zowel een preventief als een repressief doel dient, zijn de effecten moeilijk te meten doordat de behaalde

119. EHRM 25 februari 1997, Reports of judgments and Decisions 1997-I, p. 348, § 95 (Z tegen Finland), EHRM 25 februari 1993, Series A, 256-A, § 55-58 (Funke). Zie hieromtrent eveneens P.H.Blok, Preventief fouilleren en de ontwijkingsmanouvre van de wetgever, AA 52 (2003) 5, p. 376.

120. COT, Preventief fouilleren in Amsterdam*: Opbrengsten en Wapenincidenten*, Den Haag, mei 2004; Lokale gezagsdriehoek Rotterdam, Wapenstilstand, Evaluatie preventief fouilleren *20 september 2002-30 juni 2003*, beschikbaar op www.rotterdam.nl; Ministerie van Justitie, Tussen-evaluatie preventief fouilleren, Den Haag, december 2003, beschikbaar op www.justitie.nl.

resultaten elkaar wederzijds negatief beïnvloeden.[121] Daarnaast maakt preventief fouilleren doorgaans onderdeel uit van een breder pakket aan veiligheidsmaatregelen waardoor de effecten van het preventief fouilleren niet los van de andere maatregelen kunnen worden gemeten. Wel blijkt uit verschillende rapporten dat het aantal geregistreerde geweldsincidenten waar wapens bij betrokken zijn in veiligheidsrisicogebieden significant gedaald is en het gevoel van veiligheid van de burgers in veiligheidsrisicogebieden licht is gestegen.[122] Gemeentebesturen zijn van mening dat dit in ieder geval ten dele is toe te schrijven aan preventief fouilleren.

In de tweede plaats dient in het kader van de proportionaliteitstoets te worden bezien of niet kon worden volstaan met minder ingrijpende middelen om de gestelde doelen te bereiken. Deze vraag kan op verschillende niveaus worden beantwoord; het gebruik van het instrument preventief fouilleren in het algemeen, de aanwijzing van het veiligheidsrisicogebied en de concrete actie preventief fouilleren. Voor het gebruik van het instrument preventief fouilleren in het algemeen zie ik geen alternatieven waarmee een zelfde resultaat kan worden bereikt. Op het niveau van het aanwijzingsbesluit kunnen er op een tweetal punten vraagtekens worden geplaatst bij de subsidiariteit van het besluit.

Allereerst blijken een aantal gemeenten in de praktijk te kiezen voor een relatief lange aanwijzingsperiode van zes maanden tot een jaar.[123] De wetgever heeft de maximale duur van het aanwijzingsbesluit blijkens artikel 151b lid 3 Gem.w. weliswaar niet willen vastleggen, maar zij heeft wel aangegeven dat de duur niet onbeperkt mag zijn en niet langer mag zijn dan strikt noodzakelijk is ten behoeve van de bestrijding van de (ernstige vrees voor) verstoring van de openbare orde als gevolg van de aanwezigheid van wapens. Bij een dergelijke lange aanwijzingsperiode kan het vermoeden rijzen dat deze duur langer is dan strikt noodzakelijk. Dit zelfde geldt voor de omvang van het aangewezen gebied.[124] Een aantal gemeenten heeft slechts één straat aangewezen als veiligheidsrisicogebied terwijl andere gemeenten hele wijken of zelfs de gehele binnenstad hebben aangewezen.[125] Ook hier kan de relatief grote omvang van het gebied het vermoeden doen rijzen dat volstaan had kunnen worden met een minder ingrijpend middel. Of inderdaad volstaan had kunnen worden met een kortere periode of een kleiner gebied zal in de afzonderlijke gevallen door de rechter moeten worden vastgesteld aan de hand van de motivering van het besluit en de gegevens over de concrete feiten en omstandigheden in het betreffende gebied.

Ten slotte kan op het niveau van de concrete actie preventief fouilleren worden bezien of niet met een minder ingrijpende uitvoering had kunnen worden volstaan.

---

121. Een preventief doel wordt gediend door bekendheid van acties waardoor mensen hun wapens thuislaten, dit heeft echter een negatief gevolg voor het beoogde repressieve effect doordat hierdoor minder wapens zullen worden aangetroffen bij controles. Andersom zal het repressieve effect bij onverwachte acties groter zijn, dit doet tegelijkertijd echter afbreuk aan het beoogde preventieve effect.
122. COT, Preventief fouilleren in Amsterdam*:* Opbrengsten en Wapenincidenten, Den Haag, mei 2004; Lokale gezagsdriehoek Rotterdam, Wapenstilstand, Evaluatie preventief fouilleren 20 september 2002-30 juni 2003, beschikbaar op www.rotterdam.nl.
123. COT, Preventief fouilleren in Amsterdam: Opbrengsten en Wapenincidenten, Den Haag, mei 2004, p. 3. en Ministerie van Justitie, Tussen-evaluatie preventief fouilleren, Den Haag, december 2003, p. 44. Beschikbaar op www.justitie.nl.
124. P.H.Blok, Preventief fouilleren en de ontwijkingsmanoeuvre van de wetgever, AA 52 (2003) 5, p. 376.
125. Ministerie van Justitie, Tussen-evaluatie preventief fouilleren, Den Haag, december 2003, p. 43. Beschikbaar op www.justitie.nl.

Daarbij kan in de eerste plaats gekeken worden naar het middel dat wordt gebruikt om burgers aan hun kleding te onderzoeken. Een politieagent kan dit handmatig doen maar kan ook gebruikmaken van een handscan. Dit laatste levert een minder grote aantasting van de persoonlijke integriteit van de onderzochte burger op dan de betasting die een handmatig onderzoek met zich meebrengt. Tegen het gebruik van handscans kan echter worden ingebracht dat zij duur zijn in aanschaf en op ieder metalen voorwerp reageren waardoor in veel gevallen de burger alsnog handmatig zal moeten worden onderzocht. Mij lijkt derhalve niet dat op basis van het subsidiariteitscriterium kan worden gezegd dat de voorkeur moet worden gegeven aan handscans.

Naast het gebruikte middel kan ook de gekozen methode aan een subsidiariteitstoets worden onderworpen. De methoden die de politie gebruikt om personen of voertuigen te selecteren voor een onderzoek variëren in ingrijpendheid. Zo levert een gebiedssurveillance of een dynamische voertuigcontrole waarbij personen en voertuigen worden geselecteerd op basis van bepaalde (al dan niet vooraf vastgestelde) kenmerken[126] voor minder mensen een aantasting van de privacy op dan een gebiedsafsluiting, een statische voertuigcontrole of een lokaliteiten- of horecacontrole. In de praktijk laat de officier van justitie zich bij de keuze voor een methode echter (onder andere) leiden door het door de wetgever gestelde vereiste van a-selectiviteit van een controle.[127] Een methode waarbij van een politieagent een selectie op basis van bepaalde kenmerken wordt verwacht, brengt het risico van een discriminatoir onderscheid met zich mee. Op basis van het vereiste van a-selectiviteit kan een gebiedsafsluiting of een statische voertuigcontrole derhalve de voorkeur verdienen.

Een lokaliteiten- of horecacontrole vereist evenmin selectie van personen op basis van mogelijk discriminatoire gronden. Bij deze vormen van controle worden de aanwezige personen in een wachtruimte geplaatst en vervolgens gecontroleerd. Deze vormen van controle vormen een meer ingrijpende inmenging met het privé-leven van de burgers dan controles op straat. Een beroep op het criterium van a-selectiviteit kan naar mijn mening dan ook niet volstaan om deze vormen van controles te rechtvaardigen.

De rechtmatigheid van dergelijke controles is overigens überhaupt aan twijfel onderhevig daar preventief fouilleren zich blijkens de toelichting tot openbare ruimten dient te beperken. Of horecagelegenheden en andere gebouwen aan deze voorwaarde voldoen is twijfelachtig. Indien het begrip publieke ruimte moet worden uitgelegd als een ruimte die in principe voor een ieder vrij toegankelijk is,[128] kan voor bepaalde plaatsen en gebouwen betwijfeld worden of zij aan deze voorwaarde voldoen. Deze twijfel wordt nog sterker indien, zoals bij veel horecagelegenheden het geval is, het betreden van de ruimte afhankelijk is gesteld van een deurbeleid of het betalen van entree.

In de laatste plaats dient in het kader van de proportionaliteitstoets te worden gekeken naar de bescherming die de regeling burgers biedt bij een beperking van hun recht

126. Hierbij kan bijvoorbeeld worden gedacht aan bepaalde uiterlijke kenmerken, etnische afkomst, geslacht, leeftijd of verdachte gedragingen.
127. Kamerstukken II 2003-2004, 29 218, nr. 6, p. 5.
128. Zoals het ministerie van Justitie lijkt te impliceren in de Tussen-evaluatie preventief fouilleren. Ministerie van Justitie, Tussen-evaluatie preventief fouilleren, Den Haag, december 2003, p. 47. Beschikbaar op www.justitie.nl.

op privacy. De regeling dient burgers een effectief rechtsmiddel te bieden tegen een dergelijke beperking.

Volgens de memorie van toelichting staat er tegen het aanwijzingsbesluit van de burgemeester een beroep open bij de bestuursrechter. Zoals reeds in paragraaf 2.2 is aangegeven, heeft de rechter echter geoordeeld dat een burger geen rechtstreeks belang heeft bij een dergelijk besluit. Dit betekent dat de burger het aanwijzingsbesluit niet kan aanvechten bij de bestuursrechter. Wel kan de burger zich tot de burgerlijke rechter wenden. De burger kan immers stellen dat de aanwijzing van een veiligheidsrisicogebied jegens hem een onrechtmatige daad is. Voorts kan de burger de rechtsgeldigheid van het aanwijzingsbesluit aanvechten in een tegen hem ingestelde strafrechtelijke procedure. Of deze optie voldoet in het licht van de eisen die het EHRM stelt, vraag ik mij echter af. Het kan immers niet de bedoeling zijn dat de burger, teneinde een mogelijkheid van rechtsbescherming tegen een aanwijzingsbesluit te verkrijgen, eerst een strafrechtelijke procedure uitlokt door zich in een aanwijzingsgebied te laten betrappen met een verboden wapen op zak.

Tot slot heeft de burger op grond van hoofdstuk 9 Awb het recht om naar aanleiding van het feitelijk handelen van een agent in het kader van de uitoefening van de bevoegdheden van artikel 50 lid 3, 51 lid 3 en 52 lid 3 WWM een klacht in te dienen bij de korpsbeheerder. Deze procedure voldoet niet aan de eisen die het EHRM stelt aan een effectief rechtsmiddel; de korpsbeheerder heeft niet de bevoegdheid een voor de partijen bindende uitspraak te doen, maar de burger kan zich vervolgens tegen dit vermeend onrechtmatig feitelijk handelen tot de burgerlijke rechter wenden.

Het totaal van de waarborgen die het voorstel biedt is naar mijn mening vrij minimaal maar waarschijnlijk voldoende om een burger te beschermen tegen een beperking van zijn recht op privacy als gevolg van de regeling met betrekking tot preventief fouilleren. Dit neemt echter niet weg dat de problemen met de gang naar de bestuursrechter de aandacht van de wetgever verdienen.

4.2.3 Uitgebreide identificatieplicht

Grondslag in een wet in formele zin en bij wet voorzien

De bevoegdheid van toezichthoudend ambtenaren en (buitengewoon) opsporingsambtenaren om van een ieder inzage te vorderen in een geldig identiteitsbewijs wordt neergelegd in artikel 8a Pol.w. en artikel 5:16a Awb. De met deze bevoegdheid corresponderende medewerkingsplicht voor de burger wordt neergelegd in het nieuwe artikel 2 WID en ook het sluitstuk van de uitgebreide identificatieplicht, de strafbaarstelling van het niet voldoen aan een verzoek om inzage, vindt haar grondslag in een wet in formele zin, artikel 447e Sr. Blijkens de toelichting op de wet die deze grondslagen introduceert, de Wet Uitgebreide Identificatieplicht, is deze wet onder andere totstandgekomen met het doel een mogelijke beperking die de uitgebreide identificatieplicht zou vormen op het recht op eerbiediging van de persoonlijke levenssfeer te voorzien van een wettelijke grondslag.[129]

129. Kamerstukken II 2003-2004, 29 218, nr. 3, p. 3.

Hiermee is wellicht voldaan aan de door artikel 10 lid 1 Grw gestelde eis van een grondslag in een wet in formele zin doch niet noodzakelijk aan het door artikel 8 lid 2 EVRM gestelde vereiste dat een beperking bij wet voorzien moet zijn. Met de hiervoor genoemde door de Wet Uitgebreide Identificatieplicht gecreëerde grondslagen zal voldaan zijn aan de in het kader van dit vereiste gestelde voorwaarde van kenbaarheid. Ten aanzien van de voorwaarde van voorzienbaarheid vraag ik mij echter af of de bepalingen wel voldoende nauwkeurig zijn geformuleerd.

De voorwaarde van voorzienbaarheid eist dat de burger de gevolgen die de regeling voor hem heeft redelijkerwijs kan voorzien. Ingevolge artikel 2 WID dient een ieder op vordering van een opsporingsambtenaar een identiteitsbewijs te tonen. Uit artikel 8a Pol.w. en artikel 5:16a Awb blijkt dat een toezichthoudend ambtenaar of een (buitengewoon) opsporingsambtenaar een dergelijke vordering slechts mag doen voor zover dit redelijkerwijs noodzakelijk is voor de uitoefening van zijn taak. Wat redelijkerwijs noodzakelijk is voor de uitoefening van een taak, zal per taak verschillen en dit criterium op zich biedt de burger derhalve onvoldoende duidelijkheid over de vraag of hij verplicht is gehoor te geven aan een vordering tot inzage in een identiteitsbewijs. De wetgever mag de uitvoerende instanties ingevolge de jurisprudentie van het EHRM wel een zekere mate van beoordelingsvrijheid laten maar dient met een redelijke mate van duidelijkheid aan te geven wat de reikwijdte van deze beoordelingsvrijheid is.[130] Aan dit vereiste is met artikel 8a Pol.w. en artikel 5:16a Awb niet voldaan.

Legitiem belang en pressing social need

Vervolgens moet worden bezien of een uitgebreide identificatieplicht wel noodzakelijk is in het belang van de in artikel 8 lid 2 EVRM genoemde legitieme belangen en tegemoetkomt aan een zwaarwegende maatschappelijke behoefte. Volgens de toelichting is een uitbreiding van de bestaande beperkte identificatieplichten noodzakelijk voor een doeltreffende bestrijding van criminaliteit en rechtshandhaving.[131] Dit zijn belangen die onder andere kunnen vallen onder de door artikel 8 lid 2 EVRM genoemde belangen van openbare veiligheid en bescherming van de openbare orde.

Voorts is het de vraag of er ook sprake is van een dringend maatschappelijk belang dat deze maatregel noodzakelijk maakt in het licht van deze doelstelling. Volgens de toelichting is dit dringend maatschappelijk belang gelegen in de toegenomen en nog steeds toenemende complexiteit van de samenleving.[132] Deze toegenomen complexiteit heeft er volgens de regering toe geleid dat er van overheidszijde een grotere behoefte bestaat aan de correcte vaststelling van de identiteit van de burgers. Voor de goede uitoefening van de politietaak en toezicht op de naleving van bijzondere wetten moeten extra bevoegdheden in het leven geroepen worden die deze correcte vaststelling van de identiteit mogelijk maken.[133] In de nota naar aanleiding van verslag heeft de regering dit iets genuanceerd door te stellen dat een redelijke taakuitoefening van de politietaak een uitbreiding van de identificatieplicht niet noodzakelijk maakt, maar kan bijdragen aan een verbetering van de uitvoering van de politietaak.[134]

---

130. EHRM 2 augustus 1984, Series A, 84, § 66 (Malone tegen Verenigd Koninkrijk).
131. Kamerstukken II 2003-2004, 29 218, nr. 3, p. 1.
132. Kamerstukken II 2003-2004, 29 218, nr. 3, p. 3.
133. Kamerstukken II 2003-2004, 29 218, nr. 3, p. 4
134. Kamerstukken II 2003-2004, 29 218, nr. 10, p. 4.

De motivering van het bestaan van een dringende maatschappelijke behoefte tot het invoeren van een uitgebreide identificatieplicht is naar mijn mening te mager om te kunnen spreken van redenen die toereikend zijn om de aantasting van het recht op privacy van de burgers die een uitgebreide identificatieplicht meebrengt te kunnen dragen.

Allereerst is het enkele beroep op de toegenomen en nog steeds toenemende complexiteit van de samenleving niet voldoende om te kunnen spreken van een dringende maatschappelijke behoefte.[135] Een dergelijk beroep moet worden onderbouwd met gegevens waaruit blijkt dat het ontbreken van een toereikende bevoegdheid om burgers om inzage in een identiteitsbewijs te vragen heeft geleid tot concrete tekortkomingen in de handhaving.[136] Bijvoorbeeld doordat verdachten hierdoor niet konden worden vervolgd, overtredingen aan niet bestaande of onjuiste personen zijn geverbaliseerd of bepaalde wetten niet konden worden gehandhaafd. De regering laat tevens na gemotiveerd aan te geven waarom niet kon worden volstaan met minder ingrijpende middelen, zoals het intensiever benutten van bestaande identificatieplichten. Het kabinet-Kok II concludeerde amper twee jaar geleden nog dat een intensievere benutting van de bestaande identificatieplichten het handhavingsniveau reeds voldoende kan verhogen.[137] Tot slot onbreekt iedere vorm van onderzoek waaruit blijkt dat de invoering van een uitgebreide identificatieplicht daadwerkelijk zal bijdragen aan de bestrijding van de vermeende tekortkomingen in de handhaving.[138]

Zonder overtuigende motivering op deze punten kan er mijns inziens niet worden gesproken van een behoefte aan een uitgebreide identificatieplicht die voldoet aan het in het kader van de proportionaliteitstoets van artikel 8 lid 2 EVRM gestelde vereiste van een 'pressing social need'.

Proportionaliteit

Tot slot dient de vraag te worden gesteld of een uitgebreide identificatieplicht noodzakelijk is in het belang van doeltreffende bestrijding van criminaliteit en bevordering van de rechtshandhaving. Daarbij dient in de eerste plaats te worden nagegaan of dit doel niet met een minder ingrijpend middel kan worden gerealiseerd. Op dit punt kunnen verschillende kanttekeningen worden geplaatst.

In de eerste plaats heeft de regering, zoals hiervoor reeds is aangegeven, nagelaten aan te tonen waarom niet kan worden volstaan met een intensievere benutting van de bestaande bevoegdheden van toezichthoudend ambtenaren en (buitengewoon) opsporingsambtenaren om inzage in een identiteitsbewijs te vorderen.

Op dit moment hebben toezichthoudend ambtenaren op grond van de bevoegdheid om inlichtingen te vorderen van artikel 5:17 Awb, zoals in paragraaf 2.3.2 beschreven is, reeds de bevoegdheid inzage te vorderen in een identiteitsbewijs. Op basis van arti-

---

135. CBP, Advies wetsvoorstel uitbreiding identificatieplicht, beschikbaar op www.CBPweb.nl.
136. NOVA, Advies inzake het wetsvoorstel uitbreiding identificatieplicht van 23 januari 2003, beschikbaar op www.advocatenorde.nl.
137. Kamerstukken II 2001-2002, 28 069, nr. 1, p. 6; CBP, Advies wetsvoorstel uitbreiding identificatieplicht, beschikbaar op www.CBPweb.nl; M. Duker, M.E. Meijer en B.J. Schmitz, NJCM-commentaar op de voorgestelde uitbreiding van de wet identificatieplicht, NJCM-Bulletin, jrg. 29 (2004), p. 537.
138. NOVA, Advies inzake het wetsvoorstel uitbreiding identificatieplicht van 23 januari 2003, beschikbaar op www.advocatenorde.nl.

kel 5:13 Awb wordt deze bevoegdheid beperkt door de voorwaarde dat de bevoegdheid slechts mag worden gebruikt voor zover dit redelijkerwijs nodig is voor de vervulling van zijn taak. Toezichthoudend ambtenaren hebben derhalve geen algemene bevoegdheid om inzage in een identiteitsbewijs te vorderen.

Op basis van artikel 5:16a Awb krijgen toezichthoudend ambtenaren een algemene bevoegdheid om inzage in een identiteitsbewijs te vorderen. Ook deze algemene bevoegdheid is blijkens artikel 5:16a Awb echter gekoppeld aan de taak van de betreffende ambtenaar en mag, evenals de bevoegdheid tot het vorderen van inlichtingen, slechts worden uitgeoefend indien dit redelijkerwijs noodzakelijk is ten behoeve van de uitoefening van deze taak. Op dit punt biedt de voorgestelde uitgebreide identificatieplicht derhalve geen meerwaarde.

Politieagenten en buitengewoon opsporingsambtenaren hebben, zoals eveneens in paragraaf 2.3.2 uiteengezet is, slechts de bevoegdheid om een burger om zijn identiteitsgegevens en zijn sofi-nummer te vragen indien deze burger verdacht wordt van een strafbaar feit (artikel 52 en 55a Sv). In de huidige situatie hebben deze ambtenaren derhalve geen algemene bevoegdheid om inzage in een identiteitsbewijs te vorderen. artikel 8a Pol.w. introduceert voor deze ambtenaren een algemene bevoegdheid om inzage in een identiteitsbewijs te vorderen. De meerwaarde van deze bevoegdheid is gelegen in de mogelijkheid die hierdoor ontstaat om van burgers die niet verdacht worden van een strafbaar feit inzage in een identiteitsbewijs te vorderen.

Het zijn van verdachte als voorwaarde voor de toepassing van strafprocesrechtelijke dwangmiddelen door de politie vormt een belangrijke waarborg tegen willekeurig politieoptreden.[139] Ik vraag mij daarom af of het loslaten van deze voorwaarde ten aanzien van de identificatieplicht wel zo wenselijk is. Het is gemakkelijk voor te stellen dat hierdoor in veel gevallen te snel naar de toepassing van deze bevoegdheid gegrepen wordt.[140] Artikel 8a Pol.w. stelt weliswaar de voorwaarde dat de uitoefening van de bevoegdheid tot het vorderen van inzage in een identiteitsbewijs redelijkerwijs noodzakelijk moet zijn ten behoeve van de uitvoering van de taak van de betreffende (buitengewoon) opsporingsambtenaar maar in deze waarborg schuilen verschillende belangrijke problemen.

Allereerst is de formulering van deze beperking dermate vaag dat, zoals hiervoor uiteen is gezet, niet duidelijk is in welke gevallen de bevoegdheid gebruikt mag worden. Uit de jurisprudentie over de bestaande identificatieplichten zou weliswaar kunnen worden afgeleid dat voor een vordering tot inzage in ieder geval bijzondere redenen nodig zijn,[141] maar gezien de formulering van artikel 8a Pol.w. zal de rechter deze bijzondere omstandigheden echter slechts marginaal mogen toetsen.

Op basis van de nieuwe wet bestaat er geen algemene plicht om de uitgevoerde identiteitscontroles te registreren. Tenzij er een process-verbaal wordt opgemaakt voor het niet voldoen aan een vordering tot inzage is er derhalve geen bewijs van de controle en de aanleiding daarvoor. Dit maakt het in de eerste plaats voor de burger erg moeilijk om de rechtmatigheid van de controle aan te vechten en maakt het daarnaast voor de rechter bijzonder lastig om te controleren of de vordering daadwerkelijk redelijkerwijs

---

139. P.H. Blok, Preventief fouilleren en de ontwijkingsmanoeuvre van de wetgever, AA 52 (2003) 5, p. 376.
140. M. Duker, M.E. Meijer en B.J. Schmitz, NJCM-commentaar op de voorgestelde uitbreiding van de wet identificatieplicht, NJCM-Bulletin, jrg. 29 (2004), p. 541.
141. Rb. Den Haag zp Assen 10 mei 2001, RN 2001, 6.

noodzakelijk was ten behoeve van de uitoefening van de taak van de betreffende ambtenaar. Ook brengt het ontbreken van een algemene registratieplicht het risico mee dat deze ruime bevoegdheid discriminatoir wordt toegepast, hetgeen wederom, bij gebrek aan bewijs van de controles en de aanleiding daarvoor, niet door de rechter gecontroleerd kan worden.[142]

Een algemene plicht om de uitgevoerde controles te registreren is echter evenmin een oplossing. Een dergelijke registratie, die slechts wordt uitgesloten door de toezegging van de regering, versterkt het effect van de inbreuk op de privacy doordat in dat geval van iedere gecontroleerde burger wordt vastgelegd wat zij waar en wanneer deden dat aanleiding gaf voor een controle. Daarnaast betekent een dergelijke administratie een onwenselijke toename van de administratieve lasten voor de betrokken ambtenaren,[143] dit zou ertoe kunnen leiden dat een registratieplicht op grote schaal ontdoken wordt.[144]

In het kader van de proportionaliteitstoets moet tevens worden gekeken naar de effectiviteit van een uitgebreide identificatieplicht bij een doeltreffende bestrijding van criminaliteit en bevordering van de rechtshandhaving. Hoewel ik mij kan voorstellen dat een uitgebreide identificatieplicht, waarbij mensen die niet verdacht worden van een strafbaar feit maar zich wel verdacht gedragen kunnen worden verplicht zich te identificeren, bijdraagt aan een betere handhaving en criminaliteitsbestrijding, wordt dit punt door de regering niet gestaafd met onderzoek dat deze verwachting rechtvaardigt. Ook geeft de regering niet aan of deze verwachte resultaten zullen opwegen tegen de extra belasting die het aantal strafzaken in verband met de overtreding van de identificatieplicht naar alle waarschijnlijkheid zal meebrengen.[145]

Tot slot dient in het kader van de proportionaliteitstoets te worden gekeken naar de bescherming die de regeling burgers biedt indien hun recht op privacy beperkt wordt als gevolg van de uitgebreide identificatieplicht. De regeling dient burgers een effectief rechtsmiddel te bieden tegen een dergelijke beperking. Indien een burger een vordering tot inzage wil aanvechten, kan hij zich in de eerste plaats beklagen bij de korpsbeheerder op grond van de klachtregeling van hoofdstuk 9 van de Awb. Deze niet-rechterlijke procedure voldoet weliswaar niet aan de eisen van een effectief rechtsmiddel omdat de korpsbeheerder geen bindende uitspraak kan doen maar dit hoeft niet problematisch te zijn. Een burger kan tegen een vermeende onrechtmatige vordering immers een beroep instellen bij de burgerlijke rechter. Zoals gezegd biedt de gang naar de rechter echter niet bijzonder veel bescherming omdat de burger bij het ontbreken van een proces-verbaal geconfronteerd wordt met een bewijsprobleem. Wanneer er wel een process-verbaal is opgemaakt, heeft de burger dat bewijs wel maar kan de rechter slechts terughoudend toetsen. Tot slot kan de burger, indien er tegen hem een strafprocedure aanhangig wordt gemaakt, de rechtmatigheid van de controle aanvechten in het kader van deze procedure.

---

142. CBP, Advies wetsvoorstel uitbreiding identificatieplicht, beschikbaar op www.CBPweb.nl; M. Duker, M.E. Meijer en B.J. Schmitz, NJCM-commentaar op de voorgestelde uitbreiding van de wet identificatieplicht, NJCM-Bulletin, jrg. 29 (2004), p. 541.
143. Kamerstukken II 2003-2004, 29 218, nr. 3, p. 13.
144. CBP, Advies wetsvoorstel uitbreiding identificatieplicht, beschikbaar op www.CBPweb.nl.
145. NVvR, Advies inzake het conceptwetsvoorstel inzake uitbreiding van de identificatieplicht van 20 februari 2003, beschikbaar op www.verenigingvoorrechtspraak.nl.

5 Conclusie

Het streven naar vergroting van de veiligheid van het huidige kabinet is in onze huidige maatschappij (helaas) een noodzakelijk streven. De huidige regering is met de maatregelen die zij de laatste jaren getroffen heeft op de goede weg om dit streven te realiseren. Het is echter belangrijk dat de overheid in het streven naar het vergroten van de veiligheid niet te ver doorschiet. Dit is voornamelijk belangrijk indien de getroffen maatregelen ten koste gaan van de grondrechten van de burger, zoals het recht op privacy. In dit preadvies heb ik mij dan ook de vraag gesteld of de (voorgestelde) regelgeving ten aanzien van drie maatregelen ter bestrijding van de onveiligheid (cameratoezicht op openbare plaatsen, preventief fouilleren en een uitgebreide identificatieplicht) voldoende waarborgen biedt om haar concrete toepassing te laten voldoen aan de eisen die het recht op privacy stelt.

Nadat ik in hoofdstuk 3 heb vastgesteld dat de (voorgestelde) regelgeving met betrekking tot deze maatregelen een beperking vormt van het recht op privacy van de burgers zoals beschermd door artikel 10 lid 1 Grw en artikel 8 EVRM, ben ik vervolgens in hoofdstuk 4 nagegaan of deze beperkingen gerechtvaardigd kunnen worden onder de beperkingsclausules van deze artikelen. Naar mijn mening dient te worden geconcludeerd dat deze regelingen op punten onvoldoende waarborgen bieden om te voldoen aan de door artikel 8 lid 2 EVRM gestelde eisen aan een rechtmatige beperking van artikel 8 EVRM.

De beperking op het recht op privacy die het voorstel cameratoezicht op openbare plaatsen meebrengt, kan op het punt van het opslaan en bewaren van de gemaakte beelden naar mijn mening niet gerechtvaardigd worden onder artikel 8 lid 2 EVRM omdat het stelselmatig opslaan en bewaren van de gemaakte beelden niet noodzakelijk is in het belang van de handhaving van de openbare orde.

De regeling met betrekking tot preventief fouilleren van artikel 151 b Gem.w. en artikel 50 lid 3, 51 lid 3 en 52 lid 3 WWM is eveneens problematisch in het licht van de eisen van artikel 8 lid 2 EVRM omdat het op basis van deze regeling mogelijk is dat de bevoegdheden worden gebruikt op een wijze die niet in een evenredige verhouding staat tot het belang van het tegengaan van wapengeweld. In dit kader kan in de eerste plaats de door artikel 151b lid 3 Gem.w. geboden mogelijkheid dat een gebied voor lange tijd wordt aangewezen als veiligheidsrisicogebied een probleem opleveren. Ook de mogelijkheid dat een groot gebied wordt aangewezen kan leiden tot problemen op het terrein van de evenredigheid. Het voornaamste probleem is echter gelegen in de methoden die de politie kan gebruiken om personen te selecteren voor een onderzoek. In het belang van een niet-discriminatoir gebruik van de bevoegdheden kan het noodzakelijk zijn dat er meer mensen onderzocht worden dan nodig is in het kader van het belang van het tegengaan van de aanwezigheid van wapens. Dit belang staat echter niet

in een evenredige verhouding tot het bijzonder ingrijpende karakter van de methode wanneer gebruik wordt gemaakt van een lokaliteiten- of horecacontrole.

Tot slot vormt de uitgebreide identificatieplicht een ontoelaatbare beperking van het recht op privacy omdat de regeling op een aantal punten niet voldoet aan de door artikel 8 lid 2 EVRM gestelde eisen aan een rechtmatige beperking. In de eerste plaats is voor de burger op basis van het vage criterium dat een beperking redelijkerwijs noodzakelijk moet zijn voor de uitoefening van de taak van de betreffende ambtenaar (artikel 8a Pol.w., artikel 5:16a Awb en artikel 2 WID) niet voldoende duidelijk wanneer een ambtenaar bevoegd is tot het vorderen van inzage in een identiteitsbewijs. In de tweede plaats kunnen er vraagtekens worden geplaatst bij de noodzaak van een uitbreiding van de identificatieplicht. Ten eerste omdat de gebrekkig onderbouwde reden voor de uitbreiding, de toegenomen complexiteit van de samenleving, geen voldoende zwaarwegend maatschappelijk belang vormt. Ten tweede staat de plicht niet in een evenredige verhouding tot het doel van verbetering van de criminaliteitsbestrijding en de rechtshandhaving omdat onvoldoende aannemelijk is gemaakt dat niet kan worden volstaan met minder ingrijpende middelen, zoals het intensiever gebruik van de huidige beperkte identificatieplichten. Tot slot is de effectiviteit van de voorgestelde identificatieplicht twijfelachtig. Er wordt niet onderbouwd in welk opzicht en in welke mate de identificatieplicht zal bijdragen aan verbetering van de criminaliteitsbestrijding en rechtshandhaving en er wordt niet aangegeven of deze effecten wel opwegen tegen de extra lasten die handhaving van de identificatieplicht meebrengt.

Deze conclusies brengen mij tot de volgende stellingen.

Stellingen

1. Het stelselmatig opslaan en bewaren van met behulp van cameratoezicht in de openbare ruimte gemaakte beelden vormt een onrechtmatige beperking van het recht op privacy omdat deze beperking niet noodzakelijk is in het belang van het doel van dit cameratoezicht, handhaving van de openbare orde.

2. Een uitgebreide identificatieplicht vormt een onrechtmatige beperking van het recht op privacy omdat het beoogde doel, verbetering van de rechtshandhaving en bestrijding van de criminaliteit, op een minder ingrijpende wijze gerealiseerd kan worden door intensiever gebruik te maken van de huidige beperkte identificatieplichten.

3. Preventief fouilleren kan een ontoelaatbare beperking van het recht op privacy meebrengen omdat de regeling toelaat dat:
   a. gebieden voor onevenredig lange periodes worden aangewezen als veiligheidsrisicogebied.
   b. onevenredig grote gebieden worden aangewezen als veiligheidsrisicogebied.
   c. gebruik wordt gemaakt van onevenredig ingrijpende methoden als lokaliteiten- en horecacontroles.

Grenzen aan gegevensverstrekking

Mr. M.P.J.M. van Grinsven[*]

* Mr. M.P.J.M. van Grinsven is jurist bij de Raad van State. Dit stuk is op persoonlijke titel geschreven.

1 Inleiding

Het spanningsveld tussen privacy en veiligheid is de laatste jaren behoorlijk toegenomen. Stond de bescherming van de persoonlijke levenssfeer lange tijd hoog op de nationale en internationale agenda, sinds enkele jaren is de nadruk in het publieke debat komen te liggen op andere belangen, zoals terrorismebestrijding en de aanpak van criminaliteit. De gebeurtenissen van 11 september 2001 hebben daar onmiskenbaar aan bijgedragen. Privacy heeft in dit debat een negatieve bijklank gekregen en wordt beschouwd als een hindernis bij het bereiken van doelstellingen op het gebied van het veiligheidsbeleid.[1] Met name de regels ter bescherming van persoonsgegevens staan daarbij ter discussie. De praktijk van de bestrijding van terrorisme en andere misdaad wil het liefst de beschikking over alle relevante gegevens, waaronder persoonsgegevens. De huidige privacyregels staan dit niet toe. De aanhoudende roep om meer bevoegdheden,[2] ook in politieke kringen, dreigt echter een evenwichtige afweging tussen beide belangen verloren te doen gaan.

Het is natuurlijk niet mogelijk om binnen het korte bestek van dit preadvies een volledig overzicht te geven van alle ontwikkelingen op het spanningsveld tussen enerzijds het belang van terrorisme- en criminaliteitsbestrijding en anderzijds het belang van de persoonsgegevensbescherming. Met name het onderwerp van de terrorismebestrijding is nog volop in beweging en onttrekt zich voor een deel aan de ogen van de buitenwereld. In dit preadvies zal daarom de bestrijding van de 'gewone' criminaliteit centraal staan. De kernvraag die daarbij aan de orde wordt gesteld, is in hoeverre (vrijwillige) verstrekking van persoonsgegevens aan de politie is toegestaan, welke regels hierop zien en welke recente ontwikkelingen op dit terrein spelen.

Na een overzicht van de achtergrond van de privacydiscussie, in het bijzonder het debat rond de bescherming van persoonsgegevens en de beginselen die op dit terrein van belang zijn (hoofdstuk 2), wordt in hoofdstuk 3 ingegaan op de vraag op welke wijze de verstrekking van persoonsgegevens aan instanties belast met toezicht en opsporing op dit moment is geregeld. In hoofdstuk 4 wordt vervolgens ingegaan op de plannen van de regering om op korte termijn een verregaande informatieplicht in het Wetboek van Strafvordering op te nemen. Hoewel dit niet direct een bestuursrechte-

1. Typerend is de recente karakterisering door de Groningse korpschef van privacy als 'de schuilplaats van het kwaad'.
2. Als voorlopig dieptepunt geldt mijns inziens de onlangs gedane suggestie van een politiecommissaris dat artsen bij de geboorte van baby's al erfelijk materiaal zouden kunnen afnemen om daarmee later het oplossingspercentage van misdrijven 'gigantisch' te doen stijgen.

lijke invalshoek is, ben ik toch van mening dat juist deze ontwikkeling een goede balans tussen privacy en veiligheid bedreigt.

2 Achtergronden van het debat

2.1 Inleiding

Voor een goed begrip van de huidige ontwikkelingen met betrekking tot het spanningsveld tussen persoonsgegevensbescherming en criminaliteitsbestrijding is kennis van de achtergronden daarvan onontbeerlijk. In dit hoofdstuk wordt daarom in het algemeen stilgestaan bij de ontstaansgeschiedenis van het recht op privacy, de betekenis van dat recht in de sfeer van de bescherming van persoonsgegevens en de problematische verhouding met het belang van de veiligheid.

2.2 Ontstaansgeschiedenis

Hoewel de wortels van het privacybegrip in een verder verleden liggen,[3] is het ontstaan van een in verdragsrecht, Grondwet en lagere regelgeving erkend recht op privacy toch vooral het gevolg geweest van enerzijds de toegenomen aandacht voor mensenrechten in het algemeen, als gevolg van de verschrikkingen van de Tweede Wereldoorlog, en anderzijds de opkomst van de informatiemaatschappij enkele decennia geleden.

De toegenomen aandacht voor de mensenrechten in de periode na de Tweede Wereldoorlog heeft ertoe geleid dat deze rechten een plaats hebben gekregen in talrijke verdragen en andere internationale instrumenten, alsmede in nationale grondwetten. Op het internationale vlak valt met name te denken aan de Universele Verklaring van de rechten van de mens, het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR) en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Steeds wordt daarin ook het recht van eenieder op privacy erkend, zij het dat de gebruikte formuleringen uiteenlopen.[4] Voor de Nederlandse situatie is vooral artikel 8 van het EVRM van belang, niet alleen gelet op de rechtstreekse werking van dat artikel, maar ook vanwege de mogelijkheid voor individuele burgers om een klacht in te dienen bij het Europees Hof voor de rechten van de mens (EHRM), waarvan de uitspraken juridisch bindend zijn voor de aangesloten

3. Te denken valt bijvoorbeeld aan de beroemd geworden omschrijving van privacy als 'the right to be let alone' door de Amerikaanse juristen Warren en Brandeis aan het einde van de negentiende eeuw. S.D. Warren en L.D. Brandeis, The right to privacy: the implicit made explicit, Harvard Law Review 1890, p. 193-220. Bron: P.H. Blok en A.H. Vedder, Privacy in ontwikkeling, in: J.E.J. Prins en J.M.A. Berkvens, Privacyregulering in theorie en praktijk, Deventer 2002 (derde druk), p. 13.
4. Zo heeft artikel 12 van de Universele Verklaring het over iemands persoonlijke aangelegenheden, terwijl artikel 8 van het EVRM en 17 van het IVBPR aanhaken bij het begrip privé-leven.

lidstaten. Daarnaast kent Nederland sinds 1983 een door artikel 10 van de Grondwet gewaarborgd recht op bescherming van de persoonlijke levenssfeer. Daarbij heeft men zich niet alleen laten inspireren door de hiervoor genoemde mensenrechtenverdragen, maar ook door (internationale) ontwikkelingen op het specifieke terrein van de bescherming van persoonsgegevens.

Eind jaren zestig, begin jaren zeventig werd duidelijk dat het dankzij de voortschrijdende ontwikkelingen op technologisch gebied steeds beter mogelijk was om op grote schaal gegevens te verzamelen, op te slaan en te verwerken. Op individuele personen betrekking hebbende gegevens waren hierop geen uitzondering. Vanuit het perspectief van de overheid opende dit de mogelijkheid van een efficiëntere en meer op individuele burgers toegesneden taakvervulling. Tegelijkertijd bestond echter het gevaar dat de overheid steeds meer macht over diezelfde burgers zou krijgen en daarmee hun gedrag meer en meer zou kunnen beïnvloeden. Critici, wellicht bevreesd voor een door schrijvers als Huxley (Brave New World) en Orwell (1984) beschreven toekomstbeeld van een samenleving die in al haar aspecten door de staat wordt gecontroleerd, wezen op de potentiële risico's verbonden aan de informatierevolutie. Het wantrouwen jegens de overheid was in deze periode niet toevallig erg groot.[5]

Als reactie hierop kwamen zowel op nationaal als internationaal niveau diverse instrumenten tot ontwikkeling met als doel het creëren van voorwaarden waaronder de verwerking van persoonsgegevens plaats diende te vinden. Landen als Zweden en Duitsland namen daarin het voortouw en brachten reeds in de jaren zeventig specifieke wetgeving met betrekking tot de bescherming van persoonsgegevens tot stand. In Nederland duurde de ontwikkeling van deze wetgeving beduidend langer. Pas in 1988, na een lang wetgevingstraject, kwam op dit terrein de Wet persoonsregistraties (WPR) tot stand. Dat die wet er kwam, was overigens in belangrijke mate het gevolg van internationale ontwikkelingen, alsmede van de sinds 1983 bestaande grondwettelijke opdracht tot het stellen van regels inzake de registratie van persoonsgegevens.[6]

Ook op internationaal vlak stond de kwestie van de persoonsgegevens hoog op de agenda. De noodzaak van een adequate bescherming van de privacy was daarvoor overigens niet de enige reden. Zeker zo belangrijk was de wens een vrij (grensoverschrijdend) verkeer van gegevens te waarborgen. Ongerechtvaardigde belemmeringen in nationale wetgeving moesten daarom vermeden worden. Om dit te bewerkstelligen kwamen in korte tijd zowel de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO),[7] als de Raad van Europa[8] met initiatieven op het gebied van de persoonsgegevensbescherming. De wijze van aanpak was daarbij gelijk. Beide organisaties formuleerden grotendeels dezelfde basisbeginselen van gegevensbescherming,[9]

---

5. Dit uitte zich bijvoorbeeld in het grootschalige verzet tegen de volkstelling van 1970.
6. Artikel 10, tweede en derde lid, van de Grondwet.
7. OECD Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (September 23, 1980).
8. Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, 28 januari 1981, Trb. 1988, 7.
9. Zie paragraaf 2.3.

welke door de lidstaten in hun wetgeving geïncorporeerd dienden te worden. Omdat deze instrumenten toch niet afdoende bleken om de nationale wetgeving van de Europese landen in voldoende mate met elkaar in overeenstemming te brengen, kwam ook de Europese Unie in 1995 met een richtlijn op dit gebied.[10] De noodzaak tot implementatie van deze richtlijn leidde in Nederland tot de Wet bescherming persoonsgegevens (WBP), die in 2001 de WPR verving.

2.3 Beginselen van persoonsgegevensbescherming

De grondbeginselen van gegevensbescherming, zoals geformuleerd door de OESO en de Raad van Europa, hebben aan de basis gelegen van het huidige recht inzake de bescherming van persoonsgegevens. Zowel de Europese richtlijn als de daarop gebaseerde WBP grijpen grotendeels terug op dezelfde beginselen. Zij vormen daarmee de kern van het persoonsgegevensbeschermingsrecht. Of, zoals Schröder[11] het verwoordt: 'Wie zich gewetensvol aan deze beginselen houdt, zal met persoonsgegevens geen scheve schaatsen rijden.' Een kort overzicht van de grondbeginselen is daarom gewenst.[12] Uitgangspunt daarbij is dat persoonsgegevens op eerlijke en rechtmatige wijze dienen te worden verkregen en verwerkt.

Allereerst mogen de gegevens slechts voor welbepaalde en legitieme doeleinden worden verzameld en is het niet toegestaan deze te gebruiken op een wijze die onverenigbaar is met die doeleinden. Dit zogenoemde doelbindings- of finaliteitsbeginsel is een fundamenteel uitgangspunt van het recht met betrekking tot de bescherming van persoonsgegevens en vormt één van de belangrijkste waarborgen tegen een ongebreidelde verwerking en verstrekking van persoonsgegevens.[13] Het doel waarvoor de persoonsgegevens verzameld worden, bepaalt bovendien ook op andere wijze de grenzen van de gegevensverwerking. Uitgaande van dat doel, moeten de persoonsgegevens nauwkeurig, toereikend, ter zake dienend en niet bovenmatig zijn en mogen ze niet langer worden bewaard dan strikt noodzakelijk is. Periodieke bijwerking of controle van gegevens kan op grond hiervan verplicht zijn. Ten slotte dient voorzien te zijn in passende beveiligingsmaatregelen om toevallige of ongeoorloofde verwerking van de persoonsgegevens te voorkomen.

Voor bepaalde categorieën van gevoelige gegevens gelden striktere voorwaarden. Het gaat hierbij om persoonsgegevens waaruit het ras of de etniciteit, de politieke overtuiging, de godsdienst of andere levensbeschouwing of het lidmaatschap van een

---

10. Europese richtlijn bescherming persoonsgegevens, Richtlijn 95/46/EG, PbEG 1995, L 281, p. 31-50.
11. P. Schröder, Het rijk alleen: Bescherming van persoonsgegevens, de relatie tussen informationele en maatschappelijke bewegingsvrijheid, in: Rathenau Instituut, Privacy geregistreerd: Visies op de maatschappelijke betekenis van privacy, Amsterdam 1998, p. 261.
12. Bij de behandeling van het verstrekkingenregime van de WBP in hoofdstuk 3 zullen sommige beginselen in meer detail terugkomen.
13. Gutwirth noemt het zelfs het hoofdbeginsel van het persoonsgegevensbeschermingsrecht. S. Gutwirth, Privacyvrijheid versus verwerking van persoonsgegevens, in: Rathenau Instituut, Privacy geregistreerd: Visies op de maatschappelijke betekenis van privacy, Amsterdam 1998, p. 91.

vakvereniging blijkt, alsmede gegevens die betrekking hebben op de gezondheid of het seksuele leven. Ook strafrechtelijke gegevens vallen onder een bijzonder regime. Verwerking van deze gegevens is in beginsel verboden, tenzij de wet in een uitzondering voorziet, met inachtneming van passende waarborgen.

Degene wiens gegevens verwerkt worden, beschikt over een aantal algemene rechten. Zo dient hij kennis te kunnen nemen van het bestaan en het doel van de op hem betrekking hebbende gegevensverwerking, alsmede van de identiteit van de daarvoor verantwoordelijke. In sommige gevallen vereist dit een actieve informatieplicht voor laatstgenoemde. In ieder geval verplicht het beginsel van transparantie de verantwoordelijke ertoe zorg te dragen dat de herkomst van persoonsgegevens, alsmede verwerkingen daarvan, zorgvuldig worden bijgehouden, zodat controle daarop achteraf mogelijk blijft. Naast een recht op kennisneming moet de betrokkene de mogelijkheid hebben om verbetering of verwijdering van persoonsgegevens te eisen, indien deze in strijd met de beginselen zijn verwerkt. Dit betekent ook dat in passende mogelijkheden van rechtsbescherming moet zijn voorzien. Uitzonderingen of beperkingen van de werking van de beginselen is over het algemeen slechts toegestaan indien daarin is voorzien bij wet en dit noodzakelijk is ten behoeve van bepaalde zwaarwegende belangen.

2.4 Het karakter van het persoonsgegevensbeschermingsrecht

Sinds de opkomst van de informatiemaatschappij heeft de kwestie van de bescherming van persoonsgegevens bijna voortdurend in de aandacht gestaan. Het is dan ook niet verwonderlijk dat privacy soms op één lijn wordt gesteld met 'informationele privacy': het recht om (enige) invloed te hebben op de wijze waarop en mate waarin op de eigen persoon betrekking hebbende informatie door anderen wordt gebruikt. Toch is deze vereenzelviging van privacy met informationele privacy niet terecht.

Aan de ene kant omvat het privacybegrip veel meer dan enkel de bescherming tegen vergaring en gebruik van persoonsgegevens. Aspecten van de persoonlijke levenssfeer komen onder meer terug in traditionele grondrechten als de vrijheid van godsdienst, het recht op lichamelijke integriteit, de bescherming van de woning en het briefgeheim, maar ook in bijvoorbeeld regels op het gebied van het portretrecht of die met betrekking tot de bescherming van de goede naam (verbod van smaad en laster). Privacy kan zelfs in het geding zijn in verband met zaken als overlast, hinder of vervuiling.[14] Het recht op privacy kan in dat geval worden ingeroepen om invloeden van buitenaf fysiek af te weren.[15]

Aan de andere kant is het persoonsgegevensbeschermingsrecht op haar beurt meer dan alleen een verzameling privacyregels. De regelgeving op dit terrein streeft eigenlijk twee

14. Vgl. EHRM 19 februari 1998, Guerra.
15. Voor een uitgebreider overzicht van de verschillende dimensies van het privacybegrip, zie P.H. Blok en A.H. Vedder, Privacy in ontwikkeling, in: J.E.J. Prins en J.M.A. Berkvens, Privacyregulering in theorie en praktijk, Deventer 2002 (derde druk), p. 5-31.

doeleinden na die zich maar moeilijk met elkaar verdragen. Naast de bescherming van het belang van degene op wie de gegevens zien, wordt tegelijk beoogd het belang van een vrije vergaring en verspreiding van die gegevens te waarborgen. Het is een paradox die, in navolging van de in paragraaf 2.2 beschreven internationale instrumenten, ook haar weg heeft gevonden in de Nederlandse wetgeving. Het gevolg is een constante afweging van het belang van de privacy tegen het belang van een vrije gegevensvergaring. Gelet op de vele hoedanigheden die laatstgenoemd belang kan hebben, dreigt daarbij het gevaar van een verregaande relativering van het grondrecht op privacy. Het belang van de privacy lijkt in de context van de gegevensbescherming niet bij voorbaat meer gewicht te hebben dan bijvoorbeeld het belang van een goede boekhouding. Maar als we aanvaarden dat laatstgenoemd belang de verwerking van bijvoorbeeld adresgegevens rechtvaardigt, hoe kan de verwerking van diezelfde gegevens dan nog als problematisch worden beschouwd indien dit geschiedt ten behoeve van een veel zwaarder belang als bijvoorbeeld het algemeen belang van de veiligheid?

Ontstaan als reactie op de als gevolg van de informatierevolutie gevreesde machtsongelijkheid tussen de overheid (en andere instanties) als verzamelaar van informatie en de burger als het object van informatie, kunnen veel van de regels inzake de bescherming van persoonsgegevens daarom wellicht mede of zelfs beter begrepen worden als instrumenten van beheersing en scheiding van macht. Zo vertoont het beginsel dat gegevens slechts voor een welbepaald doel mogen worden verzameld (doelbinding) veel overeenkomsten met het leerstuk van détournement de pouvoir. Deze uitleg heeft als voordeel dat het een verklaring biedt voor het wisselende gewicht van hetzelfde privacybelang in verschillende situaties waarin sprake is van meer of minder machtige gegevensverwerkers. Daarnaast biedt het een tegenargument voor typeringen van privacy als 'het recht van zonderlingen' of 'de schuilplaats van het kwaad'. Machtenscheiding is immers een oud en beproefd concept, dat haar waarde in vele situaties heeft bewezen.

Het voorgaande is voor sommige schrijvers reden geweest de vraag op te werpen of aanknoping van het persoonsgegevensbeschermingsrecht bij het grondwettelijk recht op privacy wel in ieder opzicht een goede zet is geweest. Blok[16] spreekt zelfs van een historische misser. Toch staat vast dat ook bij de bescherming van persoonsgegevens het grond- en mensenrecht op privacy in het geding is. Artikel 10 van de Grondwet is op dit punt volstrekt helder en ook artikel 8 van het EVRM ziet, blijkens de jurisprudentie van het EHRM,[17] mede op de bescherming van persoonsgegevens. Daarmee zijn de waarborgen van beide artikelen volledig van toepassing. Op zichzelf vertonen deze veel overeenkomsten met de op het gebied van de persoonsgegevensbescherming ontwikkelde beginselen. Artikel 10 van de Grondwet en artikel 8 van het EVRM stellen beide als voorwaarde dat een inbreuk op het recht op privacy te herleiden is tot de wet.[18] Daarnaast eist laatstgenoemd artikel dat de inbreuk noodzakelijk is in een

16. P.H. Blok, De grondslagen van het gegevensbeschermingsrecht herzien, RM Themis 2002, nr. 1, p. 17.
17. Vgl. EHRM 5 mei 2000, Rotaru. Onderwerp van geschil was in deze zaak overigens de verwerking van persoonsgegevens door de Roemeense geheime dienst.
18. In artikel 10 van de Grondwet wordt daarmee bedoeld wetgeving in formele zin. Het begrip 'wet' in artikel 8 van het EVRM wordt door het EHRM ruimer uitgelegd. Ook lagere regelgeving en zelfs een in jurisprudentie ontwikkelde regel valt eronder.

democratische samenleving ten behoeve van één of meer van de in het artikel opgesomde zwaarwegende belangen. Met name het economisch welzijn van het land en de rechten en vrijheden van anderen kunnen potentieel dienen ter rechtvaardiging van veel verwerkingen van persoonsgegevens, maar de kans blijft natuurlijk aanwezig dat het EHRM in een bepaald geval meer gewicht aan het privacybelang zal toekennen dan door bijvoorbeeld de Nederlandse overheid is gedaan.

2.5 Het bijzondere belang van de veiligheid

De vaststelling dat het privacybelang zich eigenlijk in een constant spanningsveld bevindt ten opzichte van een groot aantal tegengestelde belangen, laat onverlet dat de relatie met bepaalde belangen in het bijzonder problematisch kan zijn. Misschien wel het beste voorbeeld daarvan is het algemeen belang van de veiligheid.

Nog meer dan voor andere overheidsinstellingen is informatie van vitaal belang voor de instanties belast met de bestrijding van terrorisme en criminaliteit. In de context van hun taak kan bovendien ieder gegeven van belang zijn, ondanks het soort en de herkomst ervan. Vanuit die optiek is het niet verwonderlijk dat juist veiligheids- en politiediensten over uitgebreide mogelijkheden beschikken tot informatieverzameling. Vanuit een oogpunt van privacy, of machtsbeheersing, kan dit problematisch zijn. Temeer daar veel van de gegevens worden verzameld zonder medeweten van degenen waarop ze betrekking hebben. Ook krijgen gegevens in de context van terrorisme- en criminaliteitsbestrijding al snel een gevoelig karakter, waar ze dat onder andere omstandigheden misschien niet zouden hebben. Beveiliging van die gegevens en beperking van hun gebruik zijn dan in het bijzonder van belang.

Daar komt nog bij dat de politiek als het erop aankomt vaak meer gewicht toekent aan het belang van de veiligheid dan aan het belang van de privacy. Dient zich een nieuwe bedreiging van de veiligheid aan, of een nieuw (technologisch) middel om een reeds bestaande dreiging aan te pakken, dan valt de keuze vaak uit in het voordeel van het belang van de veiligheid. We zien dit op momenteel in de discussie rond het terrorisme en de noodzaak daar adequaat tegen op te kunnen treden. Het lijkt echter een terugkerend fenomeen.[19] Steeds roept dit de vraag op of en hoe nieuwe bevoegdheden in te passen zijn in de bestaande regels op privacygebied.

Onder meer vanwege het voorafgaande zijn in de loop van jaren op het gebied van de veiligheid bijzondere privacyregels totstandgekomen. Vaak blijven daarnaast de algemene regels van groot belang, zij het dat ook daarin in bijzondere uitzonderingsmogelijkheden is voorzien ten behoeve van de veiligheidszorg.

---

19. Een vroeg voorbeeld vormt de fraudebestrijding, die vanaf het eind van de jaren tachtig hoog op de politieke agenda kwam te staan. Instanties actief op dit terrein zagen de mogelijkheden die de invoering van het sofi-nummer meebracht voor de bestrijding van fraude met bijvoorbeeld belastingen en uitkeringen, doordat het de koppeling van diverse overheidsbestanden danig vergemakkelijkte. Deze koppeling stond evenwel haaks op eerdere uitlatingen van de regering dat het sofi-circuit een gesloten systeem zou zijn. Zie F. Kuitenbrouwer, Privacy: een historisch-vergelijkend overzicht, in: J.E.J. Prins en J.M.A. Berkvens, Privacyregulering in theorie en praktijk, Deventer 2002 (derde druk), p. 47.

3 Gegevensverstrekking in het kader van de criminaliteitsbestrijding

3.1 Inleiding

Instanties actief op het gebied van de criminaliteitsbestrijding, zoals politie, bijzondere opsporingsinstanties,[20] alsmede instanties belast met bestuurlijk toezicht op de naleving van wetten zijn alle voor hun taakvervulling in grote mate afhankelijk van informatie die in handen is van derden. Om deze informatie te vergaren beschikken ze over een (steeds groter) arsenaal aan dwangmiddelen. De toepassing van deze bevoegdheden is echter noodzakelijkerwijs gebonden aan voorwaarden en beperkingen. Dit betekent dat uitoefening van dwangmiddelen enerzijds niet altijd mogelijk is en anderzijds de nodige tijd kan kosten. Daarom komt het in de praktijk veelvuldig voor dat aan derden het verzoek wordt gedaan om relevante gegevens vrijwillig te verstrekken. Met sommige derden kan zo zelfs een 'innige' verstandhouding ontstaan, waarbij met grote regelmaat informatie wordt uitgewisseld en daarover ook algemene afspraken worden gemaakt. Gedacht kan bijvoorbeeld worden aan internetproviders of verzekeraars.

Bij deze informatieverstrekking kunnen ook persoonsgegevens worden uitgewisseld. De vraag rijst dan of en in hoeverre verstrekking is toegestaan en welke regels daarop van toepassing zijn. Over deze vraag gaat het komende hoofdstuk.

3.2 De relevante wetgeving

De algemene regels voor de omgang met persoonsgegevens zijn neergelegd in de Wet bescherming persoonsgegevens (WBP). Deze wet wordt gekenmerkt door een ruime

20. Een voorbeeld van een bijzondere opsporingsinstantie is de FIOD-ECD, ontstaan uit het samengaan van de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) en de Economische Controledienst (ECD).

werkingssfeer en ziet in beginsel op iedere verwerking[21] van persoonsgegevens,[22] ongeacht door wie en voor welk doel. Een onderscheid tussen de publieke en private sector wordt daarbij niet gemaakt. De WBP is dus evenzeer van toepassing op het ledenbestand van een studentenvereniging, opgeslagen op de thuiscomputer van een van de bestuursleden,[23] als op het veel omvangrijkere 'leden'-bestand van bijvoorbeeld de Informatie Beheer Groep of Belastingdienst.

Voor verwerkingen door de politie bestaat echter ingevolge artikel 2, tweede lid, onder c, van de WBP een uitzondering.[24] Indien de politie persoonsgegevens opslaat en gebruikt ten behoeve van de uitvoering van de aan haar opgedragen taken,[25] waaronder de voorkoming en opsporing van strafbare feiten, is daarop de Wet politieregisters (Wet Pol.r.) van toepassing. Wat de bijzondere opsporingsinstanties betreft, is de situatie genuanceerder. Op hen blijft de WBP van toepassing, tenzij bij algemene maatregel van bestuur is bepaald dat de Wet Pol.r. ook voor hen geldt.[26]

De Wet Pol.r. bevat onder meer een groot aantal bepalingen inzake de mogelijkheden tot verstrekking van persoonsgegevens door de politie aan derden.[27] De bepalingen over de *verkrijging* van gegevens door de politie zijn echter beperkt. Weliswaar bepaalt artikel 4 van de Wet Pol.r. dat in een politieregister slechts rechtmatig verkregen gegevens kunnen worden opgenomen, maar de wet geeft zelf niet aan wanneer van een rechtmatige verkrijging sprake is. Om deze vraag te kunnen beantwoorden dient dus naar andere regelgeving gekeken te worden.

Is sprake van de toepassing van dwangmiddelen, bijvoorbeeld op basis van het Wetboek van Strafvordering, dan zal de rechtmatigheid van de verkrijging door die wet bepaald worden.[28] Voor de beoordeling van de rechtmatigheid van een vrijwillige verstrekking van persoonsgegevens door een derde aan de politie zal evenwel in de meeste gevallen naar de WBP gekeken moeten worden. De verstrekkende derde zal

---

21. Artikel 1, onder b, van de WBP maakt duidelijk dat het begrip 'verwerking' alle stadia van gegevensbehandeling, van verkrijging tot verwijdering, omvat. Wel moet ingevolge artikel 2, eerste lid, van de WBP sprake zijn van een geheel of gedeeltelijk geautomatiseerde verwerking, dan wel van een niet geautomatiseerde verwerking van persoonsgegevens die in een bestand (een gestructureerd geheel van persoonsgegevens) zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
22. Onder 'persoonsgegeven' wordt ingevolge artikel 1, onder a, van de WBP verstaan elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat de informatie in ieder geval herleidbaar moet zijn tot een natuurlijke persoon.
23. Verwerkingen van persoonsgegevens puur voor persoonlijke doeleinden vallen overigens ingevolge artikel 2, tweede lid, onder a, van de WBP buiten de reikwijdte van die wet.
24. Ook voor gegevensverwerkingen door justitie en de inlichtingen- en veiligheidsdiensten is in een uitzondering voorzien. Voor hen is een afzonderlijke regeling neergelegd in respectievelijk de Wet justitiële gegevens en de Wet op de inlichtingen- en veiligheidsdiensten 2002.
25. Ingevolge artikel 2 van de Politiewet 1993 heeft de politie tot taak 'in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven'.
26. Vgl. artikel 13c van de Wet Pol.r., alsmede artikel 18a van het Besluit politieregisters.
27. Ik ga op deze bepalingen niet verder in, maar volsta met de opmerking dat in de Wet Pol.r. een relatief gesloten systeem van gegevensverstrekking is neergelegd. Voor een bespreking van deze wet, zie A.E.B.M. van der Ven, Overzicht Wet politieregisters, in: J.E.J. Prins en J.M.A. Berkvens, Privacyregulering in theorie en praktijk, Deventer 2002 (derde druk), p. 135-158.
28. Op de verhouding tussen de WBP en verplichtingen tot informatieverstrekking kom ik in paragraaf 3.9 terug.

immers vrijwel steeds onder laatstgenoemde wet vallen. Doordat de WBP de rechtmatigheid van de verstrekking door de derde bepaalt, bepaalt zij eveneens,[29] via artikel 4 van de Wet Pol.r., de rechtmatigheid van de verkrijging door de politie. Anders dan artikel 2 van de WBP doet vermoeden, is de WBP dus wel degelijk ook voor de politie van groot belang, zij het indirect.[30]

Een voorbeeld helpt wellicht om dit te verduidelijken. Na ernstige rellen tijdens een voetbalduel is de politie op zoek naar de mogelijke aanstichters daarvan. De voetbalclub in kwestie beschikt over potentieel relevante informatie. Daarbij kan gedacht worden aan video-opnames gemaakt door camera's in en rond het stadion, maar ook aan gegevens, verkregen door middel van elektronische registratie, over de seizoenkaarthouders die al dan niet de desbetreffende wedstrijd hebben bezocht. Beide soorten informatie kunnen de politie een beeld geven van welke notoire relschoppers bij de wedstrijd aanwezig zijn geweest. Stel dat de voetbalclub deze informatie inderdaad op verzoek aan de politie verstrekt. Net als alle andere verwerkingen van persoonsgegevens door de voetbalclub, wordt deze verstrekking genormeerd door de WBP. Blijkt achteraf dat de verstrekking onrechtmatig, want in strijd met de WBP, is geweest, dan kan dit ook de verkrijging door de politie onrechtmatig maken, hetgeen uiteindelijk als consequentie kan hebben dat de desbetreffende gegevens niet voor de bewijsvoering gebruikt kunnen worden.[31]

3.3 Enige algemene opmerkingen over de WBP

Niet alle bepalingen van de WBP zijn voor het onderwerp van dit hoofdstuk even belangrijk. In de hiernavolgende paragrafen zal in detail worden ingegaan op de materiële normen die voor de toelaatbaarheid van een verstrekking van persoonsgegevens het meest van belang zijn. Voordat dit wordt behandeld, wordt in deze paragraaf kort stilgestaan bij de inhoud en systematiek van de WBP als geheel. In grote lijnen[32] komen de bepalingen van de WBP overeen met de eerder in paragraaf 2.3 besproken grondbeginselen van persoonsgegevensbescherming. Het gaat daarbij achtereenvolgens om de toelaatbaarheid en kwaliteit van gegevensverwerkingen, transparantie en rechten van betrokkenen,[33] alsmede toezicht en rechtsbescherming.

---

29. Overigens lijkt er in de rechtspraak op dit punt - mijns inziens ten onrechte - enige terughoudendheid te bestaan. Vgl. Eric Schreuders e.a., Als de politie iets wil weten…, De informatieuitwisseling tussen de politie en de particuliere sector op basis van artikel 11 lid 2 van de Wet persoonsregistraties, Den Haag 1999, p. 32-33.
30. In ieder geval zal er rekening mee moeten worden gehouden dat een derde die aansprakelijk wordt gesteld wegens een onrechtmatige verstrekking van persoonsgegevens aan de politie, in de toekomst niet of minder snel geneigd zal zijn tot samenwerking.
31. Overigens leidt een onrechtmatige verstrekking van persoonsgegevens, zelfs indien op grond daarvan ook de verkrijging door de politie onrechtmatig wordt geacht, niet per definitie tot bewijsuitsluiting. Voor een uitgebreide bespreking van bewijsuitsluiting, zie M.C.D. Embregts, Uitsluitsel over bewijsuitsluiting: Een onderzoek naar de toelaatbaarheid van onrechtmatig verkregen bewijs in het strafrecht, het civiele recht en het bestuursrecht, Deventer 2003, alsmede A.M. van Woensel, Sanctionering van onrechtmatig verkregen bewijsmateriaal, DD 2004, nr. 2, p. 119-171.
32. Op de overige bepalingen van de WBP, bijvoorbeeld de bijzondere bepalingen omtrent het gegevensverkeer met landen van buiten de Europese Unie, ga ik niet nader in.
33. De betrokkene is degene op wie de persoonsgegevens betrekking hebben (artikel 1, onder f, van de WBP).

De regels die betrekking hebben op de toelaatbaarheid en de kwaliteit van de gegevensverwerking, zijn te vinden in de artikelen 6 tot en met 24 van de WBP. Als algemeen basisprincipe geldt artikel 6, waarin is bepaald dat persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze dienen te worden verwerkt. Dit wordt vervolgens in de daaropvolgende artikelen (7 tot en met 14) uitgewerkt. Zo worden voorwaarden gesteld aan de doeleinden van de gegevensverwerking, alsmede aan de nauwkeurigheid, toereikendheid, beveiliging en bewaring van de gegevens. Naast dit algemene regime bevat de wet voor gevoelige gegevens,[34] de WBP spreekt van bijzondere gegevens, een aangescherpt regime in de artikelen 16 tot en met 23. Verwerking van deze gegevens is verboden, tenzij de WBP uitdrukkelijk in een uitzondering voorziet. Ook in dat geval blijven de algemene regels echter van toepassing.

De artikelen 33 tot en met 42 van de WBP geven een invulling aan het beginsel van transparantie en de daarmee verband houdende rechten van betrokkenen. Uitgangspunt is een actieve informatieplicht voor de voor de verwerking verantwoordelijke[35] instantie. Deze is onder meer gehouden tot bekendmaking aan de betrokkene van zijn identiteit en het doel van de verwerking. Wel bestaan belangrijke uitzonderingen op deze verplichting, met name indien de gegevensverwerking bij of krachtens de wet is voorgeschreven.[36] Ook dan is de verantwoordelijke echter steeds gehouden de herkomst van de gegevens vast te leggen. Bovendien blijft voor de verantwoordelijke een informatieplicht bestaan, in de gevallen waarin door de betrokkene een verzoek om kennisneming van op hem betrekking hebbende gegevens wordt gedaan. Daarnaast beschikt de betrokkene over een recht op correctie van die gegevens, alsmede een recht op verzet tegen bepaalde soorten verwerkingen. Een bijzonder recht is ten slotte neergelegd in artikel 42 van de WBP, waarin grenzen worden gesteld aan de automatisering van beslissingen. Eenieder heeft, behoudens bepaalde uitzonderingen, het recht niet te worden onderworpen aan hem rakende besluiten, indien dat besluit enkel wordt genomen op grond van een geautomatiseerde gegevensverwerking betreffende bepaalde aspecten van iemands persoonlijkheid. Een menselijke afweging is in dat geval op enigerlei moment noodzakelijk. Te denken valt bijvoorbeeld aan de weigering iemand te verzekeren, omdat deze tot een risicogroep behoort.[37]

Het toezicht op de naleving van de WBP is in handen van het College bescherming persoonsgegevens (CBP). De WBP regelt de instelling en rechtspositie van het CBP en bekleedt haar met taken[38] en bevoegdheden. Zo beschikt het CBP over een aantal

---

34. Zie paragraaf 2.3.
35. Verantwoordelijke is ingevolge artikel 1, onder d, van de WBP degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Dit laat onverlet dat de eigenlijke verwerking door een ander kan worden uitgevoerd.
36. Voor kritiek op deze uitzondering, zie J.E.J. Prins en J.M.A. Berkvens, De Wet bescherming persoonsgegevens, in: J.E.J. Prins en J.M.A. Berkvens, Privacyregulering in theorie en praktijk, Deventer 2002 (derde druk), p. 93. Daarnaast bestaat geen actieve informatieplicht indien mededeling aan de betrokkene onmogelijk blijkt of een onevenredige inspanning zou vereisen.
37. Op grond van artikel 42 van de WBP kunnen wellicht ook vraagtekens gezet worden bij het plan van de Raad van de Rechtspraak om eenvoudige civiele zaken volledig geautomatiseerd af te gaan handelen.
38. Naast toezicht op de naleving van de WBP en andere wetten, houdt het CBP zich onder meer bezig met wetgevingsadvies aan de regering.

bevoegdheden waarmee opgetreden kan worden tegen onrechtmatige gegevensverwerkingen, zoals het toepassen van bestuursdwang en het opleggen van een bestuurlijke boete. De wijze waarop het CBP op het spoor komt van een mogelijke overtreding van de WBP kan verschillend zijn. Voor de meeste verwerkingen geldt een meldingsplicht bij het CBP, soms in combinatie met een verplicht voorafgaand onderzoek. Daarnaast kan het CBP naar aanleiding van een klacht of ambtshalve een onderzoek instellen. Naast het toezicht door het CBP bestaat de mogelijkheid dat binnen een instantie of sector een functionaris voor de gegevensbescherming wordt aangesteld, die een deel van de toezichthoudende taken van het CBP overneemt. Ten slotte staat voor een betrokkene wiens rechten onder de WBP zijn geschonden de gang naar de rechter open. In de WBP is daarbij gekozen voor een gedifferentieerd systeem van rechterlijke toetsing. Is er sprake van een besluit in de zin van de Algemene wet bestuursrecht, bijvoorbeeld indien een bestuursorgaan een beslissing neemt op een verzoek van een betrokkene om kennisneming, dan is de bestuursrechter bevoegd. In andere gevallen kan men zich richten tot de burgerlijk rechter.

3.4 Het doel heiligt de verstrekking

De belangrijkste materiële norm met betrekking tot de verwerking van persoonsgegevens is dat aan het gebruik van deze gegevens een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel ten grondslag dient te liggen. In de WBP is dit beginsel van doelbinding in artikel 7 neergelegd. Daaruit vloeit onder meer voort dat het doel reeds bepaald dient te zijn voordat de eerste verwerking, de verzameling van de gegevens, plaats heeft gevonden. Bovendien moet het met een zodanige precisie zijn omschreven dat ermee daadwerkelijk een kader geboden wordt voor toetsing of de gegevens noodzakelijk zijn om het doel te bereiken.

De voorwaarde dat het om een gerechtvaardigd doel dient te gaan, is nader uitgewerkt in artikel 8 van de WBP. Daarvan is slechts sprake indien het doel te herleiden is tot één of meer van de in dat artikel onder a tot en met f neergelegde gronden voor gegevensverwerking. Achtereenvolgens gaat het daarbij om toestemming van de betrokkene, uitvoering van een overeenkomst waarbij de betrokkene partij is, nakoming van een wettelijke verplichting, vrijwaring van een vitaal belang van de betrokkene, uitvoering van een publiekrechtelijke taak en behartiging van een gerechtvaardigd belang. Met uitzondering van de eerste grond geldt daarbij steeds de aanvullende voorwaarde dat de gegevensverwerking noodzakelijk dient te zijn om het doel te bereiken. In het licht van artikel 8 van het EVRM veronderstelt dit een belangenafweging tussen het met de gegevensverwerking gediende doel en het privacybelang van de betrokkene, waarbij onder meer eisen van proportionaliteit en subsidiariteit een rol spelen.

Artikel 9 van de WBP bevat de eis dat een verdere verwerking van persoonsgegevens niet onverenigbaar is met de doeleinden waarvoor deze zijn verkregen. Gebruik van de gegevens voor andere doeleinden dan waarvoor ze verzameld zijn, is dus mogelijk zolang dat gebruik verenigbaar is met het oorspronkelijke doel. Daarmee is artikel 9 van bijzonder belang voor wat betreft de mogelijkheden tot verstrekking van persoonsgegevens. Een verstrekking door de verantwoordelijke aan een derde is immers per definitie een 'verdere verwerking', waarvoor steeds de eis van verenigbaar gebruik zal

gelden.[39] Of sprake is van verenigbaar gebruik dient per geval te worden bepaald. In het tweede lid van artikel 9 zijn daartoe een aantal relevante factoren opgesomd. Zoals ook al uit deze, overigens niet-limitatieve, opsomming blijkt, is verenigbaar gebruik meer dan alleen een bepaalde mate van verwantschap tussen het doel van de verdere verwerking en het doel waarvoor de gegevens oorspronkelijk zijn verkregen. Daarnaast kunnen van belang zijn de aard van de gegevens, de gevolgen van de beoogde verwerking voor de betrokkene, de wijze van verkrijging van de gegevens en de mate waarin jegens de betrokkene in passende waarborgen is voorzien. De vraag waar het uiteindelijk om lijkt te gaan is of de betrokkene de verdere verwerking (verstrekking) redelijkerwijs kon verwachten.[40]

3.5 Gerechtvaardigd en verenigbaar: een dubbele voorwaarde

Hoewel de in artikel 9 van de WBP neergelegde voorwaarde van verenigbaar gebruik de mogelijkheid biedt tot verstrekking van persoonsgegevens voor een ander doel dan waarvoor de gegevens zijn verzameld, dient bedacht te worden dat ook deze verstrekking te herleiden moet zijn tot ten minste één van de verwerkingsgronden van artikel 8 van de WBP. Een verstrekking is immers zowel een verwerking als een verdere verwerking. De voorwaarden van gerechtvaardigde doeleinden en verenigbaar gebruik zijn derhalve cumulatief. Of een verstrekking uiteindelijk toegestaan is, hangt steeds af van zowel de gerechtvaardigdheid van het doel van de verstrekking op zichzelf, als de verenigbaarheid daarvan met het oorspronkelijke doel waarvoor de gegevens zijn verzameld. Dit is ook door het CBP in haar oordelen bevestigd.[41] Overigens zal in de praktijk niet altijd sprake zijn van een dubbele voorwaarde. Indien bijvoorbeeld de toestemming van de betrokkene wordt verkregen voor een verstrekking van zijn gegevens, zal dit volgens het CBP vrijwel[42] steeds voldoende zijn om deze te legitimeren.[43]

Voegt de voorwaarde van verenigbaar gebruik in die situatie dus niet veel toe aan de voorwaarde dat sprake dient te zijn van een gerechtvaardigd doel, bij andere verwerkingsgronden is die toegevoegde waarde prominenter aanwezig. Dit is met name het geval bij verstrekkingen ter uitvoering van een publiekrechtelijke taak of ter beharti-

---

39. De memorie van toelichting bevestigt dat de voorwaarde van verenigbaar gebruik zowel voor binnen als buiten de organisatie van de verantwoordelijke geldt, dus ook voor verstrekkingen aan derden (Kamerstukken II 1997-1998, 25 892, nr. 3, p. 89).
40. Vgl. CBP 31 juli 2001, z2001-0179.
41. Idem.
42. Het door het CBP gemaakte voorbehoud ziet waarschijnlijk op situaties waarin aan de toestemming een gebrek kleeft of waarin de wet de toestemming van de betrokkene zelfs uitdrukkelijk als rechtvaardigingsgrond heeft uitgesloten. Deze gevallen lijken mij overigens reeds verdisconteerd in de omschrijving van toestemming in artikel 1, onder i, van de WBP als elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene de gegevensverwerking aanvaardt, alsmede de eis van artikel 8 van de WBP dat het om ondubbelzinnige toestemming dient te gaan.
43. Een soortgelijk geval doet zich voor indien een gegevensverstrekking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene. Deze verwerkingsgrond dient blijkens de memorie van toelichting (Kamerstukken II 1997-1997, 25 892, nr. 3, p. 84) eng geïnterpreteerd te worden: er moet sprake zijn van een dringende *medische* noodzaak. Het enige geval dat ik me kan voorstellen waarin dit wellicht niet voldoende zou zijn om een gegevensverstrekking te legitimeren, is indien de betrokkene kenbaar heeft gemaakt niet behandeld te willen worden. In dat geval kom je echter mijns inziens niet meer toe aan de vraag of de verstrekking verenigbaar is, maar strandt zij al op de eis van noodzakelijkheid uit artikel 8 van de WBP.

ging van een gerechtvaardigd belang, de laatste twee verwerkingsgronden van artikel 8. Het is vooral hier dat het gevaar van een ongebreidelde uitwisseling van gegevens, met alle negatieve consequenties van dien, zich doet voelen. De activiteiten van de overheid, waaronder veel activiteiten zonder een uitdrukkelijke wettelijke basis, zijn dermate uitgebreid en divers dat gegevens verzameld in het kader van de ene taak vanuit een privacy-oogpunt niet per definitie gebruikt kunnen worden ter vervulling van een andere, op zichzelf legitieme taak. Hetzelfde geldt indien het gaat om verstrekking van persoonsgegevens ten behoeve van een gerechtvaardigd belang van de verantwoordelijke of een derde. Wederom is het aantal situaties waarin deze verwerkingsgrond mogelijk toepasselijk is, nagenoeg onbeperkt. Vrijwel ieder belang komt potentieel in aanmerking, waarmee artikel 8, onder f, in feite een restbepaling vormt. Een enigszins zinvolle invulling van het beginsel van doelbinding dient in dat geval grenzen te stellen aan verstrekkingen op deze grondslag, ook al is het belang in kwestie op zichzelf gerechtvaardigd.

3.6 Verenigbaarheid en criminaliteitsbestrijding

In de sfeer van de criminaliteitsbestrijding zijn het, naast de wettelijke verplichting, vooral de uitvoering van een publiekrechtelijke taak en de behartiging van een gerechtvaardigd belang, welke de grondslag voor een verstrekking zullen vormen.[44] Zoals in de vorige paragraaf bleek, is de voorwaarde van verenigbaar gebruik juist dan van groot belang.

Lopen we evenwel de factoren van artikel 9 van de WBP langs vanuit het perspectief van de verstrekking in het kader van de criminaliteitsbestrijding, dan dringt zich al snel de conclusie op dat verenigbaar gebruik in die context niet snel kan worden aangenomen. Het gaat immers vaak om gevoelige gegevens,[45] soms heimelijk verkregen, en het gebruik van deze gegevens heeft meestal ingrijpende negatieve consequenties voor de betrokkene. Daarbij kan gedacht worden aan vervolging door justitie, maar ook aan bijvoorbeeld een onrechtmatigedaadsactie. Naast juridische consequenties kunnen zich bovendien gevolgen van feitelijke aard voordoen, zoals negatieve publiciteit en aantasting van iemands goede naam. Veel zal in dat geval afhangen van de vraag in hoeverre sprake is van verwantschap met het oorspronkelijke doel van verkrijging en of voldoende waarborgen bestaan voor de betrokkene.

Een onderscheid dient daarom te worden gemaakt tussen het verstrekken van persoonsgegevens die reeds vanaf de eerste verzameling (mede) ten behoeve van de criminaliteitsbestrijding zijn verwerkt en gegevens die oorspronkelijk voor geheel andere doeleinden verzameld zijn. De voorwaarde van verenigbaar gebruik lijkt zich tegen verstrekking van laatstgenoemde gegevens te verzetten.

---

44. Toestemming van de betrokkene, uitvoering van een overeenkomst waarbij de betrokkene partij is en vrijwaring van een vitaal belang van de betrokkene zullen minder snel een grondslag voor verwerking bieden, nu het bij de criminaliteitsbestrijding veelal gaat om informatie die tegen de wil en zonder medeweten van de betrokkene wordt verzameld en gebruikt.
45. Althans gebruik van persoonsgegevens in een gevoelige context.

3.7 Criminaliteitsbestrijding als uitzondering

Geen regel zonder uitzonderingen; dat geldt ook voor de voorwaarde van verenigbaar gebruik. Ingevolge artikel 43 van de WBP kan op grond van een vijftal zwaarwegende belangen, waaronder de veiligheid van de staat en de voorkoming, opsporing en vervolging van strafbare feiten, afgeweken worden van hetgeen in artikel 9 is bepaald. Daarnaast laat artikel 43 op grond van dezelfde belangen uitzonderingen toe op het recht van de betrokkene op informatie omtrent op hem betrekking hebbende gegevensverwerkingen. De vraag rijst in hoeverre deze bepaling een oplossing biedt voor het aan het einde van de vorige paragraaf gesignaleerde probleem.

Het karakter van een uitzonderingsclausule brengt natuurlijk reeds met zich dat de bepaling beperkt moet worden opgevat. Dit bevestigt de memorie van toelichting bij de WBP,[46] waarin vermeld wordt dat artikel 43 slechts bedoeld is voor uitzonderlijke omstandigheden en restrictief geïnterpreteerd dient te worden. Ook het CBP heeft zich in vergelijkbare bewoordingen uitgelaten en daaraan nog toegevoegd dat artikel 43 geen basis kan zijn voor systematische gegevensverstrekking.[47] Welke uitzonderlijke omstandigheden precies worden bedoeld, wordt evenwel niet aangegeven.

Om hier achter te komen is het nodig terug te kijken naar de situatie onder de voorloper van de WBP, de Wet persoonsregistraties (WPR). Volgens de memorie van toelichting[48] sluit artikel 43 van de WBP aan bij artikel 11, tweede lid, van de WPR en is ten opzichte daarvan geen inhoudelijke wijziging beoogd. Artikel 11, tweede lid, maakte verstrekking aan een derde ook zonder enige doelbinding mogelijk, indien sprake was van een dringende en gewichtige reden en de persoonlijke levenssfeer van de geregistreerde niet onevenredig werd geschaad. Het artikel werd in de praktijk door de Registratiekamer, de toenmalige privacywaakhond, eng geïnterpreteerd.[49] Aan de eis van dringendheid kwam, naast de eis van gewichtigheid, een eigen betekenis toe. Het moest gaan om een spoedeisend belang, om een noodgeval. Zo oordeelde de Registratiekamer in een zaak waarin door een waterleidingmaatschappij verbruiksgegevens van een klant aan opsporingsambtenaren van de sociale dienst waren verstrekt, dat dit op grond van dringende en gewichtige redenen kon plaatsvinden 'in geval van misdrijven van ernstige aard c.q. gebeurtenissen van ernstige aard die een directe actie noodzakelijk maken, terwijl de gewenste informatie niet tijdig of zonder grote inspanning op een andere wijze kan worden verkregen'.[50] Daarvan was in die zaak geen sprake, aldus de Registratiekamer.

Nu de door de memorie van toelichting bij de WBP en het CBP gebruikte bewoordingen bevestigen dat artikel 43 van de WBP op gelijke wijze moet worden uitgelegd als artikel 11, tweede lid, van de WPR, kan de conclusie niet anders zijn dan dat de

---

46. Kamerstukken II 1997-1998, 25 892, nr. 3, p. 92.
47. CBP 24 september 2001, z2001-1280.
48. Kamerstukken II 1997-1998, 25 892, nr. 3, p. 171.
49. E.C. Mac Gillavry, Privacy en opsporing, NJB 2000/33, p. 1673-1675.
50. Registratiekamer 22 augustus 1994, 93.E.213, in: B.M.A. van Eck, U. van de Pol en C.G. Zandee, Persoonsgegevens beschermd, van WPR naar WBP, Uitspraken van de Registratiekamer, Den Haag 1999, p. 191-195.

daarin opgenomen uitzonderingsclausule slechts bedoeld is voor onverwachte gebeurtenissen, noodgevallen en calamiteiten. Buiten deze situaties zal een verstrekking ten behoeve van de criminaliteitsbestrijding moeten voldoen aan de voorwaarde van verenigbaar gebruik. Dit veronderstelt dat wanneer instanties, actief op dit terrein, een meer structurele uitwisseling van informatie noodzakelijk achten, zij daarop zullen moeten anticiperen door de relevant geachte informatie vanaf het begin mede ten behoeve van de criminaliteitsbestrijding te verwerken, met inachtneming van alle daarvoor geldende normen.

3.8 Criminaliteitsbestrijding als doel

Om de kans om aan de voorwaarde van artikel 9 te kunnen voldoen te vergroten, ligt het dus voor de hand om criminaliteitsbestrijding expliciet tot doel te stellen bij de verzameling van persoonsgegevens en reeds dan te voorzien in de mogelijkheid van uitwisseling van die gegevens met andere op dit terrein actieve instanties. De WBP biedt hier ook mogelijkheden toe. Daarbij wordt, geheel in lijn met het algemene karakter van de wet, geen fundamenteel onderscheid gemaakt tussen de publieke en de private sector. Mede vanwege het feit dat de overheid onmogelijk in staat is zelf overal en te allen tijde tegen criminaliteit op te treden, alsmede de onvrede die daarover binnen de samenleving bestaat, heeft de wetgever erkend dat ook private instanties een gerechtvaardigde beveiligingsbehoefte hebben in welk verband onder omstandigheden de verwerking van persoonsgegevens noodzakelijk kan zijn. Denk aan de reeds genoemde voetbalclub.

De verwerkingsgrond wordt in dit soort gevallen gevormd door artikel 8, onder f, van de WBP voor wat betreft particuliere organisaties en artikel 8, onder e, voor wat betreft overheidsinstanties. Wel moet er steeds rekening mee gehouden worden dat naast het algemene regime inzake gegevensverwerking ook het regime met betrekking tot de verwerking van bijzondere gegevens van toepassing kan zijn. Met name dient daarbij gedacht te worden aan de verwerking van strafrechtelijke gegevens, één van de in artikel 16 van de WBP genoemde categorieën waarvoor een verwerkingsverbod geldt, behoudens uitzonderingen in de daaropvolgende artikelen.[51]

Het begrip strafrechtelijke gegevens heeft betrekking zowel op veroordelingen als op min of meer gegronde verdenkingen. Voorts omvat het gegevens betreffende de toepassing van het formele strafrecht, bijvoorbeeld het gegeven dat iemand is gearresteerd of dat tegen hem proces-verbaal is opgemaakt. Niet ieder persoonsgegeven dat in de sfeer van de veiligheid wordt verwerkt is dus automatisch aan te merken als een strafrechtelijk gegeven. De gegevens over de aanwezigheid van seizoenkaarthouders bij een voetbalwedstrijd uit het eerder aangehaalde voorbeeld zijn bijvoorbeeld niet als

51. Ook gegevens betreffende iemands ras zullen in de sfeer van de veiligheid veelvuldig worden verzameld. Een foto of video-opname van een persoon zal immers vaak informatie over diens ras verschaffen. Artikel 18, onder a, van de WBP bepaalt evenwel dat raciale gegevens verwerkt mogen worden ter identificatie van de betrokkene indien voor dat doel onvermijdelijk.

zodanig aan te merken, nu daaruit op zichzelf geen gegronde verdenking kan worden afgeleid. Anders is het wellicht met de videobeelden van de beveiligingscamera's in het stadion. Indien op die beelden door herkenbare personen strafbare feiten worden gepleegd, kan gesproken worden van een gegronde verdenking en zijn de video-opnames aan te merken als strafrechtelijke gegevens in de zin van artikel 16 van de WBP.

Naast strafrechtelijke gegevens worden in artikel 16 als categorie van bijzondere gegevens genoemd persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Daarbij moet gedacht worden aan door een rechter opgelegde maatregelen, zoals een straatverbod of omgangsverbod. Aanzeggingen van de eigenaar van bijvoorbeeld een winkel dat iemand zijn zaak niet meer mag betreden vallen dus niet onder het bijzondere regime. In dat geval dient te worden teruggevallen op het algemene regime van persoonsgegevens.

Artikel 22 van de WBP biedt een aantal uitzonderingsmogelijkheden op het in artikel 16 vastgelegde verbod om strafrechtelijke en aanverwante gegevens te verwerken. Indien sprake is van een uitzondering op dat verbod, bepaalt artikel 22, vijfde lid, bovendien dat ook andere bijzondere persoonsgegevens dan strafrechtelijke gegevens verwerkt kunnen worden, mits noodzakelijk.[52] Voor bijzondere opsporingsinstanties voorziet het eerste lid in een algemene uitzondering, hetgeen tevens verstrekkingen door deze instanties aan derden mogelijk maakt. Voor andere instanties is voorzien in de mogelijkheid om vorenbedoelde gegevens te verwerken ter bescherming van zichzelf of hun werknemers tegen gepleegde of mogelijk nog te plegen strafbare feiten.[53] De mogelijkheden om deze gegevens ook met anderen te delen zijn echter beperkter. Daarvoor is in het algemeen vereist dat passende en specifieke waarborgen worden gecreëerd en na een voorafgaand onderzoek door het CBP toestemming is verleend.[54]

Het CBP heeft in het verleden geregeld onderzoek gedaan naar samenwerkingsverbanden op het gebied van de criminaliteitsbestrijding, waarbinnen ook bijzondere persoonsgegevens werden uitgewisseld, en meestal kon toestemming worden verkregen. Zo kreeg Stichting Brein recentelijk toestemming voor de verwerking van persoonsgegevens in een 'anti-piraterijdatabestand' dat zij ten behoeve van een groot aantal organisaties op het gebied van audio, video en interactieve producten bijhoudt.[55] Ook Koninklijk Horeca Nederland kreeg, na een eerdere afwijzing, uiteindelijk toestemming voor het voeren van een interne waarschuwingsdienst (zwarte lijst) als middel tegen bestrijding van fraude en misbruik door klanten of leveranciers van horecabedrijven.[56]

---

52. Voor wat betreft de verwerking van andere categorieën bijzondere gegevens dan strafrechtelijke gegevens in het kader van de criminaliteitsbestrijding, kan bovendien artikel 23, eerste lid, onder e, van de WBP een basis bieden.
53. Artikel 22, tweede lid, onder b, van de WBP.
54. Artikel 22, vierde lid, onder c en artikel 31, eerste lid, onder c, van de WBP. Voor samenwerking in concernverband of verwerkingen door van de juiste vergunningen voorziene particuliere beveiligingsorganisaties en recherchebureaus ten behoeve van derden geldt deze eis evenwel niet.
55. CBP 16 april 2004, z2003-1660.
56. CBP 5 februari 2003, z2002-0796.

Over het algemeen houden de 'passende en specifieke waarborgen' genoemd in artikel 22, vierde lid, onder c, van de WBP met name een aanscherping in van de ook in het algemeen voor gegevensverwerking geldende voorwaarden. Zo dient voorzien te worden in beveiliging en afscherming van de gegevens en dienen de rechten van betrokkenen gewaarborgd te zijn. Daarnaast is bij strafrechtelijke en aanverwante gegevens van groot belang dat de bewaartermijn niet langer dan noodzakelijk is.[57] Ook is van belang dat de verantwoordelijkheden van de verschillende deelnemers duidelijk geregeld zijn. Wel lijkt het CBP als eis te stellen dat de schade als gevolg van criminaliteit een bepaalde omvang heeft bereikt vooraleer het opzetten van een samenwerkingsverband en het onderling uitwisselen van bijzondere persoonsgegevens gerechtvaardigd kan worden geacht.[58] Met name beroepsgroepen die in verhoogde mate te maken krijgen met criminaliteit lijken dus in aanmerking te komen. Is slechts sprake van incidentele criminaliteit, dan is aangifte bij de politie een beter alternatief.

3.9 Wettelijke plicht en verenigbaar gebruik

Een verwerkingsgrond die tot nu toe nog niet aan de orde is geweest, is de uitvoering van een wettelijke plicht in artikel 8, onder c, van de WBP. De reden dat deze verwerkingsgrond in een aparte paragraaf behandeld wordt, is dat bij de wettelijke plicht als grondslag voor een verstrekking zich de vraag opdringt of de voorwaarde van verenigbaar gebruik, neergelegd in artikel 9, überhaupt nog wel gesteld kan worden. Dit houdt verband met de verhouding van de WBP tot andere wetten. Daarbij geldt als regel dat de WBP steeds van toepassing is, tenzij in de WBP zelf een uitzondering is gemaakt. De belangrijkste uitzonderingen op de reikwijdte van de WBP zijn te vinden in artikel 2 van de wet. Daarnaast kan evenwel uit andere dan de daar genoemde wetten een verplichting tot gegevensverstrekking voortvloeien.

Daarbij zijn twee situaties te onderscheiden. Allereerst is mogelijk dat de wet de gegevensverstrekking niet als zodanig voorschrijft, maar een andersoortige verplichting oplegt ter uitvoering waarvan de verantwoordelijke de verstrekking noodzakelijk acht. Dit noodzakelijkheidsoordeel dient uiteraard getoetst te worden, in het kader waarvan ook de eis van verenigbaar gebruik een rol kan spelen.

Daarnaast leggen veel wetten rechtstreeks een verplichting tot verstrekking van (persoons)gegevens op. Zo beschikken toezichthoudende instanties vaak over ruime bevoegdheden om informatie van derden te vorderen. In dat laatste geval rijst de vraag of artikel 9 nog wel van toepassing kan zijn. De ruimte voor een verantwoordelijke om op grond van dit artikel een verstrekking te weigeren waartoe hij ingevolge een andere wet direct verplicht is, zal, zo al aanwezig, toch zeer beperkt zijn. Overigens geldt

57. Zowel het recht van eenieder om voor onschuldig te worden gehouden zolang zijn schuld niet in rechte is komen vast te staan (presumptio innocentiae), als het belang om niet duurzaam van de samenleving te worden uitgesloten (resocialisatiebelang) spelen hierbij een rol. Vgl. de memorie van toelichting bij de WBP, Kamerstukken II 1997-1998, 25 892, nr. 3, p. 118.
58. CBP 5 februari 2003, z2002-0796.

hetzelfde voor de noodzakelijkheid van de verstrekking. Indien de wetgever reeds heeft bepaald dat de verstrekking noodzakelijk is, is moeilijk voorstelbaar dat een verantwoordelijke deze afweging zelf nog eens overdoet. Dit geldt temeer wanneer op basis van de wet in kwestie al een afweging van onder meer het recht op privacy van de betrokkene heeft plaatsgevonden, zoals bij de Wet openbaarheid van bestuur.

Ook in de oordelen van het CBP komt deze kwestie terug. In een zaak waarin de koppeling van bestanden tussen nutsbedrijven en gemeenten in het kader van de opsporing van socialezekerheidsfraude centraal stond,[59] stelt het CBP vast dat de desbetreffende koppeling als een inbreuk op de persoonlijke levenssfeer kan worden gezien, met name vanwege het niet-voorziene aspect ervan. Het gaat, aldus het CBP, om twee registraties van gegevens die in geen, althans ver verwijderd verband met elkaar staan en waarbij de koppeling daarvan ingrijpende gevolgen kan hebben voor de betrokkenen. Ondanks deze vaststelling, die toch het sterke vermoeden van onverenigbaar gebruik oproept, toetst het CBP niet aan artikel 9 van de WBP. Dit is opvallend omdat het CBP in andere beslissingen wel uitdrukkelijk aandacht besteedt aan dit artikel.[60] De reden daarvoor is mijns inziens gelegen in de omstandigheid dat de nutsbedrijven op grond van artikel 122 van de Algemene bijstandswet verplicht waren tot het desgevraagd verlenen van opgaven en inlichtingen, noodzakelijk voor de uitvoering van deze wet, aan burgemeester en wethouders. Wel toetst het CBP de verstrekking en de daaropvolgende verwerkingen expliciet aan artikel 8 van het EVRM.[61]

De verwerkingsgrond van de wettelijke plicht biedt de wetgever dus de mogelijkheid om verstrekking van persoonsgegevens mogelijk te maken, ook indien niet voldaan wordt aan de eis van verenigbaar gebruik. Daarnaast kan ook het verbod op de verwerking (verstrekking) van bijzondere gegevens op grond van een bijzondere wet opzij worden gezet.[62] Dit is met name van belang voor instanties actief op het gebied van opsporing en toezicht, voor wie ook gegevens verkregen van buiten die sfeer van groot belang kunnen zijn voor een goede taakvervulling. Het is daarbij wel te hopen dat de wetgever het fundamentele belang van doelbinding, ook als instrument van beheersing en scheiding van macht, steeds in het oog houdt. Anders kan de wettelijke plicht wel eens de achilleshiel van het verstrekkingenregime van de WBP worden. De bijzondere wet zal echter steeds moeten voldoen aan de eisen van artikel 8 van het EVRM, die onverminderd blijven gelden.

---

59. CBP 27 januari 2003, z2001-1157.
60. Vgl. CBP 13 januari 2004, z2004-0058.
61. In dat verband overweegt het CBP dat de bestrijding van fraude in het algemeen is aan te merken als een legitieme inmenging van de overheid in de persoonlijke levenssfeer van burgers. Met name kan deze inmenging worden gerechtvaardigd in het belang van het economisch welzijn van het land of de voorkoming van strafbare feiten. Wel stelt het CBP zich op het standpunt dat de koppeling van de bestanden een substantiële bijdrage moet leveren aan de fraudebestrijding. Indien en zolang daarvan sprake is, wordt voldaan aan de eis van proportionaliteit.
62. Vgl. artikel 23, eerste lid, onder e, van de WBP.

3.10 Conclusie

Verstrekkingen van persoonsgegevens ten behoeve van de criminaliteitsbestrijding zijn blijkens het voorgaande problematisch indien het gaat om gegevens die oorspronkelijk voor heel andere doeleinden zijn verzameld. Het beginsel van doelbinding en verenigbaar gebruik, neergelegd in de artikelen 7 tot en met 9 van de WBP, verzet zich veelal tegen de verstrekking. Weliswaar biedt de WBP in artikel 43 de mogelijkheid om uitzonderingen op de voorwaarde van verenigbaar gebruik te maken, indien noodzakelijk in het belang van de veiligheid van de staat of de voorkoming, opsporing en vervolging van strafbare feiten, maar deze uitzonderingsclausule wordt in de praktijk zeer beperkt geïnterpreteerd. Wil verstrekking daarbuiten mogelijk zijn, dan dient reeds bij de oorspronkelijke verzameling geanticipeerd te worden op een eventuele noodzaak om gegevens ten behoeve van criminaliteitsbestrijding te verwerken. Ook de wetgever kan dit doen door verstrekking van persoonsgegevens aan instanties belast met toezicht en opsporing verplicht te stellen in bijzondere wetgeving, maar zal daarbij steeds rekening dienen te houden met de waarborgen van artikel 8 van het EVRM.

4 Naar een algemene informatieplicht?

4.1 Inleiding

In het voorgaande hoofdstuk is uiteengezet dat het privacyregime van de WBP, in het bijzonder de voorwaarde van verenigbaar gebruik, de vrijwillige verstrekking van persoonsgegevens door derden aan opsporingsinstanties vaak niet toestaat. In de alledaagse praktijk is evenwel sprake van een aanzienlijk aantal verzoeken om informatie door laatstgenoemden aan een grote verscheidenheid van maatschappelijke instanties.

Gebleken is dat met een dergelijk informatieverzoek, zeker indien het betrekking heeft op persoonsgegevens, verschillend wordt omgegaan.[63] Sommige instanties verstrekken deze gegevens in ruime mate, andere vrijwel niet. De mate van kennis van de toepasselijke normen is daarbij van belang, hetgeen afhankelijk is van uiteenlopende factoren als het soort instantie, haar omvang en organisatie, evenals de intensiteit en frequentie van de samenwerking met opsporingsinstanties.[64] In veel gevallen ontbreekt specifieke kennis van het privacyrecht en is bij de beslissing op een verzoek het 'gezond verstand' van de toevallige[65] behandelaar van doorslaggevende betekenis. Dit zal overigens niet altijd leiden tot een meer welwillende afhandeling van het verzoek. De vrees voor aansprakelijkheid in geval van onjuiste of onrechtmatige verstrekking kan ertoe leiden dat het verzoek wordt afgewezen, ook al is die vrees in het concrete geval onterecht.

De huidige situatie is daarmee voor geen van de bij een gegevensverstrekking betrokken partijen optimaal. Zowel degene op wie de gegevens betrekking hebben, als de opsporingsinstantie is afhankelijk van de gegevenshouder, terwijl laatstgenoemde wordt geconfronteerd met een soms moeilijke belangenafweging en het risico van aansprakelijkheid. Vooral vanuit het perspectief van de opsporing is deze afhankelijkheid onwenselijk. Gegevens die in handen zijn van derden (personen, instanties en bedrijven) kunnen van groot belang zijn voor de opsporing van strafbare feiten. Door het gebruik van informatie- en communicatietechnologie beschikken derden bovendien over steeds grotere hoeveelheden (persoons)gegevens. Daar komt nog bij dat de mogelijkheden voor opsporingsinstanties om anders dan via vrijwillige verstrekking deze gegevens te vergaren in de praktijk als te beperkt worden beschouwd. In de hiernavolgende paragraaf wordt hier in meer detail bij stilgestaan.

---

63. Vgl. Eric Schreuders e.a., Als de politie iets wil weten…, De informatieuitwisseling tussen de politie en de particuliere sector op basis van artikel 11 lid 2 van de Wet persoonsregistraties, Den Haag 1999.
64. Met name instanties in de financiële sector (banken, verzekeraars) en de telecommunicatiesector (telefoonbedrijven, internetproviders) worden vrij routinematig bevraagd. Vaak bestaan daarover ook algemene afspraken.
65. Vooral veel kleine organisaties beschikken niet over een speciaal voor de afhandeling van informatieverzoeken aangewezen persoon of afdeling.

De vraag rijst in ieder geval of niet een nieuwe balans gerealiseerd dient te worden tussen de met bescherming van persoonsgegevens en opsporing van strafbare feiten gemoeide belangen, alsmede hoe dat het beste kan geschieden. De regering heeft deze vraag bevestigend beantwoord en als oplossing voor de gesignaleerde problemen gekozen voor de invoering van een vrijwel algemene strafvorderlijke informatieplicht. Na een uiteenzetting van de voorgestelde nieuwe bevoegdheden zal worden beargumenteerd waarom een dergelijke plicht niet wenselijk is en welke alternatieven bestaan om aan de op zichzelf gerechtvaardigde informatiebehoefte van opsporingsinstanties tegemoet te komen, met zo veel mogelijk behoud van privacybescherming.

4.2 Knelpunten in de huidige bevoegdheden

De mogelijkheden voor opsporingsinstanties om derden te verplichten tot het verstrekken van persoonsgegevens worden door velen als ontoereikend beschouwd. Zoals wel vaker liggen technologische ontwikkelingen aan de basis van dit ongenoegen.

Kern van het probleem is dat gegevens niet als zodanig in aanmerking komen voor inbeslagneming.[66] Een vordering tot inbeslagneming zal daarom steeds betrekking moeten hebben op de 'gegevensdrager'. Lange tijd was dit het papieren document waarin de gegevens waren vastgelegd. Steeds vaker worden gegevens evenwel enkel in digitale vorm opgeslagen. Inbeslagneming kan in dat geval problematisch zijn. Zo is niet van tevoren vast te stellen welke gegevens precies op de gegevensdrager staan en of niet méér dan de benodigde informatie wordt verkregen. Indien de gegevens op de harde schijf van een computer staan, kan het in beslag nemen daarvan bovendien al snel buitenproportioneel zijn. Soms is inbeslagneming van de gegevensdrager zelfs fysiek onmogelijk, namelijk wanneer de informatie zich op afstand (internet) bevindt. Om onderzoek te kunnen doen in de computerbestanden zelf is op dit moment inschakeling van de rechter-commissaris noodzakelijk,[67] waarmee vaak de nodige extra tijd gemoeid zal zijn.

Om dit probleem te omzeilen vorderden opsporingsambtenaren in de praktijk vaak niet inbeslagneming van de oorspronkelijke gegevensdrager, maar van een kopie of uitdraai daarvan. Ook vrijwillige verstrekking van de gegevens werd als een alternatief beschouwd. De eerste gang van zaken verdraagt zich evenwel niet met de uitdrukkelijke verdeling van bevoegdheden, neergelegd in het Wetboek van Strafvordering,[68] terwijl de tweede haar beperkingen vindt in het regime van de WBP.

66. Het zijn immers geen voorwerpen (zaken en vermogensrechten) als bedoeld in artikel 94 Sv.
67. Artikel 125i Sv.
68. Vgl. M. van Stratum, Privacy en opsporing II, NJB 2000/43, p. 2087-2088.

4.3 Nieuwe bevoegdheden tot gegevensvordering

Om een oplossing te vinden voor de gesignaleerde problemen is in maart 2000 de Commissie-Mevis[69] ingesteld. In haar rapport, uitgebracht in mei 2001, bepleit de commissie als oplossing een forse uitbreiding van de bevoegdheden op het gebied van de strafvorderlijke gegevensvergaring. Naar aanleiding hiervan heeft de regering op 23 februari 2004 een wetsvoorstel[70] bij de Tweede Kamer ingediend strekkende tot opneming in het Wetboek van Strafvordering van algemene bevoegdheden voor met opsporing belaste instanties tot het vorderen van gegevens, daaronder begrepen persoonsgegevens.

De kern van het wetsvoorstel wordt gevormd door de nieuw te creëren bevoegdheden tot het vorderen van gegevens. Daarbij wordt een onderscheid gemaakt tussen verschillende soorten informatie: identificerende gegevens, andere gegevens en gevoelige gegevens. Het hoeft daarbij overigens niet te gaan om de gegevens van de verdachte. Ook van niet-verdachte personen kunnen gegevens worden opgevraagd indien dat in het belang van het onderzoek is.[71] De kring van tot vordering bevoegden verschilt al naar gelang het soort informatie. Hetzelfde geldt voor de categorieën van strafbare feiten ten aanzien waarvan een vorderingsbevoegdheid kan worden aangewend. Een vordering tot gegevensverstrekking kan in beginsel worden gericht tot iedere persoon of instantie die de desbetreffende gegevens heeft opgeslagen of vastgelegd. Dit kunnen natuurlijke personen, bedrijven of andere particuliere instanties zijn, maar ook overheidsinstellingen. De vordering kan echter niet tot de verdachte worden gericht of betrekking hebben op gegevens die onder het verschoningsrecht van een beroepsgeheimhouder vallen.

Aan opsporingsambtenaren[72] wordt de bevoegdheid toegekend om ter opsporing van ieder misdrijf identificerende gegevens van een persoon te vorderen. Onder identificerende gegevens worden verstaan: naam, adres, woonplaats, postadres, geboortedatum, geslacht, administratieve kenmerken (bijvoorbeeld een lidmaatschapsnummer) en, in geval van een rechtspersoon, rechtsvorm en vestigingsplaats.

Andere dan identificerende gegevens kunnen door de officier van justitie worden gevorderd in geval van een misdrijf waarvoor voorlopige hechtenis mogelijk is, dan wel indien sprake is van het in georganiseerd verband plegen of beramen van misdrijven. In geval van verdenking van een ander strafbaar feit, waaronder overtredingen, kunnen deze gegevens worden gevorderd na machtiging door de rechter-commissaris. Deze machtiging is ook noodzakelijk indien de officier van justitie voornemens is gevoelige gegevens te vorderen. In dat geval is de categorie van misdrijven waarvoor dit mogelijk

---

69. De Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, naar haar voorzitter Commissie-Mevis genoemd.
70. Kamerstukken II 2003-2004, 29 441, nr. 2.
71. Wel zal volgens de memorie van toelichting bij een niet-verdachte persoon minder snel voldaan zijn aan eisen van proportionaliteit en subsidiariteit. Vgl. Kamerstukken II 2003-2004, 29 441, nr. 3, p. 6.
72. In de praktijk zal naar alle waarschijnlijkheid een beper\king worden aangebracht in het aantal opsporingsambtenaren dat de bevoegdheid kan toepassen.

is bovendien nog verder beperkt.[73] Wel dient bedacht te worden dat de officier van justitie slechts gehouden is deze procedure te volgen indien de vordering expliciet ziet op gevoelige gegevens of in situaties waarin het voor de hand ligt dat dergelijke gegevens het resultaat zullen zijn van een vordering, bijvoorbeeld indien een vordering gericht wordt aan een kerkgenootschap. In andere situaties kan de officier van justitie de gewone procedure volgen. Indien later blijkt dat daarbij ook gevoelige gegevens zijn vergaard, maakt dat de uitoefening van de vorderingsbevoegdheid niet achteraf onrechtmatig, aldus de memorie van toelichting.[74]

Van belang is ook de bevoegdheid van de officier van justitie om de vordering van andere gegevens, niet zijnde gevoelige gegevens, (mede) betrekking te laten hebben op gegevens die na het tijdstip van de vordering worden verwerkt. Het betreft hier dus toekomstige gegevens. Het dient daarbij wel te gaan om gegevens die door de desbetreffende instantie in het kader van de reguliere werkzaamheden zullen worden verzameld en de verplichting mag niet onevenredig belastend zijn. De periode waarover de vordering zich uitstrekt is maximaal vier weken, maar kan telkens met wederom maximaal vier weken worden verlengd. Indien het belang van het onderzoek dit dringend vordert, kan daarbij, met tussenkomst van de rechter-commissaris, de verplichting worden opgelegd om de gegevens onverwijld na de verwerking te verstrekken. De memorie van toelichting noemt als voorbeeld het geval waarin herhaaldelijk fraude wordt gepleegd met een gestolen bankpasje. Een snelle verstrekking kan er dan aan bijdragen dat het spoor naar de dader zichtbaar blijft.

Indien de voorgestelde bevoegdheden totstandkomen, zal er volgens de regering geen ruimte meer zijn voor opsporingsambtenaren om een verzoek tot vrijwillige verstrekking van persoonsgegevens te doen op basis van de WBP.[75] Wel blijft denkbaar dat een derde op eigen initiatief persoonsgegevens verstrekt, bijvoorbeeld in geval van een noodsituatie als bedoeld in artikel 43 van de WBP. In alle overige gevallen zal een verstrekking echter met gebruikmaking van de nieuwe bevoegdheden gevorderd dienen te worden, met inachtneming van de daaraan verbonden beperkingen en formaliteiten. Omzeiling hiervan zou immers de in het wetsvoorstel gemaakte afweging tussen opsporing en privacy teniet doen.[76]

Om misbruik of omzeiling van de bevoegdheden en willekeurige inmenging in de persoonlijke levenssfeer van burgers te voorkomen zijn een aantal vereisten geformuleerd waaraan een vordering tot gegevensverstrekking dient te voldoen. Zo moet de vordering in beginsel schriftelijk zijn en dient zij een zo nauwkeurig mogelijke aandui-

---

73. Het moet in dat geval gaan om verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.
74. Kamerstukken II 2003-2004, 29 441, nr. 3, p. 10.
75. Dit was ook een door het CBP gestelde eis.
76. Het is te hopen dat het in de praktijk ook zo zal uitpakken. Ik voorzie wat dat betreft toch nog wel problemen, met name wanneer het de opsporing van overtredingen betreft. Daarvoor is ingevolge het wetsvoorstel steeds inschakeling van de rechter-commissaris nodig, ook indien het gaat om het vorderen van identificerende gegevens. De neiging zal voor opsporingsambtenaren in de praktijk wellicht groot zijn om juist in het geval van overtredingen te kiezen voor de gemakkelijkere en snellere optie van een vormvrij verzoek aan de desbetreffende instantie. Strikt toezicht daarop is vanzelfsprekend van groot belang.

ding te bevatten van de gegevens die worden gevorderd. Dit sluit overigens niet uit dat ten aanzien van hele groepen personen bepaalde gegevens worden gevorderd. Wederom kan daarbij gedacht worden aan het in het vorige hoofdstuk aangehaalde voorbeeld van de voetbalclub die over gegevens beschikt omtrent de aan- en afwezigheid van seizoenkaarthouders bij een voetbalduel waar zich ernstige rellen hebben voorgedaan, ervan uitgaande natuurlijk dat bij die rellen dusdanig ernstige strafbare feiten zijn begaan dat van de bevoegdheid tot gegevensvordering gebruik kan worden gemaakt.[77] Daarnaast dient van de gegevensverstrekking een proces-verbaal te worden opgemaakt, waarin de feiten en omstandigheden moeten worden vermeld waaruit blijkt dat is voldaan aan het vereiste van een verdenking van een strafbaar feit van een bepaalde ernst en waarin de reden waarom de gegevens in het belang van het onderzoek worden gevorderd dient te worden vermeld. Aan de hand van dit proces-verbaal kan later worden vastgesteld of een vordering terecht is gedaan.

Ten slotte wordt ook de in het wetsvoorstel voorziene kostenvergoeding gezien als een middel om een buitenproportionele toepassing van de bevoegdheden tegen te gaan.[78]

Op het gebied van de rechtsbescherming is in het wetsvoorstel voorzien in een beklagrecht voor belanghebbenden. Dit betekent dat zowel degene op wie de gevorderde gegevens betrekking hebben als degene die tot verstrekking wordt verplicht beklag kunnen doen. Het beklag heeft evenwel geen schorsende werking.[79] Bovendien hoeft notificatie van de gegevensverstrekking aan degene op wie de gegevens zien niet plaats te vinden zolang het belang van het onderzoek zich daartegen verzet, zodat het wel even kan duren voordat de betrokkene van het beklagrecht gebruik kan maken.[80]

4.4 Kritiek vanuit privacy-oogpunt

Bij het wetsvoorstel en het rapport van de Commissie-Mevis zijn door onder meer het CBP de nodige kanttekeningen geplaatst.[81] Ten dele is de regering aan deze kritiek tegemoetgekomen. Op het gebied van de formele waarborgen, zoals transparantie en controleerbaarheid lijkt het wetsvoorstel, althans op papier, te voldoen. Het meest fundamentele punt van kritiek is door de regering evenwel niet weggenomen. Dit betreft het ruime toepassingsbereik van de te creëren bevoegdheden en de vraag naar de rechtvaardiging daarvan.

Vooropgesteld dient te worden dat hier sprake is van een verregaande algemene informatieplicht. Met de nieuwe bevoegdheden zal het in beginsel mogelijk worden om van

77. De memorie van toelichting noemt zelf het voorbeeld van de vondst van een pakket cocaïne in de bagage van een bepaalde vlucht, in welk geval de vordering van de passagierslijst kan bijdragen aan het achterhalen van de persoon die de bagage heeft meegebracht.
78. Overigens komen kosten slechts voor vergoeding in aanmerking, indien zij boven op de kosten van een reguliere bedrijfsvoering komen.
79. Het CBP is van mening dat de mogelijkheid van een voorafgaande rechterlijke toets van de vordering noodzakelijk is.
80. Van de verstrekking van identificerende gegevens behoeft zelfs helemaal geen notificatie plaats te vinden, nu deze verstrekking slechts als een 'lichte' inbreuk op de privacy wordt beschouwd.
81. Vgl. CBP 7 november 2001, z2001-0735, waarin het CBP advies uitbrengt naar aanleiding van het rapport van de Commissie-Mevis.

elk gegeven verstrekking te vorderen, inclusief persoonsgegevens. Een onderscheid tussen de gegevens van verdachte en niet-verdachte personen wordt daarbij niet gemaakt. Ook de groep van personen en instanties tot wie de vordering tot gegevensverstrekking kan worden gericht, is vrijwel onbeperkt. In feite betekent dit een omkering van de huidige situatie. Onder de WBP vormt de verstrekking van gegevens aan de politie, in ieder geval indien het gegevens betreft die oorspronkelijk voor andere doelen verwerkt zijn, de uitzondering op de regel. Bovendien geschiedt deze verstrekking op vrijwillige basis. De nieuwe wet zal verstrekking verplicht stellen en tot regel maken. Fundamentele beginselen van doelbinding en verenigbaar gebruik kunnen dan nauwelijks nog een rol spelen.

Een dusdanig ingrijpende wijziging veronderstelt een duidelijk aantoonbare noodzaak. Het is aan de regering om dit te onderbouwen. Zoals het CBP terecht vaststelt, is de regering daar tot op heden niet in geslaagd. De in de praktijk gesignaleerde knelpunten lijken zich vooral voor te doen in bepaalde maatschappelijke sectoren, waarin sprake is van een meer dan incidentele samenwerking tussen opsporingsinstanties en bedrijfsleven. Daarbij dient met name gedacht te worden aan de telecommunicatiesector en de financiële sector. Dit wordt overigens door de regering zelf bevestigd.[82] Voor de genoemde sectoren bestaan echter al strafvorderlijke bevoegdheden tot het vorderen van gegevens. Op geen enkele wijze wordt door de regering inzichtelijk gemaakt waarom met deze bevoegdheden, of een beperkte uitbreiding daarvan, bijvoorbeeld tot alleen bedrijven,[83] niet zou kunnen worden volstaan. Een algemeen betoog over de noodzaak van adequate gegevensvergaring door opsporingsinstanties is daarvoor volstrekt onvoldoende. Veel te gemakkelijk stelt de regering de begrijpelijke wens van opsporingsinstanties om de in de informatiemaatschappij in steeds grotere mate aanwezige informatie te kunnen benutten, gelijk met de noodzaak om deze informatie ook voor hen toegankelijk te maken.

Bijzonder problematisch is bovendien de mogelijkheid om ook overheidsinstanties te verplichten tot gegevensverstrekking.[84] Vaak beschikken deze instanties over persoonsgegevens, verkregen op grond van een wettelijke verplichting ten behoeve van de uitoefening van een specifieke overheidstaak. De inbreuk op de privacy van de betrokkene die daarmee reeds is gemoeid, wordt gerechtvaardigd door beperking van het gebruik van de persoonsgegevens tot de uitvoering van de desbetreffende taak. Ook hier speelt doelbinding een cruciale rol in het scheppen van waarborgen voor de bescherming van de persoonlijke levenssfeer. Een algemene strafvorderlijke informatieplicht haalt evenwel een streep door deze waarborgen, hetgeen tevens de invoering van nieuwe wettelijke informatieplichten bij voorbaat problematisch zou maken.

Daar komt bij dat de kans vergroot wordt dat een verdachte op deze wijze verplicht wordt (indirect) mee te werken aan zijn eigen veroordeling. Net als op ieder ander

---

82. Vgl. Kamerstukken II 2003-2004, 29 441, nr. 6, p. 24.
83. Vgl. E.C. Mac Gillavry, Gegevensvergaring in de informatiemaatschappij: een strafvorderlijke informatieplicht? I. De informatieplicht van de Commissie-Mevis, RM Themis 2002, nr. 1, p. 27-30.
84. CBP 7 november 2001, z2001-0735.

zullen op een verdachte ingevolge diverse wettelijke regelingen informatieverplichtingen rusten, die op zich niets te maken hebben met de opsporing van strafbare feiten. Na invoering van de nieuwe bevoegdheden zal een verdachte er echter steeds rekening mee moeten houden dat de door hem verstrekte gegevens bij de politie terecht kunnen komen. Hoe verhoudt zich dat tot zijn, ook door het EVRM gewaarborgde recht,[85] zichzelf niet te incrimineren?[86] Het wetsvoorstel zegt hier weinig over. Het bepaalt slechts dat van de verdachte niet rechtstreeks informatie gevorderd kan worden.

Ten slotte kan worden opgemerkt dat de door de regering gekozen oplossing om nog een andere reden verder lijkt te gaan dan door het geconstateerde probleem wordt gerechtvaardigd. Naast het wegnemen van obstakels in de gegevensverstrekking door derden aan de politie beoogt het wetsvoorstel een daaraan gerelateerd probleem op te lossen.[87] Dat probleem is dat opsporingsambtenaren in de praktijk meestal niet weten welke personen of instanties voor een zaak relevante informatie in handen hebben. Dit zorgt voor een 'natuurlijke' beperking van de kring van personen en instanties waaraan een verzoek om verstrekking van gegevens zal worden gedaan. Hetzelfde geldt voor de thans in het Wetboek van Strafvordering neergelegde dwangmiddelen van inbeslagneming en onderzoek in computerbestanden. Deze kunnen slechts worden toegepast indien een redelijk vermoeden bestaat dat een persoon of instantie over voor het onderzoek relevante voorwerpen of computergegevens beschikt. Had de regering enkel het oorspronkelijke probleem op willen lossen, dan had zij kunnen volstaan met het creëren van een bevoegdheid tot het vorderen van voor het onderzoek relevante gegevens van diegenen waarvan redelijkerwijs vermoed kan worden dat zij erover beschikken. Door evenwel voor opsporingsambtenaren een relatief eenvoudige mogelijkheid te creëren identificerende gegevens te vorderen, zal onder de nieuwe regeling eerder en van meer personen en instanties kunnen worden vastgesteld of sprake is van vorenbedoeld redelijk vermoeden. Juist de 'lichtste' bevoegdheid uit het wetsvoorstel is dus de grootste noviteit en potentieel het meest ingrijpend, nu daarmee alle andere dwangmiddelen uit het Wetboek van Strafvordering in stelling gebracht kunnen worden.

Gelet op het voorgaande dient ernstig te worden getwijfeld of de voorgestelde strafvorderlijke bevoegdheden de toets aan artikel 8 van het EVRM kunnen doorstaan. Het betreft hier immers de toepassing van dwangmiddelen waarmee inbreuk wordt gemaakt op het in dat artikel neergelegde recht op privacy. Daarvoor geldt naast de eis van een uitdrukkelijke wettelijke grondslag tevens de voorwaarde dat de inbreuk noodzakelijk moet zijn in een democratische samenleving.

---

85. EHRM 17 december 1996, Saunders.
86. Uit de jurisprudentie van de Hoge Raad is af te leiden dat het gebruik van toezichthoudende bevoegdheden ten behoeve van de opsporing in beginsel toegelaten is, maar dat rekening gehouden moet worden met 'de aan de verdacht als zodanig toekomende waarborgen', meer in het bijzonder diens zwijgrecht. Zie J.M. Sjöcrona en D.V.A. Brouwer, Opsporing door toezicht, Adv.bl. 2001, nr. 12, p. 440-443.
87. Vgl. E.C. Mac Gillavry, Gegevensvergaring in de informatiemaatschappij: een strafvorderlijke informatieplicht? I. de informatieplicht van de Commissie-Mevis, RM Themis 2002, nr. 1, p. 28.

4.5 Alternatieven gebaseerd op vrijwilligheid

De vraag kan worden gesteld of dwang noodzakelijk is, nu evengoed alternatieven denkbaar zijn die gebaseerd zijn op vrijwilligheid, maar meer dan thans de mogelijkheid zouden bieden om in bepaalde gevallen tegemoet te komen aan het opsporingsbelang. Het subsidiariteitsbeginsel staat in dat geval aan het creëren van een nieuw dwangmiddel in de weg.

Een mijns inziens voor de hand liggend alternatief is een aanpassing van de invulling van artikel 43 van de WBP. Een van de grootste obstakels voor vrijwillige verstrekkingen aan opsporingsinstanties is namelijk de beperkte interpretatie die op dit moment aan deze uitzonderingsclausule wordt gegeven. Verantwoordelijk daarvoor is, zoals in paragraaf 3.7 is aangegeven, het vereiste van spoedeisendheid, welk vereiste als gevolg heeft dat de toepassing van artikel 43 beperkt blijft tot onvoorziene gebeurtenissen. Dit sluit toepassing van het artikel uit indien het een bij herhaling gedaan verzoek betreft, ook al is met dat verzoek steeds een op zichzelf voldoende zwaarwegend opsporingsbelang gemoeid. Het vereiste van spoedeisendheid verplicht tot enige anticipatie.

Wordt dit vereiste evenwel losgelaten, dan wordt het mogelijk om steeds indien het onderzoeksbelang voldoende gewichtig is tot verstrekking over te gaan. Daarvoor is niet eens een wijziging van artikel 43 nodig, nu de eis van spoedeisendheid daarin niet meer als zodanig voorkomt. Een afweging per geval blijft weliswaar vereist, maar dit sluit slechts de mogelijkheid van automatische, niet van structurele verstrekking uit. Het is immers niet ondenkbaar dat in negen van de tien gevallen een afweging tussen het belang van privacy en het opsporingsbelang in het voordeel van laatstgenoemde uitvalt. Toegegeven, het verplicht degene tot wie het verzoek om informatie gericht wordt tot een soms moeilijke afweging, maar dat zal de privacybescherming alleen maar ten goede komen, nu het waarschijnlijk is dat bij twijfel verstrekking zal worden geweigerd. Overigens lijkt het me best mogelijk om de verantwoordelijke daarbij te voorzien van enige richtsnoeren, waarbij het CBP een rol kan spelen.[88]

Een ander mogelijk alternatief, voorgesteld door Mac Gillavry,[89] is het in zijn geheel opzij zetten van de in de WBP neergelegde beperkingen ten aanzien van de vrijwillige verstrekking van persoonsgegevens aan opsporingsinstanties. Voor een dergelijke oplossing is eerder ook ten aanzien van de inlichtingen- en veiligheidsdiensten gekozen. Op grond van artikel 17 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 zijn zij bevoegd zich tot iedere persoon of instantie te richten met het verzoek om verstrekking van gegevens, terwijl de regels van de WBP ten aanzien van die verstrekking niet van toepassing zijn verklaard.[90] Verstrekking van de gegevens is echter niet verplicht.

---

88. Indien (mede) sprake is van het verstrekken van bijzondere gegevens zal het CBP vaak toch al voorafgaand aan de verstrekking toestemming moeten verlenen, een situatie die mijns inziens te prefereren is boven een beklagrecht achteraf.
89. E.C. Mac Gillavry, Gegevensvergaring in de informatiemaatschappij: een strafvorderlijke informatieplicht? I. De informatieplicht van de Commissie-Mevis, RM Themis 2002, nr. 1, p. 29.
90. Deze bevoegdheid is overigens een uitbreiding ten opzichte van de oude Wet op de inlichtingen- en veiligheidsdiensten.

Meer nog dan het eerste alternatief biedt het voorstel van Mac Gillavry de mogelijkheid om tegemoet te komen aan de behoefte aan informatie van opsporingsinstanties. De mogelijkheden van verstrekking worden ruimer, maar ook in dit geval blijft het mogelijk voor bijvoorbeeld een bedrijf dat om de gegevens van zijn cliënten wordt verzocht om bij de beslissing op het verzoek de belangen van laatstgenoemden mee te laten wegen. Het creëren van een bevoegdheid tot het vragen, niet vorderen, van gegevens maakt het bovendien mogelijk om de uitoefening van deze bevoegdheid aan voorwaarden en beperkingen te binden.

Blijft over het bezwaar van Mevis[91] dat in een systeem van vrijwilligheid de verstrekking afhankelijk zou kunnen worden van degene op wie de gegevens betrekking hebben, indien deze met de gegevenshouder contractueel overeenkomt dat deze niet worden verstrekt. Ook voor dit probleem zouden mijns inziens echter minder vergaande oplossingen dan het invoeren van een vrijwel algemene informatieplicht bedacht kunnen worden, langs de lijnen van de hiervoor geopperde alternatieven.

4.6 Conclusie

De noodzaak van een algemene informatieplicht als opgenomen in het thans bij de Tweede Kamer liggende wetsvoorstel is door de regering niet aangetoond. De regering lijkt de wens van opsporingsinstanties om te kunnen beschikken over alle mogelijk relevante informatie in handen van derden, gelijk te stellen met de noodzaak om deze informatie ook voor hen toegankelijk te maken en kiest bovendien voor een veel te zwaar middel. Gelet op het verregaande karakter van de nieuw te creëren dwangmiddelen kan niet worden gesproken van een maatregel die 'noodzakelijk is in een democratische samenleving' als bedoeld in artikel 8 van het EVRM. Afgaande op de reacties uit de Tweede Kamer[92] zullen de nieuwe bevoegdheden er echter ongetwijfeld komen. Veel hangt dan af van de wijze waarop en mate waarin de rechter de toepassing daarvan in concreto zal toetsen.

91. P.A.M. Mevis, Gegevensvergaring in de informatiemaatschappij: een strafvorderlijke informatieplicht?, II. Gegevensvergaring is iets anders dan een informatieplicht, RM Themis 2002, nr. 1, p. 34.
92. Vgl. Kamerstukken II 2003-2004, 29 441, nr. 6.

5 Tot slot

Het is vrijwel onmogelijk geworden om deel te nemen aan de huidige maatschappij zonder daarbij op grote schaal persoonlijke gegevens vrij te moeten geven. Voor veel diensten zullen bijvoorbeeld op zijn minst basale gegevens als naam, adres of rekeningnummer verstrekt moeten worden. Wanneer we dit doen, verwachten we impliciet dat deze gegevens niet worden gebruikt voor een ander doel dan waarvoor ze zijn verstrekt. Juridisch heeft deze verwachting gestalte gekregen in het beginsel van doelbinding, dat daarmee terecht als de meest fundamentele norm van persoonsgegevensbescherming wordt beschouwd. Zonder deze norm zou elke controle over de eigen gegevens verloren gaan.

Even vanzelfsprekend is dat doelbinding geen harde eis kan zijn wanneer het aankomt op een effectieve aanpak van criminaliteit. Ieder gegeven kan in dat verband immers van cruciaal belang zijn. Dat uitzonderingen op het beginsel van doelbinding ten behoeve van de criminaliteitsbestrijding mogelijk moeten zijn, staat ook niet ter discussie. Inbreuk op dit fundamentele beginsel zou mijns inziens evenwel zo veel mogelijk de uitzondering moeten blijven, in plaats van de regel.

Stellingen

1. Het beginsel van doelbinding, met als sluitstuk de voorwaarde van verenigbaar gebruik, is het meest fundamentele beginsel van persoonsgegevensbescherming en inbreuken daarop dienen ook in het kader van de criminaliteitsbestrijding uitzondering te blijven.

2. Andere waarborgen op het gebied van de gegevensbescherming, zoals transparantie en rechtsbescherming, kunnen een inbreuk op het beginsel van doelbinding niet compenseren. Zij komen als mosterd na de maaltijd indien de uitkomst is dat persoonsgegevens mogen worden gebruikt voor andere doeleinden dan waarvoor ze oorspronkelijk waren bedoeld.

3. De huidige regels, zoals met name neergelegd in de Wet bescherming persoonsgegevens, bieden in het algemeen voldoende ruimte voor verstrekking van persoonsgegevens aan instanties belast met criminaliteitsbestrijding.

4. De voorgestelde strafvorderlijke bevoegdheden tot gegevensvordering gaan te ver en zijn niet noodzakelijk in een democratische samenleving, althans is deze noodzaak niet aangetoond.

Verslag

Hierna volgt een verkorte weergave van de discussies naar aanleiding van de presentaties van de beide preadviseurs. Dit verslag is opgesteld door Mathijs Raijmakers, werkzaam bij het ministerie van BZK. De discussie werd geleid door Lex Michiels, voorzitter van de VAR. Het eerste preadvies dat werd besproken is dat van Nynke Schröder, het tweede van Thijs van Grinsven.

Bespreking van het preadvies van Nynke Schröder, Veiligheid en privacy in de openbare ruimte

Stefanie Kelterman (Universiteit Leiden): Het opslaan en bewaren van gegevens door middel van cameratoezicht maakt misschien wel een ontoelaatbare inbreuk op de privacy, maar het kan in bepaalde risicogebieden wel noodzakelijk zijn. Bijvoorbeeld bij bepaalde voetbalwedstrijden. Zou er voor dergelijke gebieden misschien een apart wetsvoorstel gemaakt moeten worden?

Nynke Schröder: In het huidige wetsvoorstel is cameratoezicht alleen toegestaan voor openbareordedoeleinden. Daarvoor is het opslaan en bewaren van gegevens echter niet noodzakelijk. Als je gegevens wilt bewaren voor opsporingsdoeleinden, is daarvoor een aparte wettelijke grondslag inderdaad noodzakelijk.

Edzard Lisser (gemeente Amsterdam): Er zijn vraagtekens te plaatsen bij de maatschappelijke noodzaak van cameratoezicht en preventief fouilleren. Het rendement van de maatregelen is beperkt. Voor wat betreft de horecacontroles is het wel begrijpelijk dat gekozen is voor niet-selectieve, algemene controles. De eis dat geen onderscheid mag worden gemaakt tussen bepaalde groepen is logisch. De inbreuk op de persoonlijke levenssfeer bij dergelijke controles is bovendien beperkt.

Nynke Schröder: De horecacontroles zijn ook om andere redenen problematisch. Het is de vraag of het hier echt om openbare ruimtes gaat. Bovendien vind ik het wél een vergaande inbreuk op de privacy. In een besloten gelegenheid zoals in de horeca heb je misschien nog wel een verdergaand recht op privacy dan op straat.

Andrea Keessen (Universiteit Utrecht): Voor wat betreft het preventief fouilleren: soms weet je toch dat de mogelijkheid van preventief fouilleren bestaat? Dan is dat toch niet zo'n probleem? En wat betreft de identificatieplicht: waarom wordt dat als zo'n grote inbreuk gezien? Wat is precies het probleem dat je desgevraagd je identiteitsbewijs moet laten zien?

Nynke Schröder: Op dit moment is het nog zo dat voor het vragen van het identiteitsbewijs een redelijke aanleiding moet zijn. In de toekomst is dat niet meer zo. Je hebt dan geen zicht meer op wat er met de informatie gebeurt die je verschaft. Het risico bestaat altijd dat deze in je nadeel gebruikt zal worden.

Cees Bangma (Ministerie van Justitie): Algemene identificatieplicht is eigenlijk een onjuiste term, die de discussie vervuilt. In het wetsvoorstel is die term nu juist bewust vermeden. Het gaat om een *uitgebreide* identificatieplicht. De wet bevat bijvoorbeeld nog steeds een koppeling naar de redelijke aanleiding. Ik ben het dan ook niet met stelling 2 eens. De wet heeft een beperkte strekking. De uitbreiding van de bevoegdheid ziet op handhaving van de openbare orde, op buitengewoon opsporingsambtenaren en op de leeftijd van degenen van wie legitimatie gevraagd kan worden. Bezwaren tegen die leeftijd kan ik nog volgen, andere bezwaren niet.

Nynke Schröder: De term algemene identificatieplicht wordt in publicaties zeer veel gebruikt. Voor het gemak gebruik ik hem nu ook. In het preadvies heb ik dat wel genuanceerd.
De uitbreiding van de bevoegdheid ziet inderdaad op openbare orde en overlastbestrijding. Ik ben van mening dat je dwangmiddelen, zoals dit is, alleen moet toepassen als er sprake is van een verdachte. Anders is een specifieke wettelijke grondslag vereist. Het risico bestaat dat er te snel naar dergelijke dwangmiddelen gegrepen wordt. Identiteitscontroles hoeven nergens geregistreerd te worden. Daardoor is niet zeker dat er niet méér gebruik van wordt gemaakt dan is toegestaan.

Lex Michiels (voorzitter): Bevoegdheden kunnen altijd verkeerd gebruikt worden. Dat is op zichzelf toch geen bezwaar tegen het toekennen van een bevoegdheid?

Nynke Schröder: Maar in deze wettelijke regeling is geen controle mogelijk op onterecht gebruik van de bevoegdheid. Dan is het wel een bezwaar.

Tom Barkhuysen (Universiteit Leiden): Het idee achter grondrechtelijke bescherming is nu juist dat de overheid misbruik kan maken van zijn bevoegdheden. Daartegen moeten in de wet waarborgen worden opgenomen. Maar dan moet je wel duidelijk maken waarom die waarborgen zo belangrijk zouden zijn. Je moet een goed verhaal hebben om die grondrechten te verdedigen.

Nico Verheij (Ministerie van Justitie): Het Europees Hof voor de Rechten van de Mens in Straatsburg heeft bepaald dat het ontbreken van een grens aan een bevoegdheid een inbreuk op de privacy kan betekenen. Dat onderstreept dat procedurele waarborgen dus wel degelijk van belang zijn.

Lex Michiels: Welke waarborgen zouden in het geval van de identificatieplicht dan toegevoegd moeten worden?

Nynke Schröder: Alle controles zouden geregistreerd moeten worden, hoewel ook dat belastend kan zijn voor de privacy. Ook moet het begrip 'redelijkerwijs noodzakelijk voor de uitoefening van de bevoegdheid' aangescherpt worden.

Jannetje Bootsma (Pels Rijcken): Met betrekking tot cameratoezicht: heeft de regering niet ook een verplichting tot het garanderen van veiligheid en een goed leefmilieu, wat op gespannen voet kan staan met de verplichting tot waarborgen van de privacy?

Nynke Schröder: Je kunt ook zeggen dat privacybescherming juist van belang is om veiligheid en een goed leefmilieu te garanderen. Je moet veilig zijn tegen inbreuken op die privacy door de overheid. Ik ben ook niet tegen cameratoezicht op zich, maar het moet wel onder bepaalde voorwaarden gebeuren.

Lex Michiels: Mensen in een gevaarlijke buurt geven vaak graag hun privacy op in ruil voor veiligheid.

Nynke Schröder: Maar niet voor altijd. Alleen zolang het nodig is om de situatie te verbeteren. Een aanwijzing van een gebied voor cameratoezicht voor een beperkte tijd kan zeker noodzakelijk zijn. Onder omstandigheden kan dat ook best een jaar zijn.

Femke Vrolijk (Universiteit Leiden): Wat betreft het idee van registratie van de identiteitscontroles. Een dergelijke registratie kan ook in het belang van de burger zijn. Die krijgt dan een briefje mee naar huis: 'Ik ben gecontroleerd'. Anders is dat moeilijk te bewijzen als daar later onenigheid over ontstaat.

Nynke Schröder: Het zou inderdaad een extra waarborg zijn.

Stelling 1 wordt besproken.

Nynke Schröder licht toe dat het opslaan en bewaren van met behulp van cameratoezicht gemaakte beelden nuttig kan zijn, maar dan vooral in het belang van de opsporing van strafbare feiten en niet voor de handhaving van de openbare orde.

Tom Barkhuysen: Als dat zo is, moet dan niet alleen het doel van de wettelijke regeling aangepast worden? Het kan toch wel degelijk van belang zijn sommige banden nog eens terug te kunnen spoelen. Is het bovendien niet mogelijk in een eventuele zaak voor het Straatsburgse Hof extra doelen aan te voeren? Daar is jurisprudentie over.

Nynke Schröder: Het wijzigen van het doel van de wettelijke regeling is dan toch echt noodzakelijk. Als doelen later nog aangevuld worden, is voor de burger onvoldoende voorzienbaar geweest dat de beelden ook voor dat aanvullende doel zijn gebruikt.

Nico Verheij: De openbare orde wordt toch vaak verstoord door het plegen van een strafbaar feit. Zou het opsporen van strafbare feiten dan niet gewoon meegenomen moeten worden in dit wetsvoorstel?

Nynke Schröder: Het wetsvoorstel over cameratoezicht zou op dit punt inderdaad aangepast moeten worden als men het stelselmatig opslaan en bewaren van de gemaakte beelden mogelijk wil maken. Er moet een doel worden toegevoegd.

Lex Michiels: Als ik die beelden achteraf nu eens ga analyseren. Niet om strafbare feiten op te sporen, maar om patronen te ontdekken die voor de toekomstige handhaving van de openbare orde van belang kunnen zijn. Voor die analyse is opslag gedurende zekere tijd noodzakelijk. Dan handel ik toch binnen het doel van de huidige regeling?

Nynke Schröder: Nee, dat is niet noodzakelijk voor de handhaving van de openbare orde. In ieder geval niet het stelselmatig opslaan en bewaren van de beelden. Dat kan alleen voor een bijzonder doel en voor een beperkte periode.

Michiel van Emmerik (Ministerie van BZK): De stelling gaat nu over opslaan en bewaren van beelden in het algemeen. Ik zou me wel voor kunnen stellen dat beelden voor een kortere periode bewaard worden.

Nynke Schröder: Incidenteel gebruik van beelden moet kunnen, maar niet permanent. Je mag ook onder de huidige regeling de beelden maar een week opslaan, tenzij er strafbare feiten op geconstateerd zijn. Het gaat mij ook niet zozeer om de duur van het opslaan, als wel om de stelselmatigheid ervan.

Wouter Peters (Ministerie van LNV): Het is ook niet noodzakelijk om de beelden te bewaren. Het is mogelijk om direct mee te kijken als de beelden gemaakt worden.

Tom Barkhuysen: Uit onderzoek blijkt dat direct meekijken niet altijd even goed mogelijk is.

Lex Michiels: Bovendien is analyse van de beelden achteraf efficiënter, want dat kost minder tijd. Oninteressante stukken kunnen doorgespoeld worden. Dat is dus praktischer en goedkoper.

Marte van der Loop (Ministerie van BZK): Als er dus wel een grondslag is voor het gebruik van die beelden voor strafvervolging, dan moet je ze toch ook wel mogen opslaan en bewaren, anders kan je ze ook niet meer gebruiken?

Nynke Schröder: Maar dan moet je die doelstelling voor het opslaan en bewaren ook opnemen in de wet. Dat is nu niet het geval.

Marte van der Loop: Dat is dan dus slechts een kwestie van wetgevingstechniek.

Er wordt gestemd over stelling 1, die na nuancering door de preadviseur als volgt luidt:

> Het stelselmatig opslaan en bewaren van met behulp van cameratoezicht in de openbare ruimte gemaakte beelden vormt een onrechtmatige beperking van het recht op privacy omdat deze beperking niet noodzakelijk is in het belang van het doel van dit cameratoezicht, handhaving van de openbare orde.

De stelling wordt met een zeer kleine meerderheid verworpen.

Stelling 2 wordt besproken.

Viola Reimert (Rijksuniversiteit Groningen): Moet er geen onderscheid gemaakt worden tussen de handhaving van de openbare orde en het beleid ten aanzien van de openbare orde?

Lex Michiels: Volgens mij valt dat allemaal onder de kwalificatie handhaving van de openbare orde.

Er wordt gestemd over de tweede stelling.

> Een uitgebreide identificatieplicht vormt een onrechtmatige beperking van het recht op privacy omdat het beoogde doel, verbetering van de rechtshandhaving en bestrijding van de criminaliteit, op een minder ingrijpende wijze gerealiseerd kan worden door intensiever gebruik te maken van de huidige beperkte identificatieplichten.

Een kleine meerderheid is het met de stelling eens.

Stelling 3 over preventief fouilleren wordt besproken.

Edzard Lisser: Dat preventief fouilleren over een lange periode mogelijk is en dat het in een groot gebied mogelijk is, is op zichzelf niet zo'n probleem. Het gaat met name om de motivering voor die maatregel.

Nynke Schröder: Daar ben ik het in beginsel mee eens. Maar aanwijzing van een gebied voor een langere periode is kwetsbaar. De noodzaak voor de maatregel kan bijvoorbeeld in de tussentijd gewijzigd zijn. Dat zou dan steeds opnieuw gemotiveerd moeten worden.

Nico Verheij: We moeten wel realistisch blijven. Soms weet je toch gewoon van tevoren dat een gebied een lange tijd onveilig zal blijven?

Henk Griffioen (Universiteit Leiden): Waarom zou het aanwijzen zelf ontoelaatbaar zijn? Voor het preventief fouilleren zelf moet toch een concrete beslissing genomen worden. De aanwijzing van een gebied is toch nog niet zo'n probleem. Ook na die aanwijzing zijn er nog waarborgen voor er eenmaal een beslissing tot preventief fouilleren is genomen.

Nynke Schröder: Maar die beslissing wordt wel op precies dezelfde gronden genomen en ook op exact dezelfde wijze gemotiveerd. In de praktijk betekent dat dus geen extra hindernis en dus geen extra waarborg.

Michiel de Vries (Erasmus Universiteit): De verschillende beslissingen worden wel door verschillende organen genomen. Het gebied wordt niet aangewezen door degene die de concrete actie tot fouilleren onderneemt.

Sandra Verhagen (Pels Rijcken): Moet er niet altijd een proportionaliteitstoets per concreet geval opgenomen worden en bevat de huidige regeling die niet?

Stelling 3 wordt in stemming gebracht. Na de discussie wordt de stelling als volgt geherformuleerd:

> De huidige wettelijke regeling voor preventief fouilleren vormt op drie punten een ontoelaatbare inbreuk van het recht op privacy:
> a. Gebieden worden voor onevenredig lange periodes aangewezen als veiligheidsrisicogebied. *[een grote meerderheid is het hiermee oneens]*
> b. Onevenredig grote gebieden worden als veiligheidsriscogebied aangewezen. *[een grote meerderheid is het hiermee oneens]*
> c. Er wordt gebruikgemaakt van onevenredig ingrijpende methoden als lokaliteiten- en horecacontroles. *[een meerderheid is het hiermee oneens]*

Bespreking van het preadvies van Thijs van Grinsven, Grenzen aan gegevensverstrekking

Dennis van Berkel (Universiteit Leiden): Ik ben het ermee eens dat de nieuwe bevoegdheden te breed zijn. Er zijn echter ook oplossingen. Het CBP heeft gesteld dat het vastleggen van de bevoegdheid van politie en justitie tot het opvragen van gegevens belangrijk is. De beslissing over de verstrekking van de gegevens ligt nu bij de houder van de gegevens (meestal een privaatrechtelijk orgaan) en niet bij een publiekrechtelijk orgaan. Nu wordt de afweging over verstrekking verwacht van de houder terwijl die vaak te weinig informatie heeft voor een volwaardige afweging van de verschillende belangen. Deze situatie leidt tot onzekerheden voor alle partijen. Die zouden voorkomen kunnen worden door een aparte wettelijke grondslag in het Wetboek van Strafvordering.

Thijs van Grinsven: De betrokkene is inderdaad afhankelijk van de opstelling van de houder. In de nieuwe regeling is er wel zekerheid, maar het is ook een verslechtering: de gegevens worden namelijk altijd verstrekt. Het is goed mogelijk om een vorm van bevoegdheid van gegevensverkrijging te creëren. Die bevoegdheid moet dan wel minder algemeen zijn en goed of in ieder geval beter dan nu gemotiveerd worden. En waarom zou je een dwangmiddel creëren als vrijwilligheid ook mogelijk is?

Dennis van Berkel: Dat lost het probleem van de houder niet op. Die weet nog steeds niet voldoende om een goede afweging te maken. Dat geldt ook voor de betrokkene. Het biedt ook meer rechtszekerheid.

Lex Michiels (voorzitter): Het gaat dus ook om de zuiverheid. Waar moet de uiteindelijke beslissing voor verstrekking liggen? Bij de overheid?

Thijs van Grinsven: De overheid heeft wel de meeste kennis. Het heeft echter ook nadelen om de verantwoordelijkheid bij de overheid te leggen.

J. Brouwer (Universiteit Leiden): Bedrijven hebben ook nu al een zorgplicht. Onder de wet MOT (melding ongebruikelijke transacties) moeten ze bepaalde zaken melden, anders zijn ze zelfs strafbaar. Dat doet al af aan de vrijwilligheid.

Thijs van Grinsven: In dat geval betreft het een afgebakende bijzondere informatieverplichting. Dat is iets anders dan de algemene informatieplicht uit het voorliggende wetsvoorstel.

Laurens Buist (Universiteit Leiden): Kun je eigenlijk wel spreken van een algemene informatieplicht? Het geldt bijvoorbeeld niet voor alle strafbare feiten.

Thijs van Grinsven: Het is toch bijna een algemene informatieplicht. Er wordt wel onderscheid gemaakt naar wie de informatie kan vorderen en welke procedurele waarborgen daarbij gelden. Echte beperkingen zijn er echter alleen ten aanzien van gevoelige gegevens, bijvoorbeeld over ras, godsdienst, enzovoort. Voor wat betreft andere gegevens geldt een ruimer regime.

Tom Barkhuysen (Universiteit Leiden): Ik vind het sympathieke voorstellen voor duidelijke grenzen, maar is er dan niet ook een duidelijke sanctionering voor overschrijding van die grenzen noodzakelijk?

Thijs van Grinsven: Dat zou ik er wellicht alsnog bij kunnen betrekken. Een effectieve sanctionering richting overheid ontbreekt nu nog. Een duidelijkere regeling van bewijsuitsluiting is inderdaad nodig.

Stelling 1 wordt besproken.

> Het beginsel van doelbinding, met als sluitstuk de voorwaarde van verenigbaar gebruik, is het meest fundamentele beginsel van persoonsgegevensbescherming en inbreuken daarop dienen ook in het kader van criminaliteitsbestrijding uitzondering te blijven.

Dennis van Berkel: Hoe moet Justitie dan aan haar informatie komen?

Thijs van Grinsven: Justitie heeft eigen bevoegdheden om zelf aan relevante gegevens te komen. Een algemene verruiming op dit punt is niet nodig. De toon van het debat

is nu 'alles moet beschikbaar zijn', maar het belang van de criminaliteitsbestrijding is niet zo fundamenteel anders dan andere belangen dat die daarvoor zouden moeten wijken.

Dennis van Berkel: Maar private instanties hebben nooit als doel de criminaliteitsbestrijding. Dan kan je dus nooit wat met de door hen verzamelde gegevens.

Thijs van Grinsven: Vaste partners van de politie, zoals banken en verzekeraars, zouden best kunnen melden 'deze gegevens kunnen ook gebruikt worden voor de bestrijding van fraude' enzovoort.

Lex Michiels: Kun je niet wettelijk regelen dat deze instanties, maar bijvoorbeeld ook internetproviders, worden geacht die gegevens mede te verzamelen ter bestrijding van criminaliteit?

Nico Verheij (Ministerie van Justitie): Wat heb ik er nou aan als mijn bank dat in de kleine lettertjes opneemt? Dat levert toch geen groter gevoel van privacy op? Er moet nu al heel veel informatie verstrekt worden. Met het overgrote deel daarvan gebeurt niets. Dat werpt de vraag van evenredigheid op.

Thijs van Grinsven: Maar dan staat het in ieder geval nog in de kleine lettertjes. Dan kun je als klant in ieder geval weten waar je gegevens ook voor gebruikt kunnen worden.

Bruno Bosnjakowicz: Dan kunnen banken daarop eventueel ook gaan concurreren: 'bij ons worden uw gegevens niet doorgegeven'.

Thijs van Grinsven: Dat zie ik niet zo snel gebeuren. Maar nogmaals, het voordeel is dat je van tevoren duidelijkheid hebt over wat je bank gaat doen.

Andrea Keessen (Universiteit Utrecht): Er zijn ook voorbeelden te geven uit andere tijden. Voor sommige ouderen kan het heel bezwaarlijk zijn als instanties alles van ze kunnen weten. Dat heeft met hun ervaringen uit de oorlog te maken. Zo bezien is het niet zo verkeerd om principieel te zijn op dit punt.

Er wordt gestemd over de stelling. Een meerderheid is het met de stelling eens.

Stelling 2:

> Andere waarborgen op het gebied van gegevensbescherming, zoals transparantie en rechtsbescherming kunnen een inbreuk op het beginsel van doelbinding niet compenseren. Zij komen als mosterd na de maaltijd, indien de uitkomst is dat persoonsgegevens mogen worden gebruikt voor andere doeleinden dan waarvoor ze oorspronkelijk waren bedoeld.

Tom Barkhuysen: Je ziet op dit punt een groot verschil tussen Europa en de VS. In de VS zijn er weinig waarborgen vooraf en is er veel rechtsbescherming achteraf. In Europa bestaat de traditie om vooraf vast te leggen wanneer gegevens verstrekt mogen worden. Daar komt de rechtsbescherming dan nog bij.

De meerderheid van de aanwezigen is het met de stelling niet eens.

Stelling 3 wordt besproken.

> De huidige regels, zoals met name neergelegd in de Wet bescherming persoonsgegevens, bieden in het algemeen voldoende ruimte voor verstrekking van persoonsgegevens aan instanties belast met criminaliteitsbestrijding.

Lex Michiels: Moet daaraan toegevoegd worden dat vrijwilligheid daarbij van groot belang is?

Thijs van Grinsven: Dat is zo, maar in de praktijk wordt gegevensverstrekking bijna nooit geweigerd.

Laurens Buist: Vallen de regels die uitzonderingen maken op de Wbp, bijvoorbeeld over telecommunicatie, ook binnen de stelling?

Thijs van Grinsven: Nee, daar doelde ik niet op. Maar ik vraag me wel af of je die uitzonderingen nu echt nodig hebt. Ook dat durf ik te betwisten.

Sandra Verhagen (Pels Rijcken): Ik wil nog even terugkomen op het alternatief van de vrijwillige medewerking. Als je als private instelling zelf het doel oprekt waarvoor je gegevens verzamelt tot buiten de gewone taken die je verricht, zou dat dan wel mogen vanuit de optiek van de wetgever?

Thijs van Grinsven: In het algemeen niet. Maar bij bijvoorbeeld een bank die het voorkomen van fraude als doel opneemt, dat is wel mogelijk.

De stemmen staken over stelling 3.

Stelling 4 wordt in stemming gebracht.

> De voorgestelde strafvorderlijke bevoegdheden tot gegevensvordering gaan te ver en zijn niet noodzakelijk in een democratische samenleving, althans is deze noodzaak niet aangetoond.

Een grote meerderheid is het met deze stelling eens.