Van meld- naar aantoonplicht

Van meld- naar aantoonplicht

Een onderzoek naar een systeem van digitale surveillance

C.Veen
J.G. Brouwer

POLITIE & Wetenschap

rijksuniversiteit groningen

In opdracht van:
Programma Politie & Wetenschap

Foto omslag: George Verberne/Hollandse Hoogte

Ontwerp:
Vantilt Producties & Martien Frijns

ISBN: 978 90 3524 678 2
NUR: 800, 624

Realisatie:
Reed Business, Amsterdam

Inhoud

1

Inleiding en onderzoeksopzet

1.1 Inleiding

Sinds 1 september 2010 beschikt de burgemeester op grond van artikel 172a Gemeentewet (Gemw) over de bevoegdheid om een of meer gedragsaanwijzingen te geven aan personen die herhaaldelijk de openbare orde verstoren. Op die datum trad namelijk de Wet maatregelen bestrijding voetbalvandalisme en ernstige overlast (Wet mbveo) in werking. Wat zijn de gedragsaanwijzingen die de burgemeester kan geven?

Ten eerste kan de burgemeester een verbod opleggen om zich in een of meer bepaalde delen van of objecten binnen de gemeente te bevinden. Een object kan bijvoorbeeld een stadion zijn. Een stadionverbod, al dan niet gecombineerd met een gebiedsverbod in de omgeving van het stadion, houdt voor de verstoorder het verbod in om zich, al dan niet gedurende de vastgestelde tijdstippen, in het stadion en/of de omgeving ervan te bevinden.[1]

Ten tweede bevat de Wet mbveo voor de burgemeester de bevoegdheid om een groepsverbod op te leggen. Bij een dergelijk verbod is het de verstoorder verboden om zich in een of meer bepaalde delen van de gemeente op een voor het publiek toegankelijke plaats zonder redelijk doel met meer dan drie andere personen in groepsverband op te houden.[2]

Ten derde biedt de wet de burgemeester de mogelijkheid tot het opleggen van een meldingsplicht. In dat geval is de verstoorder verplicht om zich op vastgestelde tijdstippen op een door de burgemeester voorgeschreven plaats, al dan niet in een andere gemeente, te melden.[3] Dit onderzoek heeft betrekking op de ontwikkeling van een alternatief voor de meldingsplicht.

1 Kamerstukken II 2007/08, 31 467, nr. 3, p. 12 en artikel 172a lid 1 onder a Gemw.

2 Kamerstukken II 2007/08, 31 467, nr. 3, p. 13 en artikel 172a lid 1 onder b Gemw.

3 Artikel 172a onder c Gemw.

1.2 Onderzoeksvraag

Aanleiding voor dit onderzoek zijn de signalen uit de praktijk dat de naleving van stadionverboden allesbehalve goed verloopt. De ervaring leert dat het voor personen met een stadionverbod vrij eenvoudig is om de voor hen verboden grond te betreden. Of het nu om een bestuursrechtelijk, strafrechtelijk of een civielrechtelijk stadionverbod van een Betaald Voetbal Organisatie (bvo) dan wel de KNVB gaat, verbannen supporters bezoeken voetbalwedstrijden alsof er geen sanctie is opgelegd. De huidige regeling van de meldingsplicht verandert daar weinig aan. Langzamerhand wordt duidelijk dat die alleen soelaas biedt bij uitwedstrijden van de club van de supporter. In dat geval mag hij echter niet worden opgelegd.

Het is derhalve zaak om op zoek te gaan naar werkbare alternatieven. Kunnen we een alternatief bedenken dat een sluitende oplossing voor dit probleem biedt? Vanzelfsprekend is het mogelijk om de regeling van de meldingsplicht te wijzigen, zodanig dat de naleving van de stadionverboden waterdicht wordt. In de regeling zou dan de mogelijkheid moeten worden opgenomen om verbannen supporters te verplichten om zich vaker dan één keer tijdens een thuiswedstrijd op het politiebureau te melden. Ook zou de optie moeten worden geboden om een verbannen supporter te verplichten zich bij uitwedstrijden van zijn club te melden op het politiebureau van zijn thuishaven. Dat belet hem immers om met zijn club mee te reizen.

Het zijn allebei opties die de moeite van het overdenken waard zijn. Er is echter een bezwaar: ze kosten de politieorganisatie handenvol werk! De vraag die in dit onderzoek derhalve centraal staat, is of er geen minder arbeidsintensieve alternatieven inzetbaar zijn om de naleving van stadionverboden en niet te vergeten de stadionomgevingsverboden waterdicht te maken. Kunnen we met behulp van technologie een instrument ontwikkelen dat enerzijds de naleving van de stadionverboden waterdicht maakt en anderzijds de politieorganisatie niet te veel capaciteit kost?

Wij denken hierbij aan een geautomatiseerd systeem van digitale surveillance, met behulp waarvan de politie nauwkeuriger kan controleren of de verbannen supporter zich niet in het verboden gebied bevindt. De mobiele telefoon neemt in dit systeem een belangrijke positie in. Juridisch is het verstandig om de verantwoordelijkheid voor de controle op het zich niet bevinden in het verboden gebied bij de verbannen supporter te leggen. We spreken daarom van een digitale aantoonplicht.

Hoe zou deze verplichting het beste kunnen worden ingericht, hierbij ook

rekening houdend met het juridische kader? Is het denkbaar een dergelijke digitale aantoonplicht in te voeren zonder een tijdrovende wetswijziging? Of kan de wijziging van de regelgeving zich beperken tot een aanpassing van de verordeningen die de bvo-steden toch al hebben. Het voordeel daarvan is dat een wijziging zich sneller laat realiseren.

1.3 Doelstelling

Doel van het onderzoek is de ontwikkeling van een systeem dat het de politie mogelijk maakt om op afstand te controleren of de verbannen voetbalsupporter zich niet in het verboden gebied bevindt. Beoogd wordt om duidelijk en begrijpelijk de meerwaarde van een dergelijk systeem voor de dagelijkse (politie)praktijk uiteen te zetten.

Het onderzoek heeft tevens de strekking te kijken in hoeverre het nuttig is om, ten aanzien van de digitale aantoonplicht, een pilot te draaien. Indien een pilot positieve resultaten laat zien, kan vervolgonderzoek plaatsvinden naar de vraag in hoeverre een digitale aantoonplicht ook ten aanzien van ander overlastgevend gedrag kan worden ingezet.

1.4 Terminologie en methodologie

Het onderzoek richt zich op voetbalgerelateerde verstoringen van de openbare orde. Hieronder dient te worden verstaan: alle individuele of groepsgewijze gedragingen van 'voetbalsupporters' in of rondom voetbalstadions dan wel elders, die een verstoring van de openbare orde opleveren. Van een verstoring van de openbare orde is sprake, indien een persoon onrechtmatige hinder of onrechtmatig gevaar voor andere personen en/of goederen veroorzaakt. Met het begrip 'aantoonplichtige' wordt de persoon bedoeld aan wie de burgemeester een verblijfsverbod oplegt in combinatie met de plicht om aan te tonen dat hij zich op de verboden tijdstippen niet in het verboden gebied bevindt.

Het onderzoek focust zich op de bevoegdheden die op gemeentelijk niveau bestaan om verstoringen van de openbare orde tegen te gaan en de botsingen die de inzet van die bevoegdheden met het privacyrecht en de bewegingsvrijheid van de voetbalsupporter veroorzaakt.

In dit onderzoek neemt de mobiele telefoon een strategische positie in. Dat

is een keuze die we vooralsnog hebben gemaakt, maar vanzelfsprekend zijn er ook andere opties. In Engeland hanteert men bijvoorbeeld bij de toelating van horeca-inrichtingen het systeem Touch2id om aan te tonen dat een betrokkene 18 jaar of ouder is.[4] Dat systeem zou misschien ook goed ingezet kunnen worden voor de controle van stadionverboden. Het is een variant op de meldingsplicht. Het maakt gebruik van niet tot een natuurlijke persoon herleidbare referentiepunten van de wijsvinger. De betrokkene dient eenmalig een geldig identiteitsbewijs te overleggen, waarna de specifieke referentiepunten van de wijsvinger worden ingescand en opgeslagen op een pas met een chip met *Radio Frequency Identification* (RFID).[5] Bij deze technologie wordt gebruikgemaakt van radiogolven om iemand te identificeren. Onze verbannen supporter zou op de dag van de voetbalwedstrijd moeten 'inchecken' bij een speciaal hiervoor ontworpen 'paal', zodat vastgesteld kan worden dat hij zich niet in het verboden gebied bevindt.

Een dergelijke digitale check neemt de politie veel werk uit handen, maar is bij thuiswedstrijden allesbehalve waterdicht. Na de check kan de supporter zich alsnog naar het stadion begeven of hij zou moeten worden verplicht om meerdere keren 'in te checken'. Maar dat is wel weer een grote belasting en daarmee een forse beperking van zijn privacy. Bovendien dienen er in verband met de bewegingsvrijheid van de betrokkene een behoorlijk aantal 'palen' over het land verspreid te worden geplaatst. Aan het mogelijke gebruik van RFID besteden wij in het onderzoek om deze redenen verder geen aandacht meer.

Aan de hand van een literatuuronderzoek en analyse van de wetgeving en de rechtspraak worden de problemen met de stadion- en gebiedsverboden, waaronder de huidige meldingsplicht, geïnventariseerd, afgebakend en beschreven. Vanzelfsprekend richten wij ons in dit onderzoek op de vraag of het mogelijk is om een digitale aantoonplicht in te voeren en, zo ja hoe, die aantoonplicht eruit moet zien. Hierbij besteden we vooral aandacht aan de technische, privacygerelateerde en politionele aspecten.

Bij dit onderzoek hebben wij zowel binnen als buiten de politie verschillende experts en ervaringsdeskundigen op het gebied van ICT en privacy betrok-

4 Zie Touch2id in werking op: http://www.touch2id.co.uk/.

5 Het is ook mogelijk om alle tien de vingers in te scannen, zodat bij controle om een willekeurige vinger gevraagd kan worden. Dit maakt frauderen vermoedelijk een stuk lastiger. Belangrijk is dat de vingerafdruk zelf niet op de RFID-chip staat, dit in tegenstelling tot bij het voorgestelde biometrische paspoort.

6 In Bijlage 1 is een overzicht van de bij het onderzoek betrokken personen opgenomen.

ken.[6] In gesprekken met deze experts en ervaringsdeskundigen is meer inzicht verkregen in de wijze waarop de digitale aantoonplicht zou kunnen worden ingericht, hierbij rekening houdend met enerzijds het privacyrecht van de supporter en anderzijds de werkbaarheid voor de politieorganisatie.

Tijdens dit onderzoek heeft de minister verklaard voornemens te zijn om de Wet mbveo te herzien en het bestaande instrumentarium aan te scherpen.[7] De resultaten van dit onderzoek kunnen als input worden gebruikt bij de voorbereiding van die wetswijziging.

1.5 Leeswijzer

Dit boek is opgedeeld in zeven hoofdstukken. Hoofdstuk twee behandelt de problemen die men in de praktijk met de huidige stadiongebiedsverboden ondervindt. De nadruk ligt daarbij op de complicaties die spelen rond het opleggen en uitvoeren van de meldingsplicht.

Hoofdstuk drie introduceert de digitale aantoonplicht als alternatief voor de meldingsplicht uit de Wet mbveo. Daarnaast wordt ingegaan op het opleggen van een (digitale) aantoonplicht in combinatie met een stadiongebiedsverbod. Tevens komt de inrichting van de aantoonplicht aan bod.

In hoofdstuk vier staat het recht op privacy en de digitale aantoonplicht centraal. Daarbij gaat het om de vraag of een digitale aantoonplicht op het niveau van een plaatselijke verordening überhaupt tot de mogelijkheden behoort. Hoe verhoudt de aantoonplicht zich tot het privacyrecht en kan deze plicht de privacytoets van artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens (EVRM) wel doorstaan?

Hoofdstuk vijf gaat nog wat verder in op het privacyrecht. Dit hoofdstuk concentreert zich op de verwerking van persoonsgegevens en behandelt de Wet bescherming persoonsgegevens (Wbp) en de Wet politiegegevens (Wpg). Bij de digitale aantoonplicht zullen persoonsgegevens worden verwerkt. Derhalve wordt er gekeken aan welke vereisten die gegevensverwerking moet voldoen om rechtmatig te zijn. Daarnaast gaan we in op de inhoudelijke vereisten van het besluit van de burgemeester en wordt er kort aandacht besteed aan het verstrekken van politiegegevens.

Hoofdstuk zes zet de meerwaarde van een digitale aantoonplicht voor de

7 Zie de brief van de minister van Veiligheid en Justitie van 4 september 2012 aan de Tweede Kamer.

dagelijkse politiepraktijk en een effectieve aanpak van voetbalvandalisme uiteen. In hoofdstuk zeven treft u vervolgens de conclusie en enkele aanbevelingen aan, waarbij tevens het antwoord op de hierboven geformuleerde vraag is weergegeven.

2

Problemen in de praktijk

2.1 Inleiding

De burgemeester is krachtens artikel 172a onder c Gemw bevoegd personen te bevelen om zich op bepaalde tijdstippen op een door hem voorgeschreven plaats te melden. Deze plaats kan in de eigen, maar ook in een andere gemeente gelegen zijn.

De regering had aanvankelijk een beperkte meldingsplicht op het oog. Deze zou altijd gekoppeld moeten worden aan een object- of gebiedsverbod.[8] Tijdens de parlementaire behandeling van het wetsvoorstel uitten Kamerleden de wens om de meldingsplicht ook als zelfstandige maatregel te kunnen opleggen. Door aanname van het amendement-De Wit is dit uiteindelijk gerealiseerd.[9]

Waarin de precieze meerwaarde van deze zelfstandige meldingsplicht schuilt, is niet duidelijk. Het gaat in beginsel toch om een maatregel waarmee de burgemeester geacht wordt de naleving van een object- en/of gebiedsverbod af te dwingen. Een zelfstandige meldingsplicht zou alleen zin hebben als de burgemeester die plicht zou kunnen opleggen bij uitwedstrijden, maar dat is hem nu juist niet toegestaan. Het is niet zijn taak, noch zijn bevoegdheid om de openbare orde te handhaven in een andere gemeente.

Voor toepassing van de bevoegdheid tot het opleggen van een meldingsplicht gelden twee eisen. Het is ten eerste vereist dat een persoon herhaaldelijk individueel of groepsgewijs de openbare orde heeft verstoord of bij groepsgewijze verstoring een leidende rol heeft gehad. Bij het vervullen van een leidinggevende rol dient het te gaan om actief handelen van de betrokkene.[10] Ten tweede moet er sprake zijn van ernstige vrees voor verdere verstoring van de openbare orde.[11]

---

8 De Memorie van Toelichting bij de Wet mbveo bevat bij het artikelsgewijze commentaar uitdrukkelijk de opvatting van het kabinet dat de meldingsplicht niet zelfstandig, evenmin in combinatie met een groepsverbod kan worden opgelegd. Kamerstukken II 2007/08, 31 467, nr. 3, p. 41.

9 Kamerstukken II 2008/09, 31 467, nr. 9 en Handelingen II 2008/09, nr. 62, p. 4966.

10 Kamerstukken II 2007/08, 31 467, nr. 3, p. 40.

11 Artikel 172a lid 1 onder c Gemw.

De Memorie van Toelichting bij de Wet mbveo merkt op dat de meldingsplicht als doel heeft de harde kern snel en doeltreffend aan te pakken, zodat de goedwillende voetballiefhebber buiten schot blijft.[12] Hoe de wetgever dit voor ogen staat, is niet geheel duidelijk. Volgens ons gaat het er bij de meldingsplicht om het een persoon onmogelijk te maken zich in een vastgesteld gebied of in de nabijheid van een object te bevinden. In combinatie met een verbod beoogt de plicht ervoor te zorgen dat de verbannen voetbalsupporter het verbod naleeft. In zoverre effectueert de meldingsplicht het object- en/of gebiedsverbod. In de praktijk blijkt zelfs deze wat minder ambitieuze doelstelling problemen op te leveren. Welke dat zijn, bespreken we in dit hoofdstuk.

2.2 Problemen meldingsplicht

De Inspectie Openbare Orde en Veiligheid (Inspectie OOV)[13] en het onderzoeksbureau Pro Facto hebben onderzoek verricht naar de toepassing van de Wet mbveo in de praktijk.[14] Beide onderzoeken laten zien dat er in de praktijk een aantal knelpunten wordt ervaren.[15] Die knelpunten hebben met name betrekking op de strenge toepassingsvoorwaarden, de besluitvorming en de effectiviteit van de meldingsplicht. Voor het in kaart brengen van de problemen zijn de evaluatierapporten van de Inspectie OOV en Pro Facto een belangrijke inspiratiebron geweest.

2.2.1 *Complicaties ten aanzien van de toepassingsvoorwaarden*

Uit de evaluatierapporten blijkt dat burgemeesters de voorwaarden voor het geven van een stadionverbod als streng ervaren.[16] De meldingsplicht dient op een voldoende feitelijke grondslag te berusten. Van de supporter moet een

12 Kamerstukken II 2007/08, 31 467, nr. 3, p. 4 en 5.

13 De Inspectie heeft inmiddels een nieuwe naam gekregen, te weten Inspectie Veiligheid en Justitie (Inspectie VenJ). Zie: http://www.ioov.nl/werkwijze-en.

14 Bij de behandeling van het wetsvoorstel is door de Eerste Kamer aangedrongen op een toezegging van de minister om toepassing van de wet te monitoren. Handelingen I 2009/10, nr. 34, p. 1462-1464 en p. 1485. De tweede evaluatie over de toepassing van de wet in de praktijk heeft vervroegd plaatsgevonden. Zie: Kamerstukken II 2010/11, 25 232, nr. 57.

15 Zie voor een overzicht van deze knelpunten onder meer Evaluatierapport Inspectie OOV 2011, p. 9 en 10.

gedocumenteerd dossier worden opgebouwd. Bij een voetbalgerelateerde verstoring bevat het dossier overwegend gegevens uit politiesystemen.

Het dossier moet onder meer inzicht geven in het gedrag van de supporter, respectievelijk de aard van de ordeverstoringen, het aantal keren dat hij de openbare orde individueel of groepsgewijs heeft verstoord, de vrees voor verdere herhaling van het ordeverstorende gedrag en de noodzaak van het geven van een stadionverbod.[17] Het dossier dient sluitend en van voldoende kwaliteit te zijn. In de praktijk is echter onduidelijk wanneer hiervan sprake is.[18] Bovendien blijkt het opbouwen van een goed dossier ingewikkeld en arbeidsintensief, waardoor een lik-op-stukbeleid wat betreft de aanpak van voetbalvandalisme lastig is.[19]

Uiteraard moet men uit het dossier kunnen afleiden dat de supporter de openbare orde herhaaldelijk heeft verstoord en dat er sprake is van ernstige vrees dat hij dit opnieuw zal doen. Beide onderzoeken maken duidelijk dat burgemeesters moeite hebben met het interpreteren van de bestanddelen 'verstoring van de openbare orde', 'herhaaldelijk' en 'ernstige vrees voor verdere verstoring van de openbare orde'.[20] Dit compliceert een sluitende dossier-opbouw.

'Verstoring van de openbare orde'

Over het wat vage en abstracte begrip 'openbare orde' kan worden gezegd dat de inhoud ervan niet altijd op voorhand even duidelijk is, ondanks het feit dat het begrip zowel in de jurisprudentie als in de literatuur de nodige aandacht heeft gekregen. Tot op zekere hoogte is dit begrijpelijk. De wijze waarop het wordt ingevuld, is mede afhankelijk van de opvattingen van het lokale bestuur. Het begrip 'openbare orde' is, met andere woorden, tijd- en plaatsgebonden.

16 Brouwer en Schilder hebben hier tijdens de parlementaire behandeling reeds op gewezen. Dit blijkt eveneens uit de schaars bestaande jurisprudentie met betrekking tot artikel 172a lid 1 Gemw. Zie bijvoorbeeld Rb. Amsterdam 18 februari, AB 2011/122, m. nt. J.G. Brouwer en A.E. Schilder.

17 Kamerstukken II 2007/08, 31 467, nr. 3, p. 15.

18 Evaluatierapport Inspectie OOV 2011, p. 44.

19 Evaluatierapport Pro Facto 2012, p. 2, 56 en 68. In de praktijk is men derhalve soms genoodzaakt om terug te vallen op reeds bestaande (alternatieve) bevoegdheden.

20 Zie: Evaluatierapport Inspectie OOV 2011, p. 45 en Evaluatierapport Pro Facto 2012, p. 50.

De wetgever heeft er bij de behandeling van het wetsvoorstel bewust van afgezien om aan te geven wat er onder het begrip 'verstoring van de openbare orde' moet worden verstaan.[21] Als gevolg hiervan dient het begrip in de jurisprudentie te worden uitgekristalliseerd. Of dat verstandig is, is zeer de vraag. De bevoegdheden in de Wet mbveo zijn immers gekoppeld aan dit begrip. Een verstoring van de openbare orde is een voorwaarde voor het opleggen van een maatregel als de meldingsplicht.

Vanwege het ontbreken van een definitie van het begrip 'openbare orde' zijn rechters soms onvoldoende op de hoogte waarom een bepaalde gedraging als een verstoring van de openbare orde moet worden gezien. De voorzieningenrechter van de Rechtbank Amsterdam bepaalde in 2011 dat de bevoegdheid om een stadionverbod te geven pas ontstaat, indien er sprake is van een overtreding. Wat de rechter daarmee bedoelt, is niet geheel duidelijk. Is hij van mening dat elke overtreding van een strafbepaling een verstoring van de openbare orde in de zin van artikel 172a Gemw oplevert?[22]

Er zijn meer onduidelijkheden in de wet. Bij een groepsgewijze verstoring van de openbare orde behoeft niet ieders individuele aandeel bij de verstoring vast te staan. De burgemeester hoeft bij een groepsgewijze verstoring derhalve niet aan te tonen dat iemand zélf de openbare orde heeft verstoord. Voldoende is dat hij vaststelt dat die persoon herhaaldelijk deel heeft uitgemaakt van een groep die de openbare orde voetbalgerelateerd heeft verstoord.

Betekent dit dat een globale omschrijving van supportersgedrag voldoende is om aan te tonen dat een persoon deel heeft uitgemaakt van een groep? Een uitspraak van de Rechtbank Amsterdam uit 2011 laat zien dat het iets genuanceerder ligt. 'De enkele aanwijzing in de rapportage dat *de verstoorder* tot de groep *ordeverstoorders* behoorde [is] onvoldoende om *zijn aanwezigheid tijdens een verstoring van de openbare orde* aannemelijk te maken', aldus de rechtbank.[23]

Een jaar later hanteert de Rechtbank Amsterdam bij de vraag wat iemands bijdrage moet zijn geweest aan een groepsgewijze verstoring wel een soepele opvatting. Volgens de rechtbank is voor het aannemen dat de verstoorder deel uitmaakte van de groep ordeverstoorders, de enkele aanwezigheid in die groep voldoende om betrokkenheid bij de overlast aan te tonen.[24] Hier wordt het

21 Zie: Handelingen I 2009/10, nr. 34, p. 1449.

22 Rb. Amsterdam 18 februari 2011, LJN BP5057, r.o. 4.3.

23 Rb. Amsterdam 18 februari 2011, LJN BP5057, r.o. 4.7 (cursivering door de auteurs).

24 Rb. Amsterdam 3 april 2012, AB 2012, 174, m. nt. J.G. Brouwer en A.E. Schilder, Rb. Amsterdam 3 april 2012, LJN BW1140, r.o. 8.1-9.1.

bekende adagium 'je was erbij, dus ben je erbij' onderschreven. Het betreft hier een heel ruime aansprakelijkheid.[25] Het op deze manier invullen van het begrip 'groepsgewijze verstoring' staat op gespannen voet met de totstandkomingsgeschiedenis van artikel 172a Gemw.[26]

'Herhaaldelijk'

Wanneer een verstoring van de openbare orde slechts één keer heeft plaatsgevonden, kan de bevoegdheid van artikel 172a Gemw nog geen toepassing vinden. Vereist is immers dat men de openbare orde herhaaldelijk heeft verstoord. De burgemeester kan daarom geen meldingsplicht opleggen als het een 'first offender' betreft. Dit ervaart men in de praktijk als een belangrijk knelpunt.[27]

Hoe vaak moet de openbare orde zijn verstoord, teneinde van een 'herhaling' te kunnen spreken? Artikel 172a Gemw zelf verschaft hierover geen duidelijkheid. In de Memorie van Toelichting bij de Wet mbveo staat één keer dat het begrip tot uitdrukking brengt, dat een persoon ten minste twee keer de openbare orde moet hebben verstoord.[28] Deze uitleg heeft echter betrekking op het groepsgewijs verstoren van de openbare orde.

In verband met een individuele verstoring van de openbare orde wordt gesproken van 'structurele verstoringen van de openbare orde', 'gedrag dat bij voortduring wordt herhaald', 'structurele', 'structureel patroon', 'persistente groepsgebonden overlast' enzovoort. In de Nadere Memorie van Antwoord aan de Senaat staat: met 'herhaaldelijk' wordt

> 'tot uitdrukking gebracht dat er een patroon moet zitten in de ordeverstoringen van een bepaald individu (of groep). In de toelichting wordt

25 In Engeland/Wales geldt steeds de eis dat een persoon een bijdrage moet hebben geleverd aan het verstoren van de openbare orde.

26 J.G. Brouwer en A.E. Schilder hierover onder Rb. Amsterdam 3 april 2012, AB 2012, 174: 'Deze ruime opvatting lijkt niet te sporen met de wetsgeschiedenis. Mede naar aanleiding van kritische opmerkingen van de Raad van State over het oorspronkelijke wetsvoorstel waarin personen "rechtstreeks in verband" moesten "kunnen worden gebracht" met de ordeverstoringen (Nader rapport, p. 9), lezen we op diverse plaatsen de eis dat een persoonlijk verwijt moet kunnen worden gemaakt. De MvT [Memorie van Toelichting] noemt twee soorten van bijdragen aan een ordeverstoring: daadwerkelijk de orde verstoren of een regierol vervullen (MvT, p, 40).'

27 Evaluatierapport Pro Facto 2012, p. 1, 54, 55 en 68.

28 Kamerstukken II 2007/08, 31 467, nr. 3, p. 40 en 41.

> in dit kader gesproken van structurele overlast. Incidentele overlast van een bepaalde persoon (of groep) is niet voldoende grond [...]. Het valt niet exact aan te geven hoe vaak de openbare orde moet zijn verstoord alvorens kan worden gesproken van het herhaaldelijk verstoren van de openbare orde.'[29]

De voorzieningenrechter van de Rechtbank Amsterdam is van mening dat er sprake is van een herhaaldelijke individuele of groepsgewijze verstoring van de openbare orde, indien er twee of meer ordeverstoringen hebben plaatsgevonden.[30] Derhalve wordt er vooralsnog van uitgegaan dat de burgemeester toepassing kan geven aan artikel 172a Gemw, indien een verstoorder twee keer of meer de openbare orde heeft verstoord.

Welke eisen worden er gesteld aan de aard van de gedragingen? Moet de verstoring van de openbare orde voetbalgerelateerd zijn? Artikel 172a Gemw, noch de parlementaire geschiedenis verschaffen hierover duidelijkheid. Ook in de rechtspraak is hierover (nog) niets beslist. Volgens ons is voor het geven van de stadionverbod niet vereist dat verstoringen voetbalgerelateerd zijn. De bepaling heeft immers betrekking op veel meer verstoringen dan alleen de specifieke verstoring van de openbare orde die samenhangt met voetbal. Naar onze mening mag een burgemeester derhalve bij een voetbalincident openbareordeverstoringen optellen die geen verband houden met een voetbalwedstrijd.

Een andere vraag is of het ordeverstorende gedrag in één gemeente dient plaats te vinden. Mag de burgemeester ordeverstorend gedrag buiten de gemeentelijke of zelfs buiten de landsgrenzen voor de eis van herhaaldelijkheid meenemen?[31] De wetgever heeft niet aan deze optelsom gedacht.[32] Dit zou wel bijdragen aan een snelle dossieropbouw, zodat de burgemeester een meldingsplicht kan opleggen.[33] Wat ons betreft, zijn er geen onoverkomelijke bezwaren. Een minimale eis is wel dat er naast de verstoring van de openbare orde elders,

---

29 Kamerstukken I 2009/10, 31 467, nr. E, p. 6.

30 Zie: Rb. Amsterdam 18 februari 2011, LJN BP5057, r.o. 4.4.

31 Rb. Amsterdam 18 februari 2011, LJN BP5057, r.o. 4.5.

32 Zie: overweging 7 van de noot van Brouwer en Schilder bij Rb. Amsterdam 18 februari 2011, AB 2011/122, m. nt. J.G. Brouwer en A.E. Schilder. Zie ook: Rb. Amsterdam 3 april 2012, LJN BW1140 en AB 2012,174 m. nt. J.G. Brouwer en A.E. Schilder.

33 De voorzieningenrechter van de Rechtbank Amsterdam merkt een groepsverbod in combinatie met een meldingsplicht aan als een van de zwaarst mogelijke maatregelen die de burgemeester op grond van artikel 172a Gemw kan treffen. Zie: Rb. Amsterdam 18 februari 2011, LJN BP5057, r.o. 4.8.

ook een verstoring van de openbare orde is in de gemeente waar de burgemeester de maatregel oplegt.

Nog weer een andere vraag is in hoeverre het de burgemeester is toegestaan om ordeverstoringen uit het verleden mee te nemen. In recente rechtspraak is aangenomen dat het rechtszekerheidsbeginsel niet in de weg staat om ordeverstoringen van vóór de inwerkingtreding van de Wet mbveo mee te nemen. Over de terugwerkende kracht is tijdens de parlementaire behandeling niets gezegd. Artikel 5:4 lid 2 van de Algemene wet bestuursrecht (Awb), waarin het legaliteitsbeginsel voor zowel bestraffende als herstelsancties is vastgelegd, is echter volstrekt helder: 'Een bestuurlijke sanctie wordt slechts opgelegd indien de overtreding en de sanctie bij of krachtens een aan de gedraging voorafgaand wettelijk voorschrift zijn omschreven.'[34]

Aangezien de Wet mbveo nog maar kort van kracht is, is het op dit moment lastig een gedegen en compleet dossier op te bouwen. De problemen met betrekking tot het aanleggen van het dossier doen zich met name voor vanwege de opbouw van een voetbalseizoen. De helft van het totaal aantal voetbalwedstrijden bestaat uit uitwedstrijden en er is sprake van een winter- en zomerstop. In de praktijk wordt terecht de vraag gesteld of je nog wel van hardnekkige structurele overlast kan spreken als er maanden tussen twee geregistreerde feiten zitten. Bovendien blijken voetbalsupporters opmerkelijk weinig registraties in politiesystemen te hebben.[35] Het vereiste van artikel 172a Gemw dat de openbare orde herhaaldelijk moet zijn verstoord, is derhalve voor de aanpak van voetbalgerelateerde verstoring van de openbare orde ongeschikt.

'Ernstige vrees voor verdere verstoring'

Een laatste voorwaarde voor toepassing van de bevoegdheid is dat de burgemeester ernstige vrees dient te hebben dat de verstoorder de openbare orde wederom zal verstoren. Hierbij geldt dat de vrees aanwijsbaar moet zijn. Volgens de Memorie van Toelichting bij de Wet mbveo betekent dit, dat de ernstige vrees moet blijken uit concrete aanwijzingen. Een ernstige ordeverstoring waarbij de verstoorder in het verleden betrokken is geweest, kan een concrete aanwijzing opleveren.[36]

34 Zie: Bröring 2005, p. 64.

35 Evaluatierapport Inspectie OOV 2011, p. 45 en 49.

36 Kamerstukken II 2007/08, 31 467, nr. 3, p. 6.

Om aan te tonen dat er sprake is van ernstige vrees voor verdere verstoring van de openbare orde maken burgemeesters gebruik van politiegegevens. Toch blijkt het in de praktijk moeilijk om die 'ernstige vrees' aan te tonen. Het is duidelijk geworden dat burgemeesters behoefte hebben aan een 'sfeerbeeld' met meer geïndividualiseerde en geconcretiseerde informatie, op basis waarvan kan worden aangetoond dat ernstige vrees voor herhaling gegrond is. Ten aanzien van voetbalgerelateerde overlast is het voor de politie echter lastig om informatie te individualiseren, aangezien dergelijke overlast veelal groepsgewijs wordt veroorzaakt.[37]

Uit de Memorie van Toelichting bij de Wet mbveo kan worden afgeleid, dat het de burgemeester is toegestaan om bij het construeren van ernstige vrees voor verdere verstoring van de openbare orde, ordeverstoringen uit het verleden mee te nemen. De wet, noch de parlementaire geschiedenis geven echter aan hoever de burgemeester terug mag gaan. Geldt in dit geval eveneens de eis dat hij een stadionverbod slechts mag baseren op ordeverstoringen die hebben plaatsgevonden na de inwerkingtreding van de wet? Of mag de burgemeester ordeverstoringen van voor 2010 meenemen? In het laatste geval kan hij makkelijker aantonen dat er 'ernstige vrees voor verdere verstoring van de openbare orde' bestaat.

Het stellen van een strenge eis gaat volgens ons bij de aanpak van voetbalgerelateerd geweld te ver. Voetbalsupporters hebben weinig registraties in politiesystemen, waardoor het stellen van een dergelijke eis ertoe kan leiden dat de burgemeester de ernstige vrees voor een verdere verstoring van de openbare orde niet, of althans onvoldoende kan bewijzen.[38] Dit terwijl de Wet mbveo juist beoogt voetbalvandalisme te bestrijden.

In een uitspraak van 3 april 2012 baseert de burgemeester zijn vrees op vier factoren zonder hierover in concreto iets te zeggen:

1 het patroon van overlastgevende incidenten;[39]
2 het karakter van de groep waarvan de eiser deel uitmaakt;
3 de aard van het groepsgedrag;
4 het gegeven dat tussenkomst door de politie de eiser er niet van heeft weerhouden opnieuw deel te nemen aan groepen die de openbare orde verstoren.[40]

37 Zie voor meer informatie Evaluatierapport Inspectie OOV 2011, p. 47 e.v.

38 Uiteraard levert een eis dat de burgemeester slechts ordeverstoringen van na de inwerkingtreding van de Wet mbveo mag meenemen, naarmate de tijd vordert minder problemen op.

39 Bedoeld zal zijn openbareordeverstorende incidenten; overlastgevende incidenten is een ruimere categorie.

40 Rb. Amsterdam 3 april 2012, AB 2012, 174, m. nt. J.G. Brouwer en A.E. Schilder.

Met deze vier factoren probeert de burgemeester de vrees voor verstoring van de openbare orde zo veel mogelijk te objectiveren. De rechtbank neemt ze letterlijk over in zijn overwegingen. Daar is op zich niets op tegen, mits ze maar geen eigen leven gaan leiden in volgende procedures. We zouden moeten voorkomen dat voor het criterium 'ernstige vrees voor verdere verstoring' de strenge eisen gaan gelden van het klaarblijkelijkheidscriterium in verband met de preventieve dwangsom. Het recidivecriterium lijkt in dit geval ruimschoots te volstaan.[41]

Brouwer en Schilder stellen zich op het standpunt dat het meenemen van orderverstoringen van vóór de inwerkingtreding van de wet, bij het construeren van ernstige vrees geen probleem oplevert.[42] Op het construeren van ernstige vrees is het strenge legaliteitsbeginsel niet van toepassing.

2.2.2 Knelpunten bij de besluitvorming

Het besluit van de burgemeester om krachtens artikel 172a lid 1 onder c Gemw een meldingsplicht op te leggen, is een besluit in de zin van artikel 1:3 Awb. Op het besluit van de burgemeester zijn derhalve de bepalingen uit de Awb van toepassing.

Zorgvuldigheids- en motiveringsgebreken

Artikel 3:2 van de Awb verplicht de burgemeester ertoe zijn besluit zorgvuldig voor te bereiden. Op grond van artikel 3:46 van de Awb dient het besluit van een deugdelijke, kenbare motivering te zijn voorzien. Volgens de parlementaire stukken houdt die eis in elk geval een vermelding in van de gedragingen waarmee de openbare orde is verstoord, de tijdstippen waarop en de plaatsen waar die gedragingen hebben plaatsgevonden en waarom die gedragingen aanleiding zijn voor het geven van een of meer gedragsaanwijzingen.[43]

Indien de burgemeester een verbod met een meldingsplicht combineert moeten er, met name voor wat betreft de proportionaliteit, extra eisen aan de

41 Zie: ABRvS 21 april 2010, JG 2010/0038, m. nt. L.D. Ruigrok.

42 Rb. Amsterdam 18 februari 2011, AB 2011/122, m. nt. J.G. Brouwer en A.E. Schilder.

43 Kamerstukken II 2007/08, 31 467, nr. 3, p. 33.

motivering worden gesteld.[44] Bij de motivering kan de methode Hooligan in Beeld een handig hulpmiddel zijn.[45]

In de praktijk leveren de strenge toepassingsvoorwaarden bij de besluitvorming problemen op. De burgemeester dient zijn besluit te baseren op een gedocumenteerd dossier, maar het is lastig om voldoende concrete en ook geïndividualiseerde informatie over het ordeverstorende gedrag van voetbalsupporters te verkrijgen. Bij een onvoldoende gedocumenteerd dossier dient de burgemeester in beginsel niet over te gaan tot het opleggen van een maatregel. Aan de voorwaarden voor toepassing is immers niet voldaan, aangezien een herhaaldelijke verstoring en ernstige vrees voor het wederom verstoren van de openbare orde niet, althans onvoldoende is aan te tonen.

Vooralsnog zijn er met betrekking tot artikel 172a Gemw vier zaken voor de rechter gekomen, waarvan er twee voetbalgerelateerd zijn.[46] In drie van de vier zaken heeft de voorzieningenrechter de gedragsaanwijzing(en) geschorst. Als reden voor schorsing wordt aangevoerd dat er bij het besluit, vanwege een incompleet dossier, sprake is van een zorgvuldigheids- en motiveringsgebrek.[47]

In die gevallen was er overigens geen sprake van een zorgvuldigheids- en motiveringsgebrek. Indien de burgemeester een gedragsaanwijzing oplegt terwijl hij daartoe niet bevoegd is, kan men niet spreken van een zorgvuldigheids- en motiveringsgebrek. In deze gevallen is aan de voorwaarden voor toepassing van de bevoegdheid niet voldaan. De burgemeester had het besluit, met andere woorden, gewoon niet mogen nemen, hij was onbevoegd.

Bekendmaking

Om rechtsgevolg te kunnen hebben, dient de burgemeester het besluit bekend te maken overeenkomstig de regels van artikel 3:41 van de Awb. Het besluit treedt immers niet in werking voordat het bekend is gemaakt.[48] Bekendmaking van het bevel kan geschieden door schriftelijke toezending of door uitreiking aan de verstoorder.

---

44 Kamerstukken II 2007/08, 31 467, nr. 3, p. 13 en 33.

45 Deze methode is landelijk ingevoerd. Zie voor meer informatie Ferwerda & Adang 2005.

46 Stand van zaken in mei 2012.

47 Zie: Rb. Rotterdam 7 mei 2011, LJN BQ3848, Rb. Rotterdam 18 mei 2011, LJN BQ5186, Rb. Breda 20 mei 2011, LJN BQ5217 en Rb. Amsterdam 18 februari 2011, LJN BP5057.

48 Artikel 3:40 Awb.

Uit het onderzoek van de Inspectie OOV blijkt, dat een aantal gemeenten problemen ondervindt bij de bekendmaking van het bevel. In deze gemeenten koos de burgemeester ervoor om het besluit fysiek door de politie te laten uitreiken, maar in een aantal gevallen bleek de betrokkene onvindbaar te zijn.

2.2.3 Complicaties inzake de effectiviteit

Het opleggen van een meldingsplicht op grond van de Wet mbveo blijkt in de praktijk minder doeltreffend dan aanvankelijk werd gedacht.[49] Dit is te wijten aan twee omstandigheden. Ten eerste geldt de meldingsplicht slechts voor korte duur. Duur heeft hier een dubbele betekenis van termijn/periode en de tijd die een meldingsplichtige kwijt is met het melden. En ten tweede is de bevoegdheid om de plicht op te leggen territoriaal begrensd. Beide omstandigheden leiden tot een verminderde effectiviteit van de meldingsplicht.

Beperkte duur meldingsplicht

Allereerst kan in verband met de effectiviteit worden gewezen op de duur waarvoor de meldingsplicht geldt. Deze is afhankelijk van de omstandigheden van het geval. Bepalend zijn onder meer de frequentie, de aard en de ernst van de overlast, alsmede de achtergronden van de verstoorder.[50]

De burgemeester kan de gedragsaanwijzing voor maximaal drie maanden geven. De duur van de gedragsaanwijzing mag niet langer zijn dan strikt noodzakelijk is voor de handhaving van de openbare orde.[51] In de praktijk is duidelijk geworden dat de maximale duur waarvoor een meldingsplicht kan gelden te kort is om voetbalsupporters effectief aan te pakken. De Inspectie OOV constateert ten aanzien hiervan het volgende:

> 'Een maatregel met de termijn van drie maanden kan betekenen dat het – door zomer- of winterstop, een interlandweek of wijzigingen in de wedstrijdkalender – in de praktijk maar om een paar wedstrijden gaat.

49 Evaluatierapport Inspectie OOV 2011, p. 14.

50 Kamerstukken II 2007/08, 31 467, nr. 3, p. 14.

51 Artikel 172a leden 4 en 7 Gemw.

> Deze termijn loopt daarmee uit de pas met de jarenlange stadionverboden die de KNVB of bvo's kunnen uitdelen. […] Een belangrijke overweging om de wet wel of niet in te zetten, is de afweging tussen inspanningen en de effectiviteit van de maatregelen. Betrokkenen beschouwen de termijn van maximaal drie maanden als een knelpunt om het voetbalvandalisme goed aan te kunnen pakken.'[52]

Uit het onderzoek van Pro Facto blijkt eveneens dat men een gedragsaanwijzing van slechts drie maanden voor de aanpak van voetbalvandalisme niet effectief acht.[53]

De duur van de meldingsplicht in de zin van de tijd die een supporter kwijt is door het melden, is eveneens te kort om werkelijk effectief te zijn. Niet zelden is het voor de supporter mogelijk om na het melden gewoon naar het stadion te gaan of zich in het 'strijdgewoel' in de directe omgeving van het stadion te mengen.

De burgemeester is krachtens het vierde lid van artikel 172a Gemw bevoegd om een meldingsplicht driemaal met ten hoogste drie maanden te verlengen. Een verstoorder kan derhalve maximaal een jaar met een meldingsplicht worden geconfronteerd. Aan het verlengen van de gedragsaanwijzing zitten echter veel haken en ogen. De regering merkt in de Memorie van Toelichting bij de Wet mbveo ten aanzien van het verlengen van een gedragsaanwijzing het volgende op:

> 'Iedere verlenging moet worden aangemerkt als een nieuwe beschikking waartegen beroep openstaat, en iedere verlenging zal ook steeds met redenen omkleed moeten worden.'[54]

Teneinde de meldingsplicht te verlengen, dient de burgemeester derhalve een nieuw besluit te nemen. Op dit besluit zijn de voorschriften uit de Awb van toepassing. Bij burgemeesters bestaat echter de nodige onzekerheid over de eisen die aan het nemen van een verlengingsbesluit worden gesteld. Onduidelijk is welke feiten en omstandigheden hij moet aandragen. Een verlenging van de meldingsplicht dient uiteraard noodzakelijk te zijn met het oog op handhaving van de openbare orde. Hiermee is echter nog niet gezegd welke feiten en omstandighe-

52 Evaluatierapport Inspectie OOV 2011, p. 14 en 41.

53 Evaluatierapport Pro Facto 2012, p. 57.

54 Kamerstukken II 2007/08, 31 467, nr. 3, p. 14 en 42.

den de burgemeester aan het nemen van een verlengingsbesluit ten grondslag moet leggen, teneinde een verlengingsbesluit voldoende te motiveren.

We gaan ervan uit dat er in ieder geval sprake moet zijn van een nieuwe verstoring van de openbare orde, wil een verlenging van een object- of gebiedsverbod gerechtvaardigd zijn. Anders zou aan het stellen van een maximale termijn van drie maanden in de wet elke zin ontvallen. Vanzelfsprekend dient die eis ook aan een verlenging van de meldingsplicht te worden gesteld. Is het voor een verlengingsbesluit vereist dat de openbare orde opnieuw bij herhaling is verstoord? Of is een eenmalige verstoring, in combinatie met de 'oude' feiten voldoende? En is het eenmalig of herhaaldelijk niet naleven van de meldingsplicht te beschouwen als een verstoring van de openbare orde?

Een zinvolle uitleg van de bevoegdheid om te verlengen, is dat de voorwaarden minder streng zijn. Aan de voorwaarde van herhaalde verstoring hoeft volgens ons niet te worden voldaan. Een eenmalige hernieuwde verstoring lijkt ons voldoende. Zou men bij het nemen van een verlengingsbesluit de eis van 'herhaling' wel moeten stellen, dan kunnen de 'oude', reeds gesanctioneerde feiten geen rol meer spelen. Dat zou immers in strijd zijn met het universele beginsel van 'ne bis in idem'. Bij het motiveren van 'ernstige vrees voor verdere verstoring van de openbare orde' mogen de 'oude' feiten daarentegen wel een rol spelen. Wat de situatie na een drietal verlengingsbesluiten is of zou moeten zijn, is ook voor ons in nevelen gehuld.

Uit het evaluatierapport van de Inspectie OOV valt op te maken dat gemeenten verschillend omgaan met het verlengen van een gedragsaanwijzing:

> 'De ene gemeente [meent] dat voor verlenging opnieuw een dossier moet worden opgemaakt en vervolgens de procedures moeten worden gevolgd. De andere gemeente meent dat overtreding van een opgelegde maatregel automatisch betekent dat de maatregel kan worden verlengd.'[55]

Beperkte territoriale reikwijdte

Een tweede oorzaak van de verminderde effectiviteit van de meldingsplicht is, dat de bevoegdheid slechts kan worden toegepast bij het bestaan van vrees voor verstoring van de openbare orde op het grondgebied van de gemeente van de

55 De gemeenten Rotterdam en Helmond hebben beide een verlengingsbesluit genomen vanwege overtreding van een opgelegd gebiedsverbod. Zie: Evaluatierapport Inspectie OOV 2011, p. 52.

burgemeester die hem oplegt. De burgemeester is niet verantwoordelijk voor de handhaving van de openbare orde in een andere gemeente en kan derhalve zijn bevoegdheden niet voor dat doel aanwenden. Dit staat weliswaar niet expliciet in artikel 172a Gemw, maar volgt wel uit een systematische interpretatie van de wet.

Met de fysieke meldingsplicht dachten sommige parlementariërs een element uit de wetgeving van het Verenigd Koninkrijk over te nemen. Dat is echter een misverstand. De Football Disorder Act kent voor een verbannen supporter slechts een plicht om vijf dagen voor een internationale wedstrijd of een toernooi op een aangewezen politiebureau zijn paspoort in te leveren.[56]

Artikel 172a Gemw kent de burgemeester alleen een bevoegdheid toe om met betrekking tot wedstrijden in zijn eigen gemeente iets te ondernemen. In principe is de voetbalsupporter, ondanks de oplegging van een of meer gedragsaanwijzingen, vrij om uitwedstrijden van zijn club te bezoeken. Dat een dergelijke situatie ongewenst is, behoeft geen betoog. Een voorbeeld ter illustratie:

> Stel dat een in Utrecht woonachtige fan van FC Utrecht in zijn woonplaats bij herhaling voor ongeregeldheden zorgt. De burgemeester van Utrecht kan hem dan op grond van de Wet mbveo een stadionverbod en een meldingsplicht opleggen. Door deze gedragsaanwijzingen wordt het de supporter drie maanden belet om de thuiswedstrijden van zijn club te bezoeken. Hij kan echter gewoon de uitwedstrijden van FC Utrecht blijven bezoeken. Vanzelfsprekend is het risico dat de supporter op weg naar of in het stadion de openbare orde verstoort even groot als in Utrecht. Toch kan hem bij zijn bezoek aan een uitwedstrijd geen strobreed in de weg worden gelegd.

Kan de burgemeester van de andere stad misschien wat doen? Mag hij de feiten die zich Utrecht hebben voorgedaan gebruiken om maatregelen te treffen? Het is uit een oogpunt van effectiviteit een aantrekkelijke gedachte om hem die mogelijkheid te bieden. Maar dan is letterlijk het hek van de dam. Elke burgemeester zou dan in de toekomst de mogelijkheid hebben om de Utrechtse fei-

56 Article 1 (1) c Football Disorder Act (FDA) 2000. Zie voor een overzicht van de aanpak van voetbalvandalisme in Engeland en Wales: J.G. Brouwer en K. Jacobs, 'Naar een Engelse voetbalwet', 2010); zie ook: Evaluatierapport Pro Facto 2012, p. 69-81.

ten, in combinatie met de ernstige vrees voor verstoring van de openbare orde in zijn eigen gemeente, aan te grijpen om een maatregel, zoals een intergemeentelijke meldingsplicht, te nemen. Op deze manier kan de keten oneindig worden uitgebreid. Iemand zou in dat geval jarenlang voor zowel thuis- als uitwedstrijden geconfronteerd kunnen worden met een stadionverbod en/of een (intergemeentelijke) meldingsplicht.

Voor het opleggen van een intergemeentelijke meldingsplicht is overigens de medewerking dan wel toestemming van de burgemeester van de andere gemeente nodig. Dat levert in de praktijk de nodige problemen op. Het vergt veel afstemming tussen beide burgemeesters en zorgt voor veel administratieve lasten.[57] Het zou derhalve beter zijn om de burgemeester een bevoegdheid te geven om, per overtreding, aan voetbalsupporters een landelijk stadionverbod op te leggen.

Het aantal wedstrijden waarvoor de burgemeester een meldingsplicht kan opleggen is beperkt. Gemiddeld vindt er eens in de twee weken een thuiswedstrijd plaats. De burgemeester kan derhalve voor maximaal zes wedstrijden in zijn gemeente een gedragsaanwijzing geven. In de praktijk kan hij, onder andere door de winter- en zomerstop, een interlandwedstrijd of eventuele wijzigingen in het wedstrijdprogramma, soms voor nog minder wedstrijden een meldingsplicht opleggen. 'De inspanningen die dan moeten worden gedaan om een supporter uiteindelijk maar een paar wedstrijden op afstand te houden, worden niet altijd de moeite waard gevonden', aldus de Inspectie OOV.[58]

Pro Facto constateert eveneens dat het geven van gedragsaanwijzingen een behoorlijke inzet vraagt van gemeenten en de politie, bestaande uit tijd en capaciteit. Betrokkenen zijn van mening dat die inzet niet altijd proportioneel is in verhouding tot de opbrengsten die van de maatregel(en) zijn te verwachten.[59]

In de praktijk gaan gemeenten verschillend om met de meldingsplicht.[60] Sommige gemeenten verruimen de werkingssfeer van artikel 172a Gemw. De burgemeester van Helmond heeft bijvoorbeeld eens een meldingsplicht opgelegd voor wedstrijden buiten zijn gemeente.[61] Andere burgemeesters, zoals die

57 Evaluatierapport Pro Facto 2012, p. 2, 57 en 68.

58 Evaluatierapport Inspectie OOV 2011, p. 41.

59 Evaluatierapport Pro Facto 2012, p. 50 en 58.

60 Pro Facto merkt op dat de reikwijdte en de toepassing van de verschillende instrumenten niet altijd duidelijk zijn voor de gebruikers van de wet. Evaluatierapport Pro Facto 2012, p. 52.

61 Evaluatierapport Inspectie OOV 2001, p. 41 en de brief gemeente Helmond van 21 januari 2011.

van Rotterdam, verplichten verbannen supporters om zich meerdere keren tijdens een wedstrijd te melden. De vraag is of dit rechtens kan. De meldingsplicht is ontworpen als een vrijheidsbeperkende en niet als een vrijheidsbenemende sanctie.

2.2.4 Overige knelpunten ten aanzien van de meldingsplicht

Uit het onderzoek van de Inspectie OOV komt naar voren dat gemeenten problemen ondervinden bij de inrichting en uitvoering van de meldingsplicht. Burgemeesters die aan personen een dergelijke gedragsaanwijzing opleggen, kiezen telkens als meldlocatie het politiebureau. Ook politiebureaus hebben echter beperkte openingstijden, waardoor het kan zijn dat de verbannen supporter om aan de meldingsplicht te voldoen verder moet reizen dan het meest nabijgelegen politiebureau. Soms wordt ook moedwillig voor een veraf gelegen politiebureau gekozen. De vraag is of dit proportioneel is en of een dergelijk voorstel bij de rechter stand zal houden.[62]

De belasting die de Wet mbveo op zowel de capaciteit van de gemeente als de politie legt, vormt een potentiële barrière om een meldingsplicht op te leggen.[63] Volgens de Memorie van Toelichting bij de Wet mbveo zijn er ook andere meldlocaties denkbaar. Er worden zelfs enkele voorbeelden gegeven.[64] Handig is dat echter niet: de uitvoering van de meldingsplicht kost dan niet alleen meer mankracht,[65] maar geeft ook aanleiding tot allerlei complicaties. Bovendien zit een Van der Valk hotel niet direct te wachten op verbannen hooligans.[66]

Volgens het evaluatierapport van de Inspectie OOV doen er zich voorts complicaties voor bij de opvang en registratie van voetbalsupporters die zich op de voorgeschreven wijze melden.[67] Een politiefunctionaris kan een melding direct

62 Evaluatierapport Inspectie OOV 2011, p. 54.

63 Evaluatierapport Pro Facto 2012, p. 58.

64 Kamerstukken II 2007/08, 31 467, nr. 3, p. 7.

65 De bij het onderzoek van Pro Facto betrokken personen geven aan dat de meldingsplicht alleen goed uitvoerbaar is, indien het om een gering aantal personen gaat. Bij grotere aantallen verwacht men in de praktijk problemen. Zie: Evaluatierapport Pro Facto 2012, p. 60.

66 In de praktijk wordt doorgaans als andere meldlocatie gekozen voor het gemeentehuis of Bureau Jeugdzorg. Zie: Evaluatierapport Pro facto 2012, p. 60.

67 Evaluatierapport Inspectie OOV 2011, p. 54.

verwerken in het politiesysteem, in tegenstelling tot een gemeentelijke toezichthouder, die dikwijls geen toegang heeft tot de politiesystemen. Indien de verbannen supporter zich moet melden op het politiebureau zal de registratie derhalve weinig problemen opleveren. Pas bij de keuze voor een andere locatie dan het politiebureau kan dit tot moeilijkheden leiden.[68]

De voorzieningenrechter van de Rechtbank Rotterdam vraagt zich af of een meldingsplicht bijdraagt aan het met de gedragsaanwijzing na te streven doel. Het staat de betrokkene immers vrij om zich te melden en zich vervolgens korte tijd daarna naar het stadion te begeven.[69] De burgemeester van Rotterdam legt om die reden een meldingsplicht op volgens welke de supporter zich twee keer per wedstrijd moet melden. Hoe vaak kan men een supporter zich laten melden, zonder dat er sprake is van een ongerechtvaardigde inbreuk op zijn bewegingsvrijheid en zijn recht op privacy?[70] De grens tussen een vrijheidsbeperkende en vrijheidsbenemende maatregel is flinterdun.

2.3 Concluderende opmerkingen

De slotsom van dit hoofdstuk is, dat de meldingsplicht van artikel 172a Gemw in de praktijk (nog) niet goed functioneert.[71] De voorwaarden waaraan moet zijn voldaan om de gedragsaanwijzing te geven, zijn streng. Vanwege de aard van de verstoring en omdat voetbalsupporters in het algemeen weinig registraties in politiesystemen hebben, is het lastig om aan die voorwaarden te voldoen. Het vereist de opbouw van een gedocumenteerd dossier waaruit blijkt dat de openbare orde herhaaldelijk is verstoord en dat er ernstige vrees bestaat dat de supporter wederom de openbare orde zal verstoren.

De inhoud van de meldingsplicht is beperkt. De tijd die een voetbalsupporter kwijt is met het zich melden, is te kort om een stadionbezoek van hem te beletten. Voor uitwedstrijden beschikt de burgemeester niet over de bevoegdheid, omdat hij niet verantwoordelijk is voor de handhaving van de openbare orde in een andere gemeente.

Ten slotte kan worden gewezen op de complicaties met betrekking tot de

68 In een aantal gemeenten is het boa-registratiesysteem gekoppeld aan de Basis Voorziening Handhaving (BVH). Onduidelijk is in hoeverre in de praktijk bij de registratie van verstoorders sprake is van een probleem.

69 Rb. Rotterdam 7 mei 2011, LJN BQ3848, r.o. 4.5.

70 Hierop is geen kant-en-klaar antwoord te geven, omdat alles afhangt van de omstandigheden van het geval.

71 Zie: Evaluatierapport Inspectie OOV 2011 en Evaluatierapport Pro Facto 2012.

inrichting en uitvoering van de meldingsplicht. De verplichting om zich gedurende een wedstrijd meerdere keren te melden, levert de nodige spanning op met de bewegingsvrijheid en het recht op privacy van de supporter.

3

Naar een digitale aantoonplicht

3.1 Inleiding

Voetbalgerelateerde verstoringen van de openbare orde, vaak aangeduid met de term 'hooliganisme', vormen, alle reeds genomen maatregelen ten spijt, nog altijd een hardnekkig probleem. Het betreft een zeer specifieke, complexe en lastig aan te pakken vorm van overlast, die duidelijk verschilt van ander ordeverstorend gedrag, bijvoorbeeld structurele overlast van jongeren in een woonwijk. Voetbalgerelateerde verstoringen overschrijden vaak de gemeentegrens en zijn daardoor lastig te bestrijden.

Voetbalvandalisme vergt een geheel eigen aanpak en sanctionering. Helaas heeft de wetgever gemeend beide vormen van ordeverstorend gedrag over één kam te kunnen scheren. Het gevolg hiervan is dat een burgemeester met het in de Wet mbveo ter beschikking gestelde instrumentarium de voetbalgerelateerde overlast niet effectief kan bestrijden. Van de doelstelling om doeltreffend te kunnen optreden, zoals op meerdere momenten tijdens de parlementaire behandeling van de Wet mbveo aangegeven,[72] komt weinig terecht.

De wetgever heeft zich onvoldoende gerealiseerd hoe complex de materie is. Dit geldt ook voor het in deze wet geïntroduceerde controlemiddel voor de naleving van een stadion- of gebiedsverbod: de meldingsplicht. Die veroorzaakt in de praktijk niet alleen een keur van problemen, maar blijkt ook een weinig sluitend middel te zijn om te handhaven.[73] Op grond hiervan is het zinvol om op zoek te gaan naar werkbare alternatieven voor de meldingsplicht. Kan er met behulp van technologie een systeem worden opgezet waarmee de politie stadionverboden wel sluitend kan handhaven? Dat is de vraag waar het in dit hoofdstuk om draait.

72 Woorden van gelijke strekking staan in het Landelijk actieplan Voetbal en Veiligheid; het somt de acties op waarmee voetbalvandalisme kan worden bestreden. Zie: http://www.rijksoverheid.nl.

73 In uitzendingen van de televisiezender Powned op 26 november en 3 december 2012 kwam uiterst pijnlijk aan het licht dat ook de KNVB en de clubs er niet in slagen de civielrechtelijke stadionverboden te handhaven.

3.1.1 Stadiongebiedsverbod

Een stadiongebiedsverbod houdt voor de supporter een verbod in om zich gedurende een aantal uren op de dag van een voetbalwedstrijd in het stadion te bevinden, alsmede in een of meer gedeelten van het grondgebied van de gemeente waar de kans op voetbalgerelateerde verstoringen van de openbare orde aanzienlijk is. Men kan dan denken aan het NS-station en de route van het station naar het stadion of het gebied rondom het stamcafé van voetbalsupporters, van waaruit zij vertrekken richting het stadion.

Indien de supporter in het verboden gebied en binnen korte afstand van het stadion woont, kan de burgemeester een toegangsroute van en naar zijn woonadres van het verbod uitzonderen. Dat is noodzakelijk in verband met de bewegingsvrijheid en het privacyrecht van de betrokkene.

3.1.2 Een aantoonplicht

Zoals al eerder opgemerkt, dacht de wetgever met de meldingsplicht een juridisch verschijnsel in te voeren waarmee in Engeland/Wales al veel ervaring is opgedaan. Dat is echter een misverstand. In Engeland/Wales kent men geen meldingsplicht. Onze eigen strafrechter heeft wel eens als bijzondere voorwaarde bij een strafrechtelijk stadionverbod een meldingsplicht opgelegd. Dat was zinvol omdat de supporter van Feyenoord in Emmeloord woonde en zich bij elke wedstrijd op het plaatselijke politiebureau moest melden. Dat belette hem om welke wedstrijd dan ook van zijn club gedurende een vastgestelde periode te bezoeken.

In plaats van een verplichting om zich fysiek te melden, willen wij onderzoeken of het mogelijk is een sluitend systeem te ontwerpen waarin de verbannen supporter moet aantonen dat hij zich niet in het verboden stadion en of gebied bevindt. Het zou niet alleen de handhaving moeten faciliteren, maar ook de mankracht per gecontroleerde persoon moeten verminderen. Het voordeel van een digitale aantoonplicht in vergelijking met de meldingsplicht, is dat de controle niet beperkt hoeft te blijven tot één bepaald moment. De politie kan de supporter gedurende de verboden uren op elk gewenst moment controleren op naleving. Bij de meldingsplicht dient de voetbalsupporter zich eenmalig op het politiebureau te melden. Omdat een meldingsplicht uitsluitend bij thuiswedstrijden kan worden opgelegd, bestaat er een risico dat hij zich alsnog naar het stadion begeeft en/of (elders) voor ongeregeldheden zorgt.

Een digitale aantoonplicht zou het volgende in kunnen houden: de burgemeester legt de supporter een plicht op om op de dag van de voetbalwedstrijd tijdens de verboden uren telefonisch bereikbaar te zijn, zodat er een digitale surveillance en een stemherkenningscheck (*speaker recognition*) kan plaatsvinden. Gedurende de periode dat het de verbannen supporter verboden is om zich in het stadion en/of het verboden gebied van de gemeente te bevinden, kan hij worden gebeld. Met speaker recognition kan de politie vaststellen of zij de juiste persoon aan de telefoon heeft. Vanzelfsprekend kan de politie met behulp van achtergrondgeluiden vrij eenvoudig vaststellen of de persoon zich in het stadion bevindt. Digitale surveillance op afstand moet echter zekerheid verschaffen.

De politie kan op verschillende manieren vaststellen dat de supporter zich niet in het voor hem verboden gebied bevindt. Op welke wijze dit technisch het beste kan, is voorwerp van onderzoek in de derde paragraaf van dit hoofdstuk.

3.1.3 Inrichting aantoonplicht

Het is in beginsel aan de supporter om aan te tonen dat hij zich aan het verblijfsverbod houdt. Een niet onbelangrijke vraag is dus hoe de betrokkene aan de aantoonplicht kan voldoen en hoe de politie kan controleren dat hij zich niet in het verboden gebied bevindt.[74]

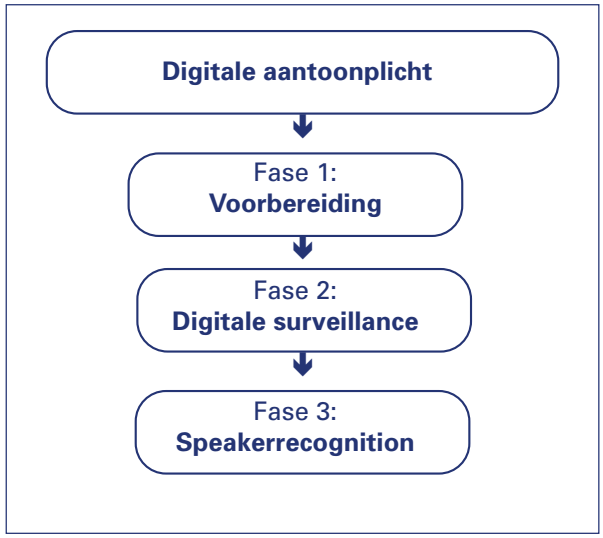
Het systeem dient zo te worden ingericht, dat het de aantoonplichtige en de politie zo min mogelijk belast.[75] Een digitale aantoonplicht belast de voetbalsupporter minder, in die zin dat het zijn bewegingsvrijheid en privacy veel minder beperkt. Door gebruik te maken van geavanceerde apparatuur en software kan de politie op afstand controleren of de supporter de gebiedsontzegging naleeft. Hiermee worden mankracht en kosten bespaard en de problemen uit de praktijk, bijvoorbeeld met betrekking tot de meldingslocatie, opgelost.

Bij de digitale aantoonplicht zijn drie verschillende fasen te onderscheiden, deze zijn in figuur 3.1 weergegeven.

---

74 De politie valt bij handhaving van de openbare orde onder het gezag van de burgemeester; artikel 12 lid 1 Polw 1993.

75 Het is uiteindelijk aan de burgemeester om per geval te bepalen hoe de aantoonplicht eruit komt te zien. Het voordeel hiervan is dat de burgemeester persoonlijke omstandigheden van de betrokkene bij de inrichting van de aantoonplicht mee kan nemen. Op deze manier kan er maatwerk worden geleverd.



Figuur 3.1: Overzicht fasen digitale aantoonplicht.

Paragraaf twee beschrijft de voorbereidende fase. In aansluiting daarop worden in de paragrafen drie en vier de digitale surveillance en de stemherkennings-check uiteengezet.

3.2 De voorbereidende fase

Het systeem van de digitale aanmeldingsplicht heeft een aantal gegevens nodig om te kunnen functioneren. In de voorbereidende fase worden de voor het uitvoeren van de digitale surveillance en de stemherkenningscheck benodigde gegevens verzameld. Het gaat hierbij om de naam, het telefoonnummer en het stemgeluid van de aantoonplichtige, gegevens over de duur van het stadion-gebiedsverbod, gegevens over de omvang van het verboden gebied en de tijdstippen waarop het de supporter verboden is om zich in een of meer gebiedsgedeelten te bevinden.[76]

De eerste drie gegevens worden verkregen van de aantoonplichtige zelf.

76 In principe werkt het systeem met mobiele telefonie, maar als fall-back kan het huistelefoonnummer worden geregistreerd. Indien het systeem vanwege een storing met de mobiele telefoon niet werkt, kan de aantoonplichtige met zijn vaste telefoon alsnog aan de aantoonplicht voldoen.

Daartoe dient hij zich eenmalig met een geldig paspoort of identiteitskaart op het politiebureau te melden. Voor de voetbalsupporter zal de voorbereidende fase ongeveer tien minuten in beslag nemen. De overige gegevens dient de politie van de burgemeester te ontvangen. De politie kan deze gegevens ontvangen door een, al dan niet telefonische, kennisgeving van het besluit van de burgemeester aan de politie.

Een politieambtenaar zal de naam van de aantoonplichtige handmatig in een database opnemen.[77] Om de privacy van de supporter te waarborgen worden de gegevens gekoppeld aan een identificatienummer en wordt de database versleuteld.[78] De naam van de aantoonplichtige is in dat geval bij het systeem en de politieambtenaren die ermee werken niet bekend.[79] Het enige wat zichtbaar is aan de gebruikerskant is of het systeem geheel heeft kunnen draaien, of dat identificatienummer X, vanwege een negatieve stemherkenning of digitale surveillance, uit het systeem is gegooid.[80]

Ook de identificatienummers worden handmatig in het systeem ingevoerd en aan dit nummer worden de overige gegevens die nodig zijn voor het uitvoeren van de aantoonplicht gekoppeld. Het systeem kan zo worden ingericht, dat het tussendoor meldingen geeft ten aanzien van identificatienummers waarvan duidelijk is dat voetbalsupporters zich niet aan het stadiongebiedsverbod houden. De politie kan dan aan de hand van de identificatienummers die niet door het systeem zijn gekomen opzoeken om welke supporters het gaat, zodat er maatregelen kunnen worden getroffen.[81] Als maatregel kan men denken aan het verscherpen van het toezicht in of rond het stadion.[82] Zo hoeven slechts een paar politiefunctionarissen toegang te hebben tot de database met de versleutelde gegevens.

---

77 Dit kan een Excelbestand zijn.

78 Zie voor het gebruik van geanonimiseerde persoonsgegevens Kikkers, Nienhuis & Rutkens 2009.

79 Dit is alleen anders als de politieambtenaar toegang heeft tot de database met de versleutelde gegevens.

80 Technisch gezien is een dergelijk systeem goed te realiseren. Door deze manier van beveiliging wordt het systeem wel complexer. Er dient derhalve een strikte procedure te zijn, zodat duidelijk is welke personen wanneer en op welke wijze toegang hebben tot het systeem. Zo moet de procedure om te decoderen duidelijk zijn omschreven. Een eenmaal gebruikte sleutel om te decoderen moet direct worden vervangen.

81 Het systeem kan zo worden ingericht, dat het direct een signaal afgeeft, zodat men door het treffen van preventieve maatregelen voetbalgerelateerde verstoringen van de openbare orde kan voorkomen. Dit verkleint het risico op voetbalvandalisme en andere voetbalgerelateerde overlast. Voor de werking van het systeem is van belang dat de politie alles in verband met de controleerbaarheid goed vastlegt.

82 Politiepersoneel, spotters en/of stewards kunnen bijvoorbeeld uitkijken naar deze persoon.

Bij de digitale aantoonplicht zal een stemherkenningscheck plaatsvinden en wordt derhalve gebruikgemaakt van biometrie. De betrokkene dient op het politiebureau een bepaalde tekst in te spreken, zodat fragmenten van de stem kunnen worden opgeslagen.[83]

Er zal in beginsel een stemherkenning (speaker recognition) en geen spraakherkenning (*speech recognition*) plaatsvinden. Hiervoor is bewust gekozen, omdat speaker recognition, in tegenstelling tot speech recognition, niet taalafhankelijk is. Bij speech recognition gaat het vooral om wat iemand zegt, terwijl het bij stemherkenning gaat om wie er iets zegt.[84] Bij de speaker recognition kan de politie voor het inspreken een willekeurige tekst, bijvoorbeeld een krantenartikel, gebruiken. Waarschijnlijk is het reeds voldoende om de aantoonplichtige een paar zinnen van een tekst voor te laten lezen.

Door van het stemgeluid een voice-model te maken (*enrollen*), kan het systeem bij de speaker recognition nagaan of het de aantoonplichtige is die de politie aan de telefoon heeft. Het voice-model wordt versleuteld opgeslagen in het systeem, zodat onbevoegden de gegevens niet kunnen uitlezen. Hierdoor kan men de privacy van de voetbalsupporter waarborgen en misbruik voorkomen. Het verdient de voorkeur om slechts een selecte groep politieambtenaren toegang te verschaffen tot het systeem en de hele procedure voor versleutelen en decoderen goed te omschrijven. Het systeem kan zo worden ingesteld, dat het bij identificatienummer X op de dag van de voetbalwedstrijd, gedurende de tijdstippen waarop het de aantoonplichtige verboden is om zich in een bepaald gebied te bevinden, draait. Daarvoor is vereist dat als parameter aan het identificatienummer de data van de voetbalwedstrijden worden gekoppeld.

3.3 *Digitale surveillance*

Bij de digitale surveillance gaat het erom daadwerkelijk vast te stellen dat de supporter niet in het verboden gebied aanwezig is. Er zijn verschillende manieren denkbaar om digitaal te surveilleren. Gedacht kan worden aan het versturen van sms-berichten, het verrichten van een driehoeksmeting of het gebruiken van gps.

83 Het systeem maakt gebruik van karakteristieken van het stemgeluid van de aantoonplichtige.

84 Willemsen (red.) 2008, p. 20. Wellicht dat een combinatie van stem- en spraakherkenning nuttig kan zijn.

3.3.1 Sms-berichten

Tijdens de digitale surveillance kan het systeem sms-berichten versturen naar de telefoon van de aantoonplichtige. Hierdoor kan de politie een grove plaatsbepaling verrichten.

Onderzocht is of dit op dezelfde wijze kan als bij de *stealth* sms-berichten die in het kader van strafrechtelijke handhaving worden gebruikt. Een stealth sms wordt heimelijk naar de ontvanger verzonden.[85] De ontvanger kan het derhalve niet zien dat naar hem een dergelijk bericht is gestuurd en dat de verzender daarmee bepaalde gegevens verkrijgt. Door middel van het stealth sms-bericht kan de politie namelijk gegevens verkrijgen over het telefoonverkeer. Daarvoor is over het algemeen wel het plaatsen van een telefoontap nodig.[86] In het strafrecht worden stealth sms-berichten als technisch hulpmiddel gebruikt om te bepalen in welk gebied de telefoon van de ontvanger van het bericht is.[87]

Voor de digitale surveillance is het niet nodig om gebruik te maken van onzichtbare sms-berichten. Uit een oogpunt van transparantie is het misschien beter om dergelijke sms-berichten zichtbaar te versturen. Van de andere kant belast dit een aantoonplichtige meer. In ieder geval dient een aantoonplichtige op de hoogte te zijn van het sturen van sms-berichten. Aan de supporter dient duidelijk uiteengezet te worden dat hij op de dag van de voetbalwedstrijd een of meerdere sms-berichten ontvangt die voor hem al dan niet zichtbaar zijn.

Voor het toepassen van deze techniek is het nodig dat de politie een geldige telefoontap plaatst. Aan de voorwaarden voor het plaatsen van een tap wordt in het kader van de aantoonplicht normaal gesproken niet voldaan. Dat wil echter niet zeggen dat deze plaatsbepalingsmethode voor het digitaal surveilleren bij de aantoonplicht geheel onbruikbaar is.[88]

---

85 De software zorgt ervoor dat het sms-bericht voor de ontvanger niet zichtbaar is.

86 In Nederland hebben veel providers hun gsm-mastennetwerk dichtgezet. Door middel van het plaatsen van een telefoontap in combinatie met het versturen van stealth sms-berichten, is in dat geval te zien binnen welke straal van de gsm-mast een persoon zich bevindt.

87 De politie maakt soms in het kader van haar hulpverleningstaak gebruik van deze methode. Zie: artikel 2 Polw 1993 en bijvoorbeeld Rb. Amsterdam 8 maart 2011, LJN BP7233.

88 Het versturen van sms-berichten en het verkrijgen van een Cell-ID kan anders worden vormgeven. Het systeem kan bijvoorbeeld zo worden ingericht, dat het sms-berichten stuurt naar de aantoonplichtige, dat deze zich moet aanmelden. Om zich aan te melden kan gebruik worden gemaakt van gps en een speciaal voor de aantoonplicht ontwikkelde app, waarmee de politie vervolgens een Cell-ID krijgt om de supporter op afstand op naleving van het stadiongebiedsverbod te kunnen controleren.

Digitaal surveilleren door sms-berichten

Hoe kan met sms-berichten een grove plaatsbepaling plaatsvinden? Een mobiele telefoon zoekt na inschakeling altijd contact met gsm-masten. Het versturen van de *overt* sms-berichten kan zo geprogrammeerd worden, dat de verzender van het bericht een ontvangstbevestiging krijgt met daarin onder meer het identificatienummer van de publieke zendmast (het Cell-ID) waarmee de telefoon in verbinding staat. Met het Cell-ID kan de politie bepalen in welk gebied de telefoon van de supporter zich bevindt.

Bij de digitale aantoonplicht kan het systeem vlak voor, tijdens en/of na het telefoongesprek dat met de aantoonplichtige plaatsvindt dergelijke sms-berichten versturen naar zijn telefoon. De telefoon van de voetbalsupporter zendt via de gsm-mast een signaal terug. Aangezien alle gsm-masten een Cell-ID hebben, kan het systeem aan de hand van de Cell-ID de dichtstbijzijnde gsm-mast uitlezen.

Voor de werking hiervan is de politie wel gedeeltelijk afhankelijk van de providers. Vereist is namelijk dat duidelijk is waar de gsm-mast met een bepaalde Cell-ID zich fysiek bevindt. De politie dient derhalve toegang te hebben tot een database (radioplan) met daarin de locaties van de desbetreffende masten. Deze databases zijn niet vrij beschikbaar, maar de politie beschikt doorgaans wel over de meest recente gegevens. Het KLPD krijgt iedere maand een bijgewerkte database en stelt deze vervolgens aan enkele personen beschikbaar.[89] Bij de digitale surveillance spelen deze gegevens ook een rol.[90]

In de voorbereidende fase dient een politieambtenaar de Cell-ID's waarvan men zeker weet dat de gsm-masten zich in het verboden gebied bevinden in het systeem in te voeren. Cell-ID's waarvan duidelijk is dat deze zo dicht bij het verboden gebied in de buurt staan dat niet is uitgesloten dat de supporter daar niet aanwezig is, worden ook in het systeem opgenomen. Het systeem kan dan op de dag van de voetbalwedstrijd in een fractie van een seconde controleren of de telefoon zich niet in het verboden gebied bevindt. Het systeem doet dit door de met het sms-bericht verkregen Cell-ID te vergelijken met de lijst Cell-ID's van de gsm-masten die in en rondom het verboden gebied staan.

89 Het KLPD verkrijgt de database van de providers zelf, maar de regels voor terbeschikkingstelling zijn streng. Zie: bijlage 1 Expertmeetings, gespreksnotitie KLPD Driebergen.

90 De politie gebruikt deze gegevens in het kader van strafrechtelijke handhaving. Voor de digitale surveillance dient derhalve gekeken te worden in hoeverre de politie bij de uitvoering van de aantoonplicht deze gegevens kan gebruiken en of zij via providers de beschikking kan krijgen over (een deel van) deze databases.

Hoe nauwkeurig is de plaatsbepaling?

Met het versturen van sms-berichten kan het systeem slechts een grove lokalisatie verrichten om te bepalen of de verbannen voetbalsupporter het stadiongebiedsverbod naleeft. Het systeem kan alleen 'zien' binnen welke straal van de gsm-mast de telefoon van de aantoonplichtige zich ophoudt. Een exacte locatiebepaling is ook niet noodzakelijk. Het is slechts van belang om te kunnen vaststellen dat de supporter zich niet in het voor hem verboden gebied bevindt. Die controle zal bij voorkeur geheel geautomatiseerd plaatsvinden, hierbij gebruikmakend van alleen telefoonverkeersgegevens zonder ze op te slaan. Omdat de dekking van gsm-masten over het algemeen goed is en in steden (rondom stadions) zelfs zeer goed, kan dit met de nodige precisie worden vastgesteld.[91]

Het systeem kan zo worden ingericht, dat de uitkomst van de plaatsbepaling niet zichtbaar is voor het politiepersoneel dat met het systeem werkt. Het systeem geeft in dat geval slechts een positief of negatief antwoord op de vraag of de desbetreffende persoon zich niet in het verboden gebied bevindt en zal dit vervolgens in een tekstsheet bij het desbetreffende identificatienummer vermelden. Het antwoord zal negatief zijn als duidelijk is dat de telefoon in het verboden gebied is. Het antwoord is eveneens negatief als de uitkomst onbetrouwbaar is, omdat het systeem een Cell-ID heeft verkregen van een gsm-mast die dicht bij het verboden gebied in de buurt staat. In dat geval kan in het gebied extra naar deze persoon worden uitgekeken of eventueel een nadere precisering plaatsvinden.

In het strafrecht wordt voor een meer nauwkeurige locatiebepaling gebruikgemaakt van een *IMSI-catcher*.[92] Dit is een technisch hulpmiddel dat feitelijk de functie van een gsm-mast overneemt. De communicatie van alle mobiele telefoons die in het naburige gebied in gebruik zijn of op stand-by staan, verloopt in dat geval via de IMSI-catcher en niet via de publieke zendmast. Het apparaat scant alle frequenties van de aanbieders van een openbaar mobiel communicatienetwerk of -dienst en registreert op dat moment de IMSI-nummers en IMEI-nummers van alle telefoons die zich aanmelden.[93] Een IMEI-nummer is een uniek 15-cijferig nummer dat aan een telefoon is verbonden zoals het chassisnummer aan een auto. De IMSI-catcher maakt het mogelijk om exact de locatie van een mobiele telefoon te bepalen.

---

91 Bij grote evenementen worden soms gedurende korte tijd extra palen bijgeplaatst.

92 Zie: Rb. Amsterdam 8 maart 2011, LJN BP 7233, Rb. Haarlem 29 april 2011, LJN BQ3272 en Hof Arnhem 24 januari 2012, LJN BV3076.

93 Rb. Amsterdam 8 maart 2011, LJN BP 7233, r.o. 3.4.3.

Aangezien een IMSI-catcher het mobieletelefoonverkeer in de omgeving van de gsm-mast 'afvangt', is dit middel niet geschikt voor het uitvoeren van een digitale surveillance bij de aantoonplicht. Bij de digitale aantoonplicht zou een meer verfijnde plaatsbepaling wellicht kunnen worden verricht via een driehoeksmeting of gps-tracking, deze worden in de paragrafen 3.3.2 en 3.3.3 verder uitgewerkt. De sms-berichten hebben in die gevallen een zeeffunctie. Met het versturen ervan wordt een trechtermodel gehanteerd, zodat een driehoeksmeting of gps-tracking slechts plaatsvindt indien dit daadwerkelijk noodzakelijk is. Hieronder een voorbeeld.[94]

Stel dat de burgemeester van Leeuwarden bij besluit van 17 maart 2012 aan twee voetbalsupporters van SC Cambuur een stadiongebiedsverbod en aantoonplicht heeft opgelegd voor de duur van zes wedstrijden. In het besluit van de burgemeester staat de aantoonplicht duidelijk omschreven.

Beide supporters zijn op het politiebureau verschenen. De eerste supporter heeft identificatienummer 5. Aan de tweede supporter is het identificatienummer 9 gekoppeld. Van beide identificatienummers zijn de benodigde gegevens in het systeem ingevoerd. Op de dag van de wedstrijd stuurt het systeem tijdens de verboden tijdstippen een of meer smsberichten naar de mobiele telefoons van de supporters.

Het systeem krijgt ten aanzien van het identificatienummer 5 zowel vóór aanvang van de voetbalwedstrijd als tijdens de wedstrijd de Cell-ID 1256670739 terug. Het betreft in dit geval een gsm-mast die in Arnhem staat en die ver van het voor deze supporter verboden gebied verwijderd is. Het systeem beperkt zich ertoe aan te geven dat identificatienummer 5 zich niet in het verboden stadiongebied bevindt.

Met betrekking tot identificatienummer 9 verkrijgt het systeem vóór aanvang van de wedstrijd Cell-ID 123507175 terug. Hoewel de gsm-mast niet in het voor de supporter verboden gebied staat, bevindt deze zich wel op loopafstand van het stadion en bij de grens van het voor hem verboden gebied. In dit geval kan een nadere specificering van de locatie nuttig zijn en kan in het verboden gebied extra naar deze persoon worden uitgekeken.

94 De Cell-ID's in dit voorbeeld zijn verkregen via http://www.antenneregister.nl/register/Map.aspx; de Cell-ID's van gsm-masten zijn niet algemeen bekend.

Toelaatbaarheid sms-berichten

In hoeverre is het gebruik van een dergelijke methode voor het doen van een plaatsbepaling toelaatbaar? Voor de toelaatbaarheid van sms-berichten is onderzocht hoe de strafrechter de rechtmatigheid van stealth sms-berichten beoordeelt.

In het strafrecht is voor het versturen van stealth sms-berichten een wettelijke grondslag vereist. In de rechtspraak wordt wisselend gedacht over welk artikel als wettelijke basis voor het versturen van dergelijke sms-berichten kan worden beschouwd. Zo is er enige onduidelijkheid over artikel 126n van het Wetboek van Strafvordering (WvSv) als rechtsbasis.

De Rechtbank Arnhem oordeelt in 2011 het volgende:

> 'vaststaat dat het WvSv noch andere wet- of regelgeving regels bevatten die een dergelijke inzet reguleren. Ook artikel 126n van het WvSv kan niet als zodanig worden aangemerkt, nu het daarbij gaat om een vordering aan de aanbieder van een telecommunicatiedienst tot het verstrekken van de zogeheten verkeersgegevens van een bepaalde gebruiker van die telecommunicatiedienst'.[95]

In 2012 oordeelt de Rechtbank Rotterdam echter dat men artikel 126n van het WvSv wel als wettelijke grondslag voor het versturen van stealth sms-berichten kan gebruiken.[96]

Artikel 2 van de Politiewet 1993 (Polw 1993) kan in beginsel niet als wettelijke grondslag dienen, tenzij het versturen van dergelijke sms-berichten onder de hulpverleningstaak van de politie kan worden gebracht.[97] Dat laatste deed zich bijvoorbeeld voor in een zaak bij de Rechtbank Amsterdam omtrent een gijzeling van een persoon.[98] Volgens de rechtbank is voor de beoordeling van de toelaatbaarheid van de inzet van stealth sms-berichten doorslaggevend in welke mate de inzet van die middelen inbreuk maakt op de fundamentele rechten van betrokkene en het met de opsporing gemoeide belang.[99]

---

95 Rb. Arnhem 8 november 2011, LJN BU3688, r.o. 3.1.

96 Rb. Rotterdam 11 april 2012, LJN BW3105.

97 Ten aanzien van IMSI-catcher heeft de rechter daarentegen bepaald dat de algemene taakomschrijving van artikel 2 Polw 1993 voldoende basis biedt. Zie: Hof Arnhem 24 januari 2012, LJN BV3076, Rb. Amsterdam 8 maart 2011, LJN BP7233 en Corstens 2011, p. 448.

98 Rb. Amsterdam 8 maart 2011, LJN BP7233.

99 Zie: Rb. Amsterdam 8 maart 2011, LJN BP7233, r.o. 3.5.2.1.

Dat de beperking van het privacyrecht een rol speelt bij de beoordeling van de toelaatbaarheid van stealth sms-berichten blijkt uit een uitspraak van de Rechtbank Arnhem in 2011. In deze zaak ging het om een persoon die werd verdacht van het voorhanden hebben van cocaïne en waarbij er, voordat er een observatie plaatsvond, stealth sms-berichten zijn verstuurd. Naar aanleiding van de sms-berichten en de observatie is de verdachte uiteindelijk aangehouden.

De Rechtbank Arnhem oordeelde dat het versturen van stealth sms-berichten niet op een wettelijke grondslag berustte en dat er derhalve sprake was van een vormverzuim. De rechtbank verbond aan dit verzuim echter geen rechtsgevolgen, omdat het verzuim gering was.

> 'Daarbij neemt de rechtbank in aanmerking dat de telefoon van verdachte met machtiging van de rechter-commissaris reeds werd afgeluisterd en dat er ook al een bevel tot stelselmatige observatie was afgegeven. De persoonlijke levenssfeer van verdachte lag daarom al onder het "vergrootglas". Het verzenden van twee stealth sms-berichten om de locatie van verdachte te bepalen zodat een aanvang kon worden gemaakt met de daadwerkelijke observatie, levert in die omstandigheden slechts een zeer beperkte extra inbreuk op de privacy op.'[100]

Uit de rechtspraak blijkt dat wanneer er reeds een geldige telefoontap loopt en de verdachte stelselmatig mag worden geobserveerd, het versturen van stealth sms-berichten, ondanks dat dit geen wettelijke basis heeft, toegelaten kan zijn.[101]

Teneinde de toelaatbaarheid van het versturen van sms-berichten te beoordelen, is gekeken naar het doel, de duur, de intensiteit en de wijze waarop de aantoonplichtige op de naleving van het stadiongebiedsverbod wordt gecontroleerd.

Het versturen van sms-berichten beoogt vast te stellen dat de voetbalsupporter zich niet in het verboden gebied bevindt. Het vindt slechts plaats met het oog op controle van het aan hem opgelegde stadiongebiedsverbod. Belangrijk is dat het voor de politie irrelevant is om te weten waar de aantoonplichtige zich precies bevindt. Het systeem kan zo worden ingericht, dat de politie dat ook niet weet.

100 Rb. Arnhem 8 november 2011, LJN BU3688, r.o. 3.1.

101 Uiteraard is in dat geval vereist dat het versturen van stealth sms-berichten proportioneel is.

Voor de aantoonplicht is verder van belang wanneer, hoe vaak en op welke wijze dit technische hulpmiddel wordt ingezet. De manier waarop de controle op de naleving van het stadiongebiedsverbod gebeurt, is reeds beschreven. Het systeem verstuurt de sms-berichten alleen gedurende de uren waarop het de supporter verboden is om in het gebied aanwezig te zijn. Een pilot kan uitwijzen of men kan volstaan met het versturen van een enkel sms-bericht of dat het systeem willekeurig een aantal berichten naar de telefoon van de aantoonplichtige moet sturen.[102] Het versturen van twee à drie sms-berichten op de dag van de voetbalwedstrijd zal met betrekking tot het privacyrecht van de supporter geen problemen opleveren. Uiteindelijk is de belasting voor hem minimaal.

Wat betreft het doel, de duur, de intensiteit en de wijze waarop de nalevingscontrole plaatsvindt, scoort het versturen van sms-berichten goed. Het versturen van dergelijke sms-berichten is derhalve geoorloofd.

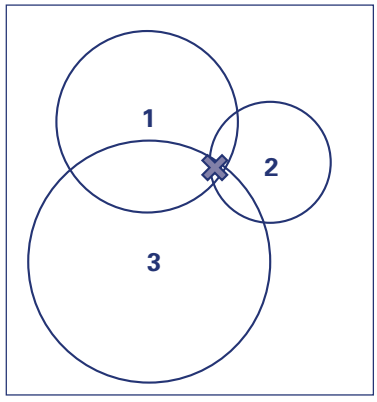
3.3.2 *Driehoeksmeting*

Via een driehoeksmeting kan eveneens worden gecontroleerd of de voetbalsupporter zich aan het stadiongebiedsverbod houdt. Een driehoeksmeting kan (gedeeltelijk) geautomatiseerd plaatsvinden en werkt als volgt: een mobiele telefoon communiceert continu, ook als deze stand-by staat, met verschillende gsm-masten. Indien de telefoon van de aantoonplichtige met minimaal drie gsm-masten contact maakt, kan de locatie van zijn mobiele telefoon worden bepaald.[103] Met behulp van de signaalsterkte van de gsm-masten kan het systeem namelijk berekenen in welk gebied de telefoon van de voetbalsupporter zich bevindt. Door de ontvangsttijd van het signaal te bepalen en deze met de gsm-masten te vergelijken, kan het systeem door het verschil in ontvangsttijd een plaatsbepaling verrichten. In figuur 3.2 is te zien hoe lokalisatie door middel een driehoeksmeting plaatsvindt.

Uit figuur 3.2 is op te maken dat de telefoon van de aantoonplichtige met gsm-mast 2 een vrij goede verbinding heeft en zich dicht in de buurt van deze gsm-mast bevindt. De telefoon van de supporter heeft van gsm-mast 3 het minst sterkte signaal opgevangen. Door te kijken waar de signaalsterktes van de

102 In het laatste geval moet men denken aan ongeveer twee of drie sms-berichten in de vier à vijf uur dat het stadiongebiedsverbod duurt.

103 Wessels 2008, p. 3.



Figuur 3.2: Driehoeksmeting

gsm-masten elkaar overlappen, kan de telefoon van de aantoonplichtige worden gelokaliseerd.

Plaatsbepaling door middel van een driehoeksmeting is nauwkeuriger dan lokalisatie via sms-berichten. In gebieden waar een behoorlijk aantal gsm-masten staat en de dekking derhalve hoog is, is een plaatsbepaling tot op 50 meter mogelijk, al is een nauwkeurigheid van 100 tot 200 meter gebruikelijker. Op het platteland en in andere dunbevolkte gebieden waar minder gsm-masten staan, neemt de nauwkeurigheid van de lokalisatie af tot op een aantal kilometers. Aangezien de dekking door gsm-masten in gebieden die door burgemeesters als verboden worden aangewezen goed is, levert dit voor de controle op de naleving van het stadiongebiedsverbod geen problemen op. Het is immers uitsluitend relevant om te kunnen vaststellen dat de verbannen voetbalsupporter zich niet in of in de buurt van het stadion bevindt.

Met de driehoeksmeting stelt de politie slechts vast dat de mobiele telefoon van de aantoonplichtige zich niet in het verboden gebied bevindt. Een exacte locatiebepaling is derhalve niet nodig. In het strafrecht zou dit, mede in verband met het bewijsrecht, soms een probleem kunnen opleveren. In dit kader, waarin de locatiegegevens worden gebruikt voor de handhaving van het openbare orde, verwachten wij geen problemen.

De controle van de locatie door middel van de driehoeksmeting is afhankelijk van de gegevens die uit de driehoeksmeting worden verkregen. Ervan uitgaande dat deze in de vorm van gps-coördinaten verkregen worden, moet een range van gps-coördinaten in het systeem worden ingevoerd. Als de verkregen gps-coördinaten binnen deze range vallen, zal het systeem vaststellen dat de

telefoon zich in het verboden gebied bevindt. De verwerking zal op eenzelfde manier als bij de digitale surveillance plaastvinden: door het versturen van sms-berichten. Het systeem vergelijkt de coördinaten van de driehoeksmeting met de coördinaten die in het systeem opgegeven zijn, zonder deze op te slaan, en geeft vervolgens slechts aan of ze wel of niet binnen de opgegeven range vallen.

Een belangrijk voordeel van een driehoeksmeting is dat deze bij elk type telefoon kan plaatsvinden. Aan het verrichten van een driehoeksmeting kleven echter een aantal onoverkomelijke bezwaren. De politie is bijvoorbeeld geheel afhankelijk van de providers. Alleen door medewerking van de providers kan via deze methode lokalisatie plaatsvinden. Providers zijn over het algemeen minder bereid om mee te werken aan het verrichten van een driehoeksmeting. Bovendien is ons gsm-netwerk volgens het KLPD niet ingericht op het verrichten van driehoeksmetingen.

Daarnaast blijkt uit ervaringen van het KLPD deze plaatsbepalingsmethode de ene dag heel goed, maar de andere dag ineens niet meer te werken. Dit komt doordat er regelmatig wijzigingen optreden in het telefoonmastenbestand. Derhalve dient te worden geconcludeerd dat het niet handig is om bij de aantoonplicht door middel van een driehoeksmeting digitaal te surveilleren.

3.3.3 *Gps*

Digitale surveillance kan ook plaatsvinden door gebruik te maken van gps. Bij gps-tracking maakt het systeem gebruik van een groot aantal satellieten die in een geostationaire, vaste baan om de aarde draaien.

Werkwijze

Om de radiosignalen die een satelliet uitzendt op te vangen, is een gps-ontvanger nodig. Alleen een gps-ontvanger kan deze signalen namelijk detecteren. Indien de telefoon van de aantoonplichtige is uitgerust met een gps-ontvanger, kan door middel van gps-tracking een plaatsbepaling worden gedaan. Tegenwoordig is in steeds meer telefoons een gps-ontvanger geïntegreerd.

Via een elektronisch communicatienetwerk kunnen de locatiegegevens naar een derde partij worden verstuurd.[104] Daarvoor is wel vereist dat de telefoon,

104 De Bot & Renette 2006, p. 210.

naast gps-technologie, een Global Packet Radio Service (GPRS) of een andere vorm van elektronische communicatie gebruikt. GPRS is een techniek die het mogelijk maakt om sneller informatie te verzenden en te ontvangen.[105]

Bij gps-tracking kan gebruik worden gemaakt van een *fencingsysteem*. Men plaatst in dat geval om het verboden gebied een digitaal hek. Zodra de telefoon van de voetbalsupporter dit 'hek' passeert, gaat er bij de politie een signaal af. In dat geval kunnen er (preventieve) maatregelen worden getroffen, doordat het in het gebied aanwezige politiepersoneel, spotters of stewards extra uitkijken naar deze persoon. Het passeren van het 'hek' is bovendien in beginsel voldoende bewijs voor de vaststelling van de niet-naleving van het stadiongebiedsverbod.

Betrouwbaarheid

Door middel van gps-tracking kan de locatie van de telefoon van de aantoonplichtige zeer precies worden bepaald. Dat is, in vergelijking met de driehoeksmeting, een belangrijk voordeel. Voor de digitale surveillance bij een aantoonplicht is een zodanige nauwkeurigheid echter niet van belang. Bovendien kan men bij de digitale surveillance door middel van gps een aantal kanttekeningen plaatsen.

Bij gps-tracking weet het systeem continu waar de aantoonplichtige zich bevindt. Het systeem kan de locatie van de telefoon van de betrokkene immers zeer precies bepalen. Uiteraard kan het systeem zo worden ingericht, dat deze gegevens voor het politiepersoneel niet zichtbaar zijn en niet te achterhalen vallen.

Een ander knelpunt bij lokalisatie door middel van gps is dat het systeem last kan hebben van storingen. Het werkt bijvoorbeeld niet of minder goed op het moment dat de aantoonplichtige zich in een gebouw bevindt. Een gps-ontvanger kan er namelijk moeite mee hebben om de radiosignalen die de satellieten uitzenden in gebouwen of onder de grond te ontvangen. Als gevolg hiervan is de kans dat de digitale surveillance ten onrechte mislukt, bij gps als plaatsbepalingsmethode waarschijnlijk groter dan bij de driehoeksmeting. Uiteraard kunnen er wel algebraïsche correcties worden toegepast.

Ten slotte is van belang dat niet iedere telefoon de radiosignalen die een satelliet uitzendt, kan ontvangen. Oudere telefoons beschikken niet over een

105 De Bot & Renette 2006, p. 210.

gps-ontvanger. Dit kan bij de digitale surveillance complicaties geven. In hoeverre kan men van de aantoonplichtige verlangen dat hij over een smartphone beschikt? Dit is een tijdelijk probleem; over een aantal jaren zal het vrijwel niet (meer) voorkomen. De verwachting is dat de meeste voetbalhooligans (vaak jonge mensen) over een smartphone beschikken. Op de zeer korte termijn kan dit echter een beletsel zijn.

Digitale surveillance door gps en een speciale app

Bij de digitale surveillance door middel van gps zou de politie gebruik kunnen maken van een speciaal voor de aantoonplicht ontwikkelde applicatie (app). Deze app kan de aantoonplichtige op zijn telefoon installeren. Doordat de telefoon van de supporter verbonden is met een gsm-mast, kan de politie via de app een Cell-ID verkrijgen. De app zorgt ervoor dat de gsm-mast het Cell-ID opstuurt.

De digitale surveillance kan in dit geval zo worden vormgegeven, dat het systeem de aantoonplichtige een sms-bericht stuurt dat hij zich moet aanmelden. Wanneer de supporter zich vervolgens aanmeldt, krijgt de politie binnen een paar seconden een Cell-ID terug. Aan de hand van het Cell-ID kan vervolgens een grove lokalisatie plaatsvinden.

Deze methode heeft als voordeel dat ze behoorlijk snel werkt en dat de locatie van de aantoonplichtige op deze manier niet exact te achterhalen is. Een ander voordeel is dat men met de app die het Cell-ID doorstuurt minder last heeft van storingen dan bij gps-tracking zonder app.[106]

Net als bij de andere methoden bestaat er een kans dat de voetbalsupporter probeert om de app te manipuleren. De kans van slagen hangt af van de app. Bij de ontwikkeling ervan dient men rekening te houden met misbruik.[107] Er bestaat verder een kans dat het systeem een Cell-ID niet herkent. Het systeem zou zo moeten zijn ingericht, dat in zo'n geval een sms-bericht naar de aan-

106 Bij digitale surveillance via gps-tracking kan interference, bijvoorbeeld doordat de betrokkene zich in een gebouw bevindt, complicaties geven.

107 Er bestaat een kans dat de aantoonplichtige de app probeert te misbruiken. De kans dat hem dat lukt is vermoedelijk klein, omdat hij daarvoor techniek moet inkopen en opdracht moet verlenen aan ICT-experts. Wanneer de app heel erg veel gebruikt gaat worden, wordt de kans op het manipuleren van de app groter. Daarvoor zou regelmatig upgraden van de app misschien een oplossing zijn. Het zich onttrekken aan de aantoonplicht is overigens een strafbaar feit.

toonplichtige wordt verstuurd met daarin het verzoek om zich opnieuw aan te melden, dan wel op een ander manier aan te tonen dat hij zich niet in het verboden gebied bevindt.

Het versturen van sms-berichten en het gebruik van gps en een speciaal ontwikkelde app is een methode die bij de aantoonplicht goed kan werken om digitaal te surveilleren. Voor de toepassing van deze methode is wel vereist dat betrokkene met de installatie van de app op zijn smartphone moet instemmen.[108] Dat levert niet per se een nadeel op, eerder biedt het mogelijkheden. In de praktijk zou men een verbannen voetbalsupporter de keuze kunnen geven tussen een meldingsplicht of een digitale aantoonplicht.[109]

3.4 Speaker recognition

Teneinde te kunnen bepalen dat het daadwerkelijk de aantoonplichtige is die op naleving van het stadiongebiedsverbod wordt gecontroleerd, kan speaker recognition plaatsvinden.[110] De stemherkenningscheck betreft een geheel geautomatiseerde biometrische toets op afstand. In deze fase belt een computer op de dag van de voetbalwedstrijd op willekeurige tijdstippen naar de supporter. Door de aantoonplichtige *at random* te bellen en dit ook duidelijk aan hem kenbaar te maken, kan worden voorkomen dat hij zich, nadat hij één keer is gebeld, alsnog naar het voetbalstadstadion begeeft. Er gaat derhalve een prikkel van uit om niet al te lichtvaardig met een verbod om te gaan.

Voor de handhaving van het stadiongebiedsverbod door middel van biometrie, is speciale apparatuur en software nodig. Tijdens het telefoongesprek dient de voetbalsupporter een bepaalde tekst voor te lezen of bepaalde zinnen na te spreken. Het systeem voert vervolgens een verificatie uit door de stem van de persoon die wordt gebeld te vergelijken met het voice-model dat aan het identificatienummer is gekoppeld. Dit kan doordat het systeem het stemgeluid van

108 Daarnaast is het van belang dat de politie goed logt. Alleen indien duidelijk is welke handelingen de politie wanneer heeft verricht, kan men aantonen dat er bij de digitale surveillance door middel van een speciale app geen sprake is van (stelselmatige) observatie.

109 Indien de voetbalsupporter de voorkeur geeft aan een digitale aantoonplicht, kan men hem bovendien de mogelijkheid geven om met een vaste telefoon of via de op zijn smartphone geïnstalleerde app aan te tonen het stadiongebiedsverbod na te leven.

110 In 2005 hebben de arrondissementen Amsterdam, Rotterdam en Arnhem in het kader van handhaving van strafrechtelijke stadionverboden al eens geëxperimenteerd met stemherkenning. Zie: http://www.recht.nl/nieuws/strafrecht/archief/index.html?nid=21920.

de beller omzet in een voiceprint en die vergelijkt met de eerdere opname (*template*). Er vindt derhalve in beginsel slechts een 'een-op-eenvergelijking' plaats. Deze manier van speaker recognition wordt ook wel aangeduid met de term *speaker verification*.[111]

Wanneer de speaker recognition negatief is, zal het systeem een signaal afgeven, zodat er eventuele maatregelen kunnen worden getroffen.[112]

3.4.1 Betrouwbaarheid

Met een biometrische toets verkrijgt men geen 100 procent zekerheid.[113] Maar dat hoeft misschien ook niet. Het betreft immers een statistisch middel, dat in dit geval wordt ingezet voor het voorkomen van voetbalgerelateerde verstoring van de openbare orde. Hoe zit het eigenlijk met de betrouwbaarheid van speaker recognition?

Dat men met speaker recognition nooit 100 procent zekerheid kan verkrijgen, betekent niet dat het gebruik van biometrie voor de handhaving van het stadiongebiedsverbod uitgesloten is. Het gebruik ervan kan juist bijdragen aan een effectievere en efficiëntere handhaving van stadiongebiedsverboden. Er zijn echter wel een aantal factoren die de betrouwbaarheid van de speaker recognition kunnen aantasten. Een van die factoren is ruis/omgevingsgeluid. In de voorbereidende fase zijn stemfragmenten van de aantoonplichtige op het politiebureau in een voice-model vastgelegd. Op het voice-model staan derhalve geen achtergrondgeluiden. Tijdens het telefonische gesprek met de voetbalsupporter zijn vaak wel achtergrondgeluiden te horen.

De vraag of de speaker recognition zal slagen en de kans op vervorming van de stem door omgevingsgeluid, is afhankelijk van de locatie waar de aantoonplichtige zich bevindt.[114] Bij de aantoonplicht kan men echter van de supporter

111 Speaker recognition kan ook plaatsvinden door middel van *speaker identification*, daarbij vindt een '1 op n vergelijking' plaats. De stem die men tijdens het telefoongesprek verkrijgt, wordt in dat geval opgespoord in een database met templates.

112 Die preventieve maatregelen kunnen bestaan uit (extra) toezicht in het verboden gebied of bijvoorbeeld de oplegging van een nieuw stadiongebiedsverbod. Indien de supporter door de politie of stewards in het verboden gebied is aangetroffen en hij zich tevens schuldig heeft gemaakt aan een strafbaar feit, kan dit resulteren in repressieve maatregelen, doordat het Openbaar Ministerie wegens dat strafbare feit tot vervolging overgaat.

113 De mate van zekerheid varieert per vorm van biometrie. De betrouwbaarheid was enige jaren geleden te gering. Zie: Willemsen (red.) 2008, p.11 en 24; inmiddels is de techniek verbeterd.

114 Een pilot kan uitwijzen in hoeverre omgevingsgeluid de betrouwbaarheid beïnvloedt.

verwachten dat hij normaal praat en handelingen die de stemherkenning negatief (kunnen) beïnvloeden nalaat. Aan de supporter moet duidelijk worden gemaakt dat het in beginsel zijn verantwoordelijkheid is dat het systeem van een 'zuiver' stemgeluid wordt voorzien.

Een andere factor die de speaker recognition kan beïnvloeden is een slechte verbinding met en tussen de mobiele telefoon van de aantoonplichtige en het communicatienetwerk van de provider. Ook ziekte en verkoudheid kunnen de betrouwbaarheid beïnvloeden. Het is echter onduidelijk in welke mate.[115] Bij de ontwikkeling van het systeem dient rekening te worden gehouden met deze factoren, evenals met het gevaar van stemimitatie.

Voor de betrouwbaarheid is van belang dat een volwassen stem niet wezenlijk veranderd.[116] Na een operatie in de mondholte of een ingreep aan de stembanden moet er een nieuwe opname worden gemaakt. In zo'n geval is het de verantwoordelijkheid van de aantoonplichtige om de politie hierop te attenderen en te staan op het afgeven van een nieuw stemsample. Indien de voetbalsupporter tijdens de uren van het stadiongebiedsverbod het bericht krijgt dat zijn stem niet is herkend, zal hij zelf maatregelen moeten nemen om alsnog aan de aantoonplicht te voldoen. Indien het bijvoorbeeld vanwege een slechte verbinding onmogelijk is om een stemherkenningscheck uit te voeren, kan men verlangen dat de aantoonplichtige zelf terugbelt of zich meldt op een politiebureau.

3.4.2 Misbruik

Het kan zijn dat de aantoonplichtige probeert de politie om de tuin te leiden bij de controle op de naleving van het stadiongebiedsverbod. Hoe zit het bijvoorbeeld met *spoofing*? Spoofing is het risico dat iemand anders zich voordoet als de aantoonplichtige, bijvoorbeeld door het afspelen van geluidsopnamen. De techniek om een computerstem zo menselijk mogelijk over te laten komen, kan gebruikt worden om te spoofen. Ondanks dat deze techniek nog volop in ontwikkeling is, is het onwaarschijnlijk dat voetbalsupporters deze inkopen.[117]

---

115 Bij de aantoonplicht hoeft dit geen probleem op te leveren. De voetbalsupporter is namelijk gebaat bij een dergelijke plicht als alternatief voor de meldingsplicht, omdat het zijn bewegingsvrijheid veel minder beperkt.

116 Zie: http://www.security.nl/artikel/28253/Stemherkenning%3A_biometrie_op_afstand_.html.

117 Het inkopen van deze techniek is zeer prijzig.

3.4.3 Kans op fouten

Bij de speaker recognition controleert het systeem in hoeverre de informatie die het tijdens het gesprek verkrijgt, overeenkomt met de informatie die reeds is vastgelegd in het voice-model.[118] Speaker recognition/verification is gebaseerd op kansberekeningen. Bij deze manier van vergelijken zijn er altijd vier verschillende uitkomsten mogelijk. Het systeem kan de beller terecht of onterecht aanmerken als de persoon die men op naleving van het stadiongebiedsverbod controleert. Daarnaast kan het zijn dat het systeem de beller terecht of onterecht juist niet herkent als de aantoonplichtige.

Teneinde de betrouwbaarheid van de speaker recognition te bepalen, is het belangrijk om naar twee verschillende foutfrequenties te kijken, te weten de False Acceptance Rate (FAR) en de False Rejection Rate (FRR). Bij de FAR gaat het om de vraag hoe groot de kans is dat het systeem de stem van de beller onterecht herkent als de stem van de aantoonplichtige. Het gaat dan om een situatie waarin bijvoorbeeld de broer van de supporter toch als aantoonplichtige wordt aangemerkt. Bij de FRR gaat het om de kans dat het systeem de stem van de beller juist ten onrechte niet als die van de supporter herkent.

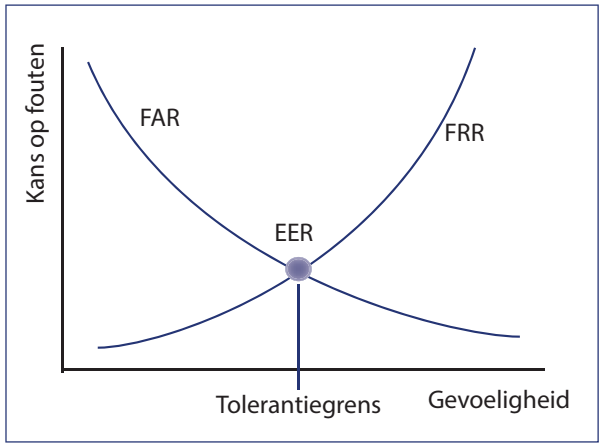
Bij het testen van het systeem moet worden gekeken naar wat acceptabele percentages onterechte herkenningen en onterechte afwijzingen zijn. Belangrijk is dat beide foutfrequenties sterk van elkaar afhankelijk zijn. Het verminderen van de FAR vergroot de FRR. Voor het ontwikkelen van een efficiënt systeem kan worden gekeken naar de Equal Error Rate (EER). De EER is het punt waarop de FAR en de FRR aan elkaar gelijk zijn. Een aantal jaren geleden had men systemen waarbij de EER 7 procent was. Inmiddels zijn er systemen beschikbaar die een EER van 3 procent laten zien.[119] Ter illustratie is in figuur 3.3 de verhouding tussen de FAR en de FRR weergegeven.

Ruifrok heeft een aantal eigenschappen geformuleerd waaraan een ideaal biometrisch systeem voldoet.[120] Een van die eigenschappen is dat de foutkans

118 Bij de aantoonplicht vindt in beginsel slechts een een-op-een vergelijking plaats. Het voicemodel wordt immers vergeleken met het stemgeluid dat tijdens het telefoongesprek met de aantoonplichtige wordt verkregen. Een een-op-een vergelijking is mogelijk doordat het voicemodel samen met het telefoonnummer gekoppeld is aan een bepaald identificatienummer.

119 De technologie is nog niet zo ver dat een EER onder de 3 procent haalbaar is.

120 Ruifrok 2006, p. 82. Zie voor de twaalf aandachts- en uitgangspunten voor zinvol en veilig gebruik van biometrie, Grijpink 2009, p. 276 en Nederlands Biometrie Forum 2009.



Figuur 3.3: Foutfrequenties

minimaal is.[121] Dat betekent dat men het systeem zo moet instellen, dat het percentage EER zo laag mogelijk is.[122] Uiteraard bestaat een ideaal systeem niet, maar bij de ontwikkeling van de digitale aantoonplicht dient men met deze eigenschappen rekening te houden.[123]

Een kleine kans op fouten of misbruik is te overzien. De kans op fouten hangt onder meer af van de kwaliteit van de speaker recognition, welke weer wordt beïnvloed dedoor duur van de speaker verification. Om de kwaliteit van de speaker recognition te waarborgen, dient er minimaal één à anderhalve minuut een gesprek met de aantoonplichtige plaats te vinden.[124]

---

121 Andere eigenschappen van een ideaal biometrisch systeem zijn volgens Ruifrok dat het systeem gebruiksvriendelijk, goed bestand tegen misleiding en fraude en sociaal geaccepteerd is. Daarnaast zijn de kosten die met het systeem zijn gemoeid laag en heeft het systeem een snelle authenticatie. De kosten van een dergelijk systeem gaan met name zitten in het ontwikkelen van een systeem dat maatwerk kan leveren. Bijlage 1 Expertmeetings, gespreksnotitie KLPD Driebergen. Het KLPD gebruikt software van Agnitio.

122 Opgemerkt dient te worden dat men met deze statistische berekening de meest optimale situatie bereikt, terwijl er altijd factoren zijn die men niet onder controle heeft. Denk hierbij aan factoren als het communicatienetwerk van de provider en omgevingsgeluiden.

123 Ook Ruifrok wijst erop dat geen enkel systeem over alle deze eigenschappen beschikt.

124 Een gespreksduur van ongeveer zeven à tien seconden kan genoeg zijn, maar uit onderzoek en de ervaringen van het KLPD blijkt dat de kwaliteit bij een gesprek van minimaal één minuut hoger is. Zie: bijlage 1 Expertmeetings, gespreksnotitie KLPD, http://www.itl.nist.gov/iad/mig//tests/sre/2010/index.html en http://www.nist.gov/itl/iad/mig/sre10results.cfm.

3.5 End of the day

De aantoonplichtige kan voorafgaand aan, tijdens en na afloop van de wedstrijd door het systeem worden gebeld. Hoe vaak het systeem de supporter belt, is mede afhankelijk van de vraag of deze in het verleden een gebiedsverbod al dan niet goed heeft nageleefd.

Indien personen herhaaldelijk een stadiongebiedsverbod hebben overtreden, ligt het voor de hand deze personen extra goed te controleren. Dat is niet noodzakelijk bij voetbalsupporters waarvan duidelijk is dat zij een opgelegd verbod correct naleven. Bij hen kan worden volstaan met het op een willekeurig tijdstip eenmalig uitvoeren van de digitale surveillance en de speaker recognition. Op deze manier wordt rekening gehouden met het privacyrecht van de betrokkene en hoeft er alleen een extra controle plaats te vinden als dat noodzakelijk is.

Welke personen het stadiongebiedsverbod hebben nageleefd en welke personen het verbod hebben overtreden, blijkt uiteindelijk uit een schematisch overzicht dat aan het einde van de dag wordt verkregen en waarvan een politieambtenaar een uitdraai kan maken. Het systeem geeft, na het uitvoeren van de digitale surveillance en de stemherkenningscheck bij identificatienummer X, op een duidelijke manier voor de eindgebruiker aan of de uitkomst positief of negatief is. Tabel 3.1 is ter illustratie opgenomen.

Tabel 3.1: Uitdraai aan het eind van de dag

ID-nummer	Gebieds-code	Stemherkenning	Over Sms	Driehoeksmeting/ gps-tracking	Uitkomst
0101	2	✓	✓	✓	✓
0102	1	✓	F3	✓	✓
0105	2	F1	✓	✓	Beller onjuist
0106	1	✓	✓	✓	✓
0107	1	✓	F2	F4	Verboden gebied
01012	3	F1	✓	✓	Geen verbinding

De gebiedscode staat voor een bepaald gedeelte van het grondgebied van de gemeente waar het de supporter verboden is om aanwezig te zijn. Gebiedscode 1 kan bijvoorbeeld zijn het stadion en/of het gebied rondom het stadion en gebiedscode 2 de omgeving van het stadion en een gedeelte van de binnenstad. Door een gebiedscode in het systeem in te voeren, kan per identificatienummer worden gecontroleerd of de supporter zich niet in het voor hem verboden grondgebied van de gemeente bevindt.

Indien blijkt dat de stemherkenning negatief is of dat de digitale surveillance een negatief resultaat geeft, zal het systeem dit aangeven door bij het gecontroleerde tijdstip een bepaalde foutcode neer te zetten. De foutcode F1 kan staan voor een negatieve stemherkenning, F2 voor een Cell-ID van een gsm-mast die in het verboden gebied staat en F3 voor een Cell-ID waarbij in verband met twijfel een nadere lokalisatie plaats moet vinden. De code F4 kan staan voor een bij de driehoeksmeting of GPS-tracking negatief verkregen resultaat. Het systeem kan bovendien zo worden ingesteld, dat het bij signalering van bepaalde foutcodes direct een signaal afgeeft. Hierdoor kunnen maatregelen worden getroffen om een voetbalgerelateerde verstoring van de openbare orde te voorkomen.

Uit tabel 3.1 valt af te leiden dat de persoon aan wie identificatienummer 0107 is toegekend het stadiongebiedsverbod niet heeft nageleefd en dat de telefoon van identificatienummer 0105 is opgenomen door een ander dan de aantoonplichtige. Na een dergelijke overtreding zou de burgemeester een sanctie moeten kunnen opleggen.

3.6 Concluderende opmerkingen

Er zijn verschillende manieren denkbaar om de problemen met de meldingsplicht op te lossen. In dit hoofdstuk is als alternatief een digitale aantoonplicht geïntroduceerd, waarmee de politie kan controleren of een voetbalsupporter het aan hem opgelegde stadiongebiedsverbod naleeft. Een speciaal voor de aantoonplicht ontwikkeld systeem zal de aantoonplichtige op willekeurige tijdstippen voor aanvang, tijdens en/of na afloop van de voetbalwedstrijd bellen. Vervolgens vindt er een digitale surveillance en een stemherkenningscheck plaats.

Ten aanzien van de uitvoering van de digitale aantoonplicht zijn drie verschillende fasen te onderscheiden. De eerste fase is de voorbereidende fase, waarbij de politie de voor de digitale surveillance en de speaker recognition benodigde gegevens verzamelt.

In de tweede fase vindt een digitale surveillance plaats. Hiermee kan de politie op afstand vaststellen dat de verbannen voetbalsupporter zich niet in het verboden gebied bevindt. Er zijn verschillende manieren denkbaar om digitaal te surveilleren. Uit het onderzoek is gebleken dat de politie het beste gebruik kan maken van gps en een speciaal voor de digitale aantoonplicht ontwikkelde app. De aantoonplichtige moet de app op zijn telefoon installeren. Op de dag van de voetbalwedstrijd ontvangt hij een sms-bericht, waarin staat dat hij zich moet

melden. Wanneer de supporter zich vervolgens aanmeldt, zorgt het programma ervoor dat de gsm-mast waarmee zijn telefoon via gps in verbinding staat, een Cell-ID opstuurt.

Tijdens de laatste fase vindt er een speaker recognition plaats. Het verrichten van een dergelijke check is noodzakelijk om vast te stellen dat het daadwerkelijk de aantoonplichtige is die de politie op naleving van het stadiongebiedsverbod controleert.

Geconcludeerd kan worden dat een digitale aantoonplicht technisch gezien goed haalbaar is. Het systeem kan zo worden ingericht, dat aan de gebruikerskant slechts zichtbaar is of het systeem al dan niet ten aanzien van een bepaald identificatienummer geheel heeft kunnen draaien. Zo blijft de privacy van de aantoonplichtige gewaarborgd.

4

Het recht op privacy en de digitale aantoonplicht

4.1 Inleiding

Een digitale aantoonplicht kan enkele van de geconstateerde nadelen van de meldingsplicht van artikel 172a Gemw ondervangen. De bevoegdheid om een digitale aantoonplicht op te leggen kan in de Gemw worden neergelegd.[125] Met de herziening van artikel 172a Gemw zullen waarschijnlijk enige jaren gemoeid zijn, het gaat per slot van rekening om een complex en politiek gevoelig onderwerp. De aantoonplicht zou daarom wellicht ook in een plaatselijke verordening kunnen worden opgenomen. Invoering op gemeentelijk niveau gaat niet alleen sneller, maar is ook goedkoper dan het bewandelen van de weg van een formele wet.

Om die reden doen we in dit hoofdstuk onderzoek naar de vraag of de bevoegdheid om een digitale aantoonplicht op te leggen in een verordening kan worden neergelegd. In veel gemeenten biedt de Algemene Plaatselijke Verordening (APV) al jaren de mogelijkheid tot het opleggen van een gebiedsontzegging, stadionomgevingsverbod of samenscholingsverbod (dit laatste weliswaar onder andere, soms strengere voorwaarden).[126] Deze verordening zou eventueel uitgebouwd kunnen worden tot een heuse Voetbalverordening, maar een zodanige operatie valt buiten het bestek van dit onderzoek.

Met de komst van de Wet mbveo heeft een aantal gemeenten de bestaande verordening die het opleggen van een gebiedsverbod mogelijk maakte ingetrokken. Uit onderzoek van de Inspectie OOV blijkt dat een deel van de gemeenten waar de verordening nog van kracht is, vanwege de beperkt mogelijke inzetbaarheid van artikel 172a Gemw weer terugvalt op de bevoegdheden uit de APV.

De toepassingsvoorwaarden in de bepaling in de APV zijn minder streng dan artikel 172a Gemw. Een eenmalige verstoring van de openbare orde is voldoen-

125 Inmiddels is een herziening van artikel 172a Gemw aangekondigd.

126 Evaluatierapport Inspectie OOV 2011, p. 8, 9, 13, 39 en 41. Een aantal gemeenten heeft een stadionomgevingsverbod uit de APV gecombineerd met een meldingsplicht uit artikel 172a Gemw. Evaluatierapport Inspectie OOV 2011, p. 37.

de om een stadiongebiedsverbod op te leggen. Dat is een voordeel, want de burgemeester kan dan in een eerder stadium een ordemaatregel nemen.

Indien de burgemeester een voetbalsupporter een stadiongebiedsverbod oplegt, zou hij tevens aan deze persoon een digitale aantoonplicht moeten kunnen opleggen. Of dat juridisch mogelijk is op het niveau van een lokale verordening, hangt met name af van de ruimte die het recht op privacy biedt. In dit hoofdstuk staat derhalve de juridische toelaatbaarheid van de aantoonplicht met het oog op het privacyrecht centraal. Hoe verhoudt die plicht zich tot dat fundamentele recht?

Paragraaf twee zet in het kort het recht op privacy uiteen, zoals dat is neergelegd in artikel 10 Grondwet (Gw) en artikel 8 EVRM. Daarna wordt in paragraaf drie onderzocht of het mogelijk is om in een autonome verordening een aantoonplicht op te nemen. Paragraaf vier sluit dit hoofdstuk af met een aantal concluderende opmerkingen.

4.2 Het recht op privacy

Privacy komt in een tijdperk waarin informatie- en communicatietechnologie zich snel ontwikkelen steeds meer onder druk te staan. Privacy is een ruim begrip en er zijn talrijke handelingen die dit recht beïnvloeden. Het begrip leent zich daardoor niet voor het geven van een uitputtende definitie.[127]

In de literatuur wordt het recht op privacy onderverdeeld in vier groepen, te weten een recht op ruimtelijke privacy, relationele privacy, lichamelijke integriteit en informationele privacy.[128] Voor de inrichting en uitvoering van de aantoonplicht is de informationele privacy van belang.

Informationele privacy heeft betrekking op het verrichten van diverse handelingen met persoonlijke informatie en de invloed die personen op de verwerking van dergelijke gegevens kunnen uitoefenen. Volgens Borking gaat het om alle persoonsgegevens, ook als deze niet rechtstreeks uit de privésfeer afkomstig zijn.[129]

127 Zie voor de term 'privéleven' uit artikel 8 EVRM onder meer EHRM 17 juli 2003, no. 44787/98 (P.G. and J.H. v. the United Kingdom) paragraaf 56, EHRM 17 juli 2003, no. 63737/00 (Perry v. the United Kingdom), paragraaf 36.

128 Zie: Terstegge 2000, p. 14 en 15, Terstegge, De Vries, Reinders & Van der Helm 2001, p. 10 en 11, Holvast 2004, p. 11 e.v., Berkvens & Prins 2007, p. 8 en Borking 2010, p. 21.

129 Borking 2010, p. 21.

Artikel 10 Gw waarborgt het privacyrecht van burgers. Het eerste lid van dit artikel omvat het klassieke grondrecht op eerbiediging van de persoonlijke levenssfeer. Ten aanzien van informationele privacy is het sociale grondrecht uit het tweede en derde lid van dit artikel van belang. In het tweede lid heeft de grondwetgever een niet afdwingbare instructienorm voor de wetgever opgenomen, inhoudende dat hij regels stelt over het vastleggen en verstrekken van persoonsgegevens. In het derde lid is een vergelijkbare norm opgenomen voor het inzage- en correctierecht.[130]

Artikel 8 EVRM waarborgt eveneens het recht op respect voor het privéleven, het familie- of gezinsleven, de woning en correspondentie. Voor de digitale aantoonplicht is het recht op respect voor het privéleven van belang. Artikel 8 EVRM is een verdragsbepaling die als zodanig geldt in de Nederlandse rechtsorde en bijna altijd door de rechter kan worden toegepast.[131]

De verwerking van persoonsgegevens valt zowel onder het toepassingsbereik van artikel 10 Gw als artikel 8 EVRM. Voor de vraag of er al dan niet sprake is van een legitieme beperking van het recht op privacy dient men artikel 10 Gw in samenhang met artikel 8 EVRM te bezien en zich aan de daarbij door het EHRM gegeven interpretatie te houden.[132] Artikel 8 EVRM en de jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) hebben een aanvullende werking op artikel 10 Gw. Een beperking van het privacyrecht is derhalve pas legitiem, indien deze bij wet is voorzien, een legitiem doel nastreeft en noodzakelijk is in een democratische samenleving.

---

130 De Staatscommissie Grondrechten in het digitale tijdperk adviseerde om bij de instructienorm niet meer te spreken van 'het vastleggen en verstrekken', maar van 'het verwerken van persoonsgegevens'. Hiermee wordt aangesloten bij de terminologie van de Wet bescherming persoonsgegevens. De Staatscommissie stelde ten aanzien van het derde lid van artikel 10 Gw voor om de daar genoemde aanspraken uit te breiden met een recht op verwijdering van verwerkte gegevens en, onder omstandigheden, het recht van verzet. Zie: Commissie Grondrechten in het digitale tijdperk 2000, p. 131-133. Het kabinet zag weinig meerwaarde in deze voorstellen; zie: Kamerstukken II 2011/12, 31 570, nr. 20, p. 8. In de Eerste Kamer wordt door verscheidene Kamerleden toch gewezen op een eventuele wijziging van artikel 10 Gw; zie: Kamerstukken II 2011/12, 31 570, nr. 22, p. 20 en Handelingen I 2011/12, nr. 18, 3, p. 21. In 2010 heeft de Staatscommissie Grondwet voorstellen gedaan om het huidige artikel 10 Gw aan te passen. Zie: Rapport Staatscommissie Grondwet 2010, Kamerstukken I 2011/12, 31 570, nr. A (bijlage).

131 Burgers kunnen derhalve voor de Nederlandse rechter een beroep doen op artikel 8 EVRM.

132 Zie: HR 9 januari 1987, AB 1987, 231 m. nt. F.H. Burg, r.o. 4.4.

4.3 Een aantoonplicht bij autonome verordening

Ten aanzien van het vereiste dat een beperking bij wet moet zijn voorzien, bestaat tussen artikel 10 Gw en artikel 8 EVRM een belangrijk verschil. Beide artikelen eisen dat de mogelijkheid om het privacyrecht te beperken een basis moet hebben in het (nationale) recht, maar het begrip 'wet' in artikel 10 Gw dient uitgelegd te worden als een wet in formele zin. 'Wet' in artikel 8 EVRM kan daarentegen ook lagere regelgeving inhouden en zelfs door de rechter ontwikkelde rechtsregels kunnen een basis bieden om het recht op privacy te beperken.[133]

Vanuit het Europese recht gezien, behoort een digitale aantoonplicht op het niveau van een plaatselijke verordening derhalve tot de mogelijkheden.[134] Volgens artikel 10 Gw is dat geen vanzelfsprekendheid.[135] Daaruit volgt namelijk dat alleen bij of krachtens formele wet beperkingen aan het privacyrecht mogen worden gesteld. Dit betekent dat er een formele wet moet bestaan waarin de beperking is opgenomen of een formele wet waarin de mogelijkheid om het privacyrecht te beperken aan een lagere regelgever wordt gedelegeerd.[136]

Daarvan is geen sprake bij een digitale aantoonplicht voor voetbalsupporters in een lokale verordening. De gemeenteraad is op basis van artikel 149 van de Gemw bevoegd om verordeningen vast te stellen. Het betreft hier weliswaar een formeel wettelijke bepaling, maar dit artikel kan niet als formeel wettelijke grondslag voor de beperking van het privacyrecht dienen. Daarvoor is de bepaling te algemeen geformuleerd.

In de rechtspraak is reeds lange tijd duidelijk dat een (autonome) gemeentelijke verordening de persoonlijke levenssfeer niet zomaar kan beperken. In 1996 doet de Afdeling Bestuursrechtspraak van de Raad van State (ABRvS) een belangwekkende uitspraak in dezen. De burgemeester van Venlo legt in 1993 op grond van een verordening aan een inwoner met onmiddellijke ingang voor de duur van drie maanden een bezoekersverbod op. De ABRvS bevestigt het oor-

133 EHRM 26 april 1979 (*Sunday Times* v. the United Kingdom).

134 Daarvoor is uiteraard wel vereist dat de aantoonplicht aan overige voorwaarden voor het legitiem beperken van het privacyrecht voldoet.

135 Zie: Burkens, Kummeling, Vermeulen & Widdershoven 2012.

136 Wanneer de bevoegdheid om een gebiedsverbod te combineren met een digitale aantoonplicht in een formele wetsbepaling wordt opgenomen, speelt deze vraag niet. Immers voor het beperken van het privacyrecht van de betrokkene bestaat in dat geval een formeel wettelijke grondslag.

deel van de Rechtbank Roermond dat een beperking van het privacyrecht op grond van de APV in strijd is met artikel 10 Gw. Een zodanig vergaande beperking dient een formeel wettelijke grondslag te hebben.[137]

Is een (digitale) aantoonplicht op basis van een plaatselijke verordening per definitie dan ook een beperking van het privacyrecht die niet is toegestaan? In de rechtspraak wordt een uitzondering op de door de grondwetgever aangebrachte beperkingensystematiek toegelaten. Herhaaldelijk hebben rechters geringe inbreuken op het privacyrecht zonder (specifieke) formeel wettelijke grondslag aanvaard.[138]

De Hoge Raad heeft in zijn strafrechtelijke jurisprudentie bijvoorbeeld een vaste lijn ontwikkeld dat bij een geringe inbreuk een algemene wettelijke regeling volstaat.[139] De Rechtbank Arnhem ging nog een stapje verder door te beslissen dat het gebruik van stealth sms-berichten slechts een geringe inbreuk op het privacyrecht oplevert en derhalve is toegestaan als een specifieke wettelijke basis ontbreekt.[140]

Ook in de rechtspraak van de ABRvS lijkt er ruimte te bestaan voor geringe inbreuken op het privacyrecht. In de eerder genoemde uitspraak over het bezoekersverbod overweegt de ABRvS dat 'een geslotenverklaring van een woning als bedoeld in artikel 35b eerste lid van de verordening een beperking [vormt] van het recht, bedoeld in artikel 10 eerste lid Gw. Een dergelijke beperking is […] slechts toegestaan op basis van een wet in formele zin'.[141] Het gebruiken van het woord 'dergelijke' wijst erop dat ook de ABRvS niet elke beperking zonder specifieke formeel wettelijke grondslag strijdig oordeelt met artikel 10 Gw.

4.3.1 *Geringe-inbreuktoets*

Geringe inbreuken op artikel 10 Gw worden in de rechtspraak gesauveerd met als argument dat het slechts een onbetekenende inbreuk op het grondrecht vormt. Dat maakt de vraag wanneer er sprake is van een geringe inbreuk uiterst

137 ABRvS 28 augustus 1995, AB 1996, 204, r.o. 2.

138 Zie: Brouwer en Vols 2010.

139 Veel jurisprudentie heeft zich bijvoorbeeld ontwikkeld met betrekking tot artikel 2 van de Polw 1993. Zie: Hof Arnhem 24 januari 2012, LJN BV3076, Rb. Amsterdam 8 maart 2011, LJN BP7233 en HR 20 januari 2009, LJN BF5603.

140 Rb. Arnhem 8 november 2011, LJN BU3688, r.o. 3.1.

141 ABRvS 28 augustus 1995, AB 1996, 204, r.o.2.

interessant. De Hoge Raad beantwoordt deze vraag met behulp van vier criteria: duur, intensiteit, plaats en doel van de inbreuk. Hoe zou deze geringe-inbreuk-toets bij de digitale aantoonplicht uitvallen?[142]

Ten aanzien van de duur van een digitale aantoonplicht is van belang dat de plicht slechts op zeer beperkte tijden geldt. Uitgangspunt is dat een stadiongebiedsverbod slechts twintig weken per jaar eenmalig per week gedurende zes uur geldt: twee uur voor aanvang van de wedstrijd, tijdens de wedstrijd en twee uur na afloop van de wedstrijd. Als een supporter voor zes wedstrijden een stadiongebiedsverbod en een aantoonplicht opgelegd krijgt, wordt hij gedurende maximaal 36 uur belast met de plicht om aan te tonen dat hij zich niet in het verboden gebied bevindt.[143]

Een aantoonplicht van zes uur per wedstrijd betekent op jaarbasis ongeveer 102 uur (zeventien thuiswedstrijden maal zes uur per wedstrijd). De verbannen supporter moet slechts gedurende de verboden tijdstippen telefonisch bereikbaar zijn. Vanwege de korte tijdsduur scoort de aantoonplicht op het criterium van de duur goed.

Bij het intensiteitscriterium gaat het erom of de aantoonplicht ook de kern raakt van het ongestoord zichzelf willen zijn. Kijkend naar de verschillende fasen van de aantoonplicht, kan worden gesteld dat de supporter gewoon ongestoord zichzelf kan zijn. Op het criterium van intensiteit scoort de aantoonplicht derhalve goed.

In hoeverre de aantoonplichtige ongestoord zichzelf kan zijn terwijl hij op afstand op de naleving van het stadiongebiedsverbod wordt gecontroleerd, hangt vanzelfsprekend wel af van de manier waarop de politie digitaal surveilleert. Het systeem dient zodanig te worden ingericht dat politieambtenaren niet (kunnen) weten waar de supporter zich bevindt. Een politiefunctionaris wordt daarop slechts geattendeerd wanneer onmiskenbaar vaststaat dat de aantoonplichtige zich daadwerkelijk in het verboden gebied ophoudt.

Bij het plaatscriterium gaat het erom wat het karakter is van de plaats die inbreuk op het privacyrecht van de voetbalsupporter maakt. Bij een digitale aantoonplicht kan een betrokkene in beginsel op elke willekeurige plaats wor-

142 Brouwer en Vols passen deze toets onder meer toe op een autonome verordening waarin de gemeenteraad een verbod wil geven op het stoken van hout en kolen in woonschepen. Zie: Brouwer en Vols 2010.

143 Een stadiongebiedsverbod in een verordening voor zes wedstrijden staat gelijk aan een verbod van drie maanden op grond van de Wet mbveo. Er is gekozen voor een verbod van zes wedstrijden om ervoor te zorgen dat een supporter ook met de winter- en zomerstop, interlandwedstrijden of een eventuele wijziging in het wedstrijdprogramma effectief door het verbod wordt getroffen.

den gebeld en dit wordt in het algemeen niet gezien als een meer dan geringe inbreuk op iemands privacy. Dit criterium zal bij de digitale aantoonplicht geen probleem opleveren.

De aantoonplicht scoort ten slotte ook wat betreft het doel van de inbreuk goed. De aantoonplicht dient een publiek belang en heeft niet als doel zich te mengen in de particuliere sfeer. Het beoogt immers slechts naleving van het stadiongebiedsverbod te bewerkstelligen, teneinde voetbalgerelateerde verstoringen van de openbare orde te voorkomen. Er wordt een maatschappelijk ongewenst verschijnsel bestreden.

Op grond van het bovenstaande kan worden geconcludeerd dat er bij een digitale aantoonplicht sprake is van een geringe inbreuk op het privacyrecht. Opname van een aantoonplicht in een plaatselijke verordening is denkbaar, mits dit aan alle overige vereisten van artikel 8 EVRM en de daarop berustende privacywetgeving voldoet.

4.3.2 *Eisen artikel 8 EVRM*

Met de vaststelling dat het opnemen van een aantoonplicht in een lokale verordening slechts een geringe inbreuk is op artikel 10 van de Gw, is nog niet gezegd dat een dergelijke plicht ook daadwerkelijk kan worden ingevoerd. Ook artikel 8 EVRM stelt eisen aan de opname van de aantoonplicht in een verordening.

Allereerst is vereist dat de beperking bij wet is voorzien. Inmiddels is duidelijk dat een verordening als rechtsbasis voor de beperking van het recht op privacy kan dienen. Dat de beperking een basis in nationaal recht heeft, betekent echter nog niet dat de beperking ook bij wet is voorzien. Volgens vaste jurisprudentie van het EHRM moet de rechtsbasis aan een aantal bijkomende eisen voldoen. De rechtsbasis dient van een bepaalde kwaliteit te zijn, zodat wordt voldaan aan de eisen die voortvloeien uit de 'rule of law'. Vereist is dat de rechtsbasis voldoende toegankelijk (*accessible*) en voorzienbaar (*foreseeable*) is.[144]

De rechtsbasis is voldoende accessible als het voor de burger mogelijk is om kennis te nemen van de toepasselijke regelgeving en foreseeable als de wet voldoende nauwkeurig is geformuleerd. Voor de burger moet kenbaar zijn onder

144 Henrard 2008, p. 197, EHRM 24 april 1990 (Kruslin), NJ 1991, 523, paragraaf 27, EHRM 2 augustus 1984 (Malone), NJ 1988, 534, paragraaf 67en EHRM 12 januari 2010, no. 4158/05, paragraaf 76.

welke omstandigheden zijn privacyrecht kan worden beperkt en hij moet de gevolgen van zijn handelen kunnen voorzien. Wil het recht aan deze eis voldoen, dan moet het bescherming bieden tegen willekeurige inmengingen en de omvang en wijze van uitoefening van de bevoegdheid voldoende duidelijk aangeven.[145]

Bij de digitale aantoonplicht kunnen supporters van de bevoegdheid om een stadiongebiedsverbod gecombineerd met een digitale aantoonplicht op te leggen kennis nemen. Het betreft namelijk een algemeen verbindend voorschrift en dit wordt bekendgemaakt in het gemeenteblad of, bij gebreke daarvan, door bijvoorbeeld ter inzage legging op het gemeentehuis of plaatsing in een dag-, nieuws- of huis-aan-huisblad.[146] Bovendien heeft een gemeente de plicht alle verordeningen via haar website digitaal beschikbaar te stellen.

Uit een toelichting op het stadiongebiedsverbod en de aantoonplicht zal duidelijk worden op welke wijze de aantoonplicht werkt en onder welke omstandigheden het privacyrecht van de supporter beperkt kan worden. Verder is controle in een bezwaarschriftprocedure en daarna door een onafhankelijke en onpartijdige rechter mogelijk.[147] De digitale aantoonplicht is daarmee voldoende accessible en foreseeable.

Artikel 8 EVRM eist voorts dat de beperking een legitiem doel nastreeft. De burgemeester legt een digitale aantoonplicht op met als doel het voorkomen van wanordelijkheden en strafbare feiten. De aantoonplicht dient derhalve een legitiem doel.

Een beperking van het privacyrecht moet ten slotte noodzakelijk zijn in een democratische samenleving.[148] Daarvan is sprake indien aan de vereisten van geschiktheid, subsidiariteit en proportionaliteit wordt voldaan. Een digitale aantoonplicht is geschikt om het doel van het voorkomen van wanordelijkheden en strafbare feiten te verwezenlijken.

Er zijn voor zover bekend geen minder ingrijpende alternatieve manieren om dit doel te realiseren. De fysieke meldingsplicht van artikel 172a Gemw

145 EHRM 26 april 1979 (*Sunday Times* v. the United Kingdom), paragrafen 47-49, EHRM 2 augustus 1984 (Malone), NJ 1988, 534, paragraaf 66 en EHRM 17 februari 2004 (Maestri v. Italy), paragraaf 30.

146 Zie: artikel 139 lid 2 Gemw.

147 De bestuursrechtelijke rechtsbescherming biedt voldoende waarborgen tegen misbruik.

148 Doorgaans komt de nationale overheid een 'margin of appreciation' toe, aangezien zij beter in staat is om de situatie in het land en de belangen van het land te beoordelen. De 'margin of appreciation' is echter niet absoluut. Een beperking van het privacyrecht dient namelijk altijd proportioneel te zijn.

zien wij, evenals de digitale meldzuil,[149] als een ingrijpender middel.[150] Een nalevingscontrole op afstand door middel van speaker recognition en een digitale surveillance is naar onze mening het minst ingrijpende middel.

Voor de invoering bestaat bovendien een dringende maatschappelijke behoefte. De bevoegdheden om een stadiongebiedsverbod en een digitale aantoonplicht op te leggen zijn tot stand gekomen, omdat de bevoegdheden van artikel 172a Gemw ontoereikend zijn om voetbalvandalisme effectief te bestrijden. In de praktijk bestaat behoefte aan werkbare alternatieven en voor de invoering van digitale aantoonplicht bestaan relevante en voldoende redenen.

Het antwoord op de vraag of een combinatie van een stadiongebiedsverbod met een digitale aantoonplicht proportioneel is, hangt af van de omstandigheden van het geval. De omvang en de duur van de aantoonplicht zijn in abstracto beperkt en een afgeleide van de zwaarte van de verstoring van de openbare orde. Bij de uitoefening van de bevoegdheden blijkt pas werkelijk of de opgelegde aantoonplicht proportioneel is. Wel dienen op voorhand in verband met de proportionaliteit waarborgen te worden opgenomen.

De burgemeester kan een digitale aantoonplicht alleen in combinatie met een gebiedsontzegging opleggen. Toepassingsvoorwaarde is een eenmalige voetbalgerelateerde verstoring van de openbare orde. De burgemeester dient op basis van feiten en omstandigheden de noodzaak van een stadiongebiedsverbod en een aantoonplicht te bewijzen. Dat betekent dat hij concrete aanwijzingen moet hebben dat de supporter de openbare orde voetbalgerelateerd heeft verstoord.

Het gebied dat de burgemeester als verboden aanwijst, moet zich kenmerken door een aanzienlijk risico op voetbalgerelateerde verstoringen van de openbare orde. Bovendien mag het gebied niet groter zijn en mogen het verblijfsverbod en de aantoonplicht niet langer duren dan strikt noodzakelijk is voor de handhaving van de openbare orde.[151] De maximale geldigheidsduur van beide gedragsaanwijzingen is beperkt.[152] De burgemeester richt de aantoonplicht op zodanige wijze in dat die de betrokkene zo min mogelijk belast. De supporter geniet uiteraard gewoon bestuursrechtelijke rechtsbescherming.

---

149 De regiopolitie Twente experimenteert met een digitale meldzuil waarbij gebruik wordt gemaakt van gezichtsherkenning. Het betreft een pilot van het Openbaar Ministerie en de Dienst Justitiële Inlichtingen.

150 De VNG stelt voor om te kijken of een enkelband nuttig kan zijn voor handhaving van het stadiongebiedsverbod.

151 Zie ook Rb. 's-Gravenhage 23 juli 2012, LJN BX4292, r.o. 5.4.

152 De lengte van een stadiongebiedsverbod is gekoppeld aan bepaalde categorieën van gedragingen. De aantoonplicht moet gekoppeld worden aan het stadiongebiedsverbod, zodat beide dezelfde lengte hebben.

Hierdoor is voldoende gewaarborgd dat het opleggen van de gedragsaanwijzingen noodzakelijk is, de bevoegdheden niet willekeurig zullen worden gebruikt en er een behoorlijk evenwicht bestaat tussen het legitieme doel en het privacyrecht van de supporter. Een aantoonplicht kan derhalve de privacytoets van artikel 8 EVRM goed doorstaan.

4.4 Concluderende opmerkingen

In dit hoofdstuk staat de juridische toelaatbaarheid van een digitale aantoonplicht in een verordening centraal. Hoe verhoudt deze zich tot het recht op privacy? Of een dergelijke plicht kan worden ingevoerd in een verordening, hangt met name af van de ruimte die artikel 10 Gw en artikel 8 EVRM bieden.

Uit het onderzoek blijkt dat een aantoonplicht bij autonome verordening tot de mogelijkheden behoort. Bij de digitale aantoonplicht is er slechts sprake van een geringe inbreuk op het privacyrecht van de voetbalsupporter en in de rechtspraak wordt in dat geval een uitzondering op de door de grondwetgever aangebrachte beperkingensystematiek toegelaten. Een digitale aantoonplicht kan bovendien de privacytoets van artikel 8 EVRM doorstaan. Opname van een aantoonplicht in een plaatselijke verordening is derhalve denkbaar.

Ook het opleggen van een langdurig verblijfsverbod levert geen probleem op, mits het stadiongebiedsverbod proportioneel is en er geen minder ingrijpende alternatieve maatregelen voorhanden zijn. Dat men een aantoonplicht in een autonome verordening kan opnemen, betekent echter nog niet dat invoering daarvan ook haalbaar is. Daarvoor is vereist dat de aantoonplicht geheel in overeenstemming is met de privacywetgeving. In het volgende hoofdstuk wordt derhalve ingegaan op de Wbp en de Wpg.

5

De Wet bescherming persoonsgegevens

5.1 Inleiding

In het vorige hoofdstuk is duidelijk geworden dat grondwettelijke bescherming van het recht op privacy geen beletsel is om een digitale aantoonplicht in een autonome verordening op te nemen. Dit betekent niet dat er geen andere obstakels zijn die de invoering van een dergelijke plicht in de weg staan. Bij een digitale aantoonplicht wordt onder meer gebruikgemaakt van privacygevoelige informatie. Wanneer voor de uitvoering persoonsgegevens nodig zijn, moet de aantoonplicht aan de vereisten van de privacywetgeving voldoen. Alleen dan is de verwerking van die gegevens geoorloofd en heeft een digitale aantoonplicht kans van slagen.

In paragraaf 5.2 behandelen we de Wbp en zetten we het algemene kader van de wet uiteen. In aansluiting daarop wordt in de paragrafen 5.3 en 5.4 uitvoeriger ingegaan op de inhoud van de Wbp. Is de Wbp op de verwerking van gegevens bij de digitale aantoonplicht van toepassing en, zo ja, is er dan sprake van een geoorloofde verwerking van persoonsgegevens?

In paragraaf 5.5 besteden we aandacht aan het besluit van de burgemeester om aan een supporter een stadiongebiedsverbod in combinatie met een aantoonplicht op te leggen. Onderzocht wordt welke (inhoudelijke) eisen er gelden voor een zodanig besluit. Voor het geven van deze gedragsaanwijzingen heeft de burgemeester politiegegevens nodig. Op de verstrekking van dergelijke persoonsgegevens is niet de Wbp, maar de Wpg van toepassing. Dit maakt het noodzakelijk ook in te gaan op de Wpg.

In paragraaf 5.6 sluiten we het hoofdstuk af met een aantal concluderende opmerkingen. Vooraf roepen we nog even in herinnering dat een digitale aantoonplicht uit twee componenten bestaat: vaststellen of iemands telefoon zich niet in het verboden gebied bevindt (digitale surveillance) en vaststellen of de verbannen persoon zich in de directe nabijheid van de telefoon bevindt (stemherkenningscheck).

5.2 Bescherming van persoonsgegevens

De formele wetgever heeft met de Wet persoonsregistraties (Wpr) en later met haar vervanger de Wbp, de door de grondwetgever in artikel 10 Gw gegeven opdracht uitgevoerd. De Wbp bevat algemene regels over hoe men met de verwerking van persoonsgegevens moet omgaan, maar geeft niet expliciet aan wat al dan niet is toegestaan. Dat laatste is anders indien er bijzondere persoonsgegevens worden verwerkt. Dergelijke gevoelige gegevens mogen namelijk slechts worden verwerkt als de Wbp de verwerking daarvan toestaat.[153]

De wet kent hoofdzakelijk open normen en technologieonafhankelijke begrippen. De wetgever heeft hiervoor gekozen om ervoor te zorgen dat het begrippenkader van de Wbp minder snel zal verouderen dan dat bij de Wpr het geval was. Open normen bieden immers flexibiliteit en de mogelijkheid om (meer) maatwerk te leveren. Het nadeel is dat deze normen organisaties die persoonsgegevens (willen gaan) verwerken weinig houvast bieden. Uit onderzoek blijkt dat het begrippenapparaat van de Wbp in de praktijk moeilijk te hanteren is, aangezien de begrippen voor meerdere interpretaties vatbaar zijn.[154]

Bovendien is inmiddels gebleken dat de gesuggereerde technologieonafhankelijke normen toch (deels) techniekafhankelijk zijn. De technologische ontwikkelingen sinds de invoering van de wet leveren nogal wat knelpunten op. Bij de toepassing van biometrie loopt men bijvoorbeeld tegen de grenzen van de Wbp aan en ook het gebruik van RFID roept nieuwe privacyvragen op.[155] De ontwikkeling van de techniek gaat veel sneller dan de ontwerpers van de wet zich voorstelden.[156]

Omstandigheden en opvattingen in de rechtspraktijk en de jurisprudentie bepalen voor een groot deel de inhoud van de normen van de Wbp.[157] Bij de vraag of een bepaalde verwerking van persoonsgegevens is toegestaan, zijn de omstandigheden van het concrete geval doorslaggevend. De Wbp gaat ervan uit dat men telkens een zorgvuldige belangenafweging maakt, waarvan de uitkomst vatbaar is voor toetsing door de rechter.[158] In de publieke sector wordt

153 Winter 2009, p. 83 en Winter, De Jong, Sibma e.a. 2009, p. 35.

154 Winter, De Jong, Sibma e.a. 2009, p. 44.

155 Winter, De Jong, Sibma e.a. 2009, p. 49.

156 De wetgever is zich hiervan bewust; Kamerstukken II 1997/98, 25 892, nr. 3, p. 7.

157 Zie: Kamerstukken II 1997/98, 25 892, nr. 3, p. 15.

158 Kamerstukken II 1997/98, 25 892, nr. 3, p. 14.

die belangenafweging begrensd door de algemene beginselen van behoorlijk bestuur die het bestuursorgaan in acht moet nemen.

Naar aanleiding van vragen van Kamerleden over de (on)duidelijkheid van de materiële normen van de Wbp, heeft de minister van Justitie aan de Tweede Kamer toegezegd om voor verwerkers van persoonsgegevens een handleiding op te stellen.[159] Het College bescherming persoonsgegevens (Cbp) heeft inmiddels ook verschillende informatiebladen ontwikkeld.[160] Van die handleiding en informatiebladen is bij dit onderzoek, meer specifiek bij het zoeken van een antwoord op de vraag of en, zo ja, onder welke voorwaarden persoonsgegevens bij de aantoonplicht mogen worden verwerkt, dankbaar gebruikgemaakt.[161]

5.3 Toepasselijkheid Wbp

Voor de politie die bij de digitale aantoonplicht met de persoonsgegevens moet gaan werken, is het zeer belangrijk om te weten of de Wbp op de verwerking van die gegevens van toepassing is. Belangrijk is dat de reikwijdte van de Wbp zich niet uitstrekt tot alle gegevensverwerkingen. Volgens artikel 2 van de Wbp is de wet alleen van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en op de niet geautomatiseerde verwerking van persoonsgegevens, mits deze gegevens in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen.

Om te beoordelen of de Wbp op de gegevensverwerking bij de digitale aantoonplicht van toepassing is, moet er worden getoetst aan een drietal eisen. Vereist is dat het gegeven een persoonsgegeven is, er sprake is van een verwerking in de zin van de Wbp en dat er zich geen situatie voordoet waarin de werking van deze wet is uitgezonderd.

159 Handelingen II 1999/00, nr. 24, Kamerstukken I 1999/00, 25 892, nr. 92c, p. 26, Handelingen I 1999/00, nr. 34 en Kamerstukken I 2000/01, 25 892, nr. 200.

160 Deze informatiebladen zijn te downloaden via http://www.cbpweb.nl/Pages/ind_publ_inf.aspx.

161 Inmiddels heeft de Europese Commissie een voorstel gedaan om de Europese wetgeving over de bescherming van persoonsgegevens te herzien. Richtlijn 95/46/EG zal in dat geval door een verordening worden vervangen. Het doel van deze herziening is om duidelijke normen te creëren die ook bestand zijn tegen toekomstige en thans onvoorziene ontwikkelingen. Voor meer informatie verwijzen wij naar Hijmans 2012 en de site van het Cbp, waar ook de hoofdpunten van het voorlopig standpunt van het Cbp zijn te vinden.

5.3.1 Persoonsgegevens

Allereerst is vereist dat de bij de aantoonplicht te verwerken gegevens als persoonsgegevens zijn aan te merken. Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.[162] In de definitie van een persoonsgegeven kunnen drie verschillende elementen worden onderscheiden.[163]

Het eerste element is dat het moet gaan om 'elk gegeven'. Het woordje 'elk' geeft aan dat de Wbp zich in principe niet beperkt tot gegevens uit het privéleven van betrokkenen. Het begrip 'gegeven' dient men ruim te interpreteren. Het omvat niet alleen informatie in geschreven tekst, maar bijvoorbeeld ook beeld en geluid.[164]

Het tweede element heeft betrekking op informatie 'betreffende een natuurlijke persoon'. Of gegevens informatie bevatten over een natuurlijke persoon blijkt doorgaans uit de aard van de gegevens.[165] Een gegeven dat naar zijn aard geen betrekking heeft op een persoon, kan onder omstandigheden toch als een persoonsgegeven worden aangemerkt.[166] Daarvoor is vereist dat het gegeven de betrokkene kan identificeren. De context waarin men de gegevens gebruikt, de feitelijke situatie, is (mede) bepalend voor de vraag of het gegeven een persoonsgegeven is. Belangrijk is dat het moet gaan om gegevens die mede bepalend zijn voor de wijze waarop de betrokken persoon wordt beoordeeld of behandeld. Niet elk technisch of toevallig verband tussen een gegeven en een persoon betekent derhalve dat er sprake is van een persoonsgegeven.

Het derde element betreft het vereiste dat een persoon is geïdentificeerd of althans identificeerbaar moet zijn. Volgens de Memorie van Toelichting bij

---

162 Artikel 1 onder a Wbp. De definitie van een persoonsgegeven komt vrijwel overeen met de definities van persoonsgegevens uit de Europese Privacyrichtlijn en het Databeschermingsverdrag. Zie ook: Article 29 Data Protection Working Party 2007, p. 6.

163 The Article 29 Data Protection Working Party (een onafhankelijke advies-en overlegorgaan van Europese privacytoezichthouders) heeft een advies uitgebracht over wat wel en wat niet onder het begrip 'persoonsgegevens' valt. Zie: Article 29 Data Protection Working Party 2007. Het advies is te vinden via http://www.cbpweb.nl/downloads_int/20070710_ harmonisering _speerpunt_wp136.pdf.

164 Kranenborg & Verhey 2011, p. 60. The Article 29 Data Protection Working Party heeft aandacht besteed aan de vraag wanneer er sprake is van 'informatie betreffende een persoon'. Daarbij kan worden gekeken naar de inhoud, het doel en het resultaat. Deze voorwaarden zijn niet cumulatief. Zie: Article 29 Data Protection Working Party 2007, p. 11.

165 Kamerstukken II 1997/98, 25 892, nr. 3, p. 46 en Sauerwein & Linnemann 2002, p. 12.

166 Article 29 Data Protection Working Party 2007, p. 10.

de Wbp spelen twee factoren een rol, te weten de aard van de gegevens en de mogelijkheid om identificatie tot stand te brengen.[167] Ten aanzien van de aard van de gegevens geldt dat het moet gaan om gegevens die, alleen of in combinatie met andere gegevens, zo kenmerkend zijn voor een bepaalde persoon dat deze aan de hand daarvan kan worden geïdentificeerd. Een persoon is identificeerbaar, indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning kan worden vastgesteld.[168] Identificatie kan op vele manieren plaatsvinden.[169] Technische ontwikkelingen spelen eveneens een rol. Met moderne technieken zijn de mogelijkheden om personen zonder onevenredige inspanningen te identificeren toegenomen, waardoor bepaalde gegevens voorheen niet, maar nu wel onder het bereik van de Wbp kunnen vallen.

Naam, telefoonnummer en stemgeluid

Voor de digitale aantoonplicht worden de naam van de aantoonplichtige en diens telefoonnummer verzameld en opgeslagen in een database. Daarnaast wordt het stemgeluid van de supporter opgenomen, opgeslagen en gebruikt voor de uitvoering van de aantoonplicht. De naam van de aantoonplichtige is een gegeven dat betrekking heeft op een natuurlijke persoon, waarmee men de betrokkene met een grote mate van waarschijnlijkheid kan identificeren.[170]

Het telefoonnummer van de aantoonplichtige heeft geen betrekking op een natuurlijke persoon. Dat betekent echter niet dat het in dit geval geen persoonsgegeven betreft. In combinatie met de naam van de aantoonplichtige kan de politie namelijk zijn identiteit zonder veel omwegen vaststellen. Er is geen sprake van een disproportionele inspanning om identificatie te bewerkstelligen.

---

167 Kamerstukken II 1997/98, 25 892, nr. 3, p. 46.

168 Met moet een persoon door de toepassing van een bepaald identificatiemiddel van andere personen kunnen onderscheiden. Zie: Article 29 Data Protection Working Party 2007, p. 13, 15 en 16.

169 De Wbp gaat uit van een redelijk met middelen uitgeruste verantwoordelijke, maar houdt er eveneens rekening mee dat de verantwoordelijke ten aanzien van identificatie over bijzondere expertise kan beschikken. Bij de beoordeling of er sprake is van een persoonsgegeven dient dat laatste te worden meegewogen. Zie: Kamerstukken II 1997/98, 25 892, nr. 3, p. 49.

170 Er kan zich een situatie voordoen waarin alleen de naam onvoldoende is om de aantoonplichtige te identificeren en er meer specificerende gegevens nodig zijn om identificatie tot stand te brengen. Bij de digitale aantoonplicht wordt eveneens het telefoonnummer en het stemgeluid van de supporter afgenomen en opgeslagen. De naam van de aantoonplichtige zal in combinatie met deze gegevens derhalve altijd een identificerend gegeven opleveren.

Ook de registratie van het telefoonnummer van de aantoonplichtige moet derhalve met voldoende waarborgen zijn omgeven.

Stemgeluid is eveneens een persoonsgegeven. Het betreft in dit geval een uniek biometrisch gegeven. Biometrische gegevens geven informatie over een bepaalde persoon en kunnen derhalve als identificatiemiddel dienen.[171] Volgens Grijpink zegt een biometrisch gegeven niets over de juistheid van documenten en gegevens, noch over de juistheid van de koppeling. Daarom geeft een biometrisch gegeven geen uitsluitsel over wie iemand is. Volgens hem betreft biometrie alleen persoonsherkenning, geen identiteitsvaststelling.[172] Bij de digitale aantoonplicht kan echter door de koppeling met andere persoonsgegevens identificatie van de persoon plaatsvinden. Het voice-model is immers gekoppeld aan een identificatienummer en door raadpleging van een andere (versleutelde) database kan de politie de identiteit van de supporter achterhalen.[173] Ook bij de verwerking van stemgeluid is er dus sprake van identificerende informatie die herleidbaar is tot een natuurlijke persoon.[174]

Gegevens die verband houden met het stadiongebiedsverbod

De politie dient verder gegevens omtrent de duur van de opgelegde maatregelen, de omvang van het verboden gebied en de tijdstippen waarop het de sup-

171 OpiniArticle 29 Data Protection Working Party 2007, p. 9.

172 Grijpink 2009, p. 273. Zie ook: Nederlands Biometrie Forum 2009.

173 Teneinde de privacy van de supporter te waarborgen, worden de gegevens gekoppeld aan een identificatienummer. Het gebruik van identificatienummers heeft echter niet tot gevolg dat er niet meer kan worden gesproken van een persoonsgegeven. Het betreft slechts een beveiligingsmaatregel.

174 Onder bepaalde omstandigheden kan stemgeluid een bijzonder persoonsgegeven zijn, namelijk als men daaruit gegevens omtrent het ras, levensovertuiging of bijvoorbeeld de gezondheid van die persoon kan afleiden. Is er bij de verwerking van stemgeluid in het kader van de aantoonplicht sprake van een bijzonder persoonsgegeven? Voor beeld- en geluidmateriaal is volgens het Cbp beslissend of dit materiaal verwerkt wordt met het uitdrukkelijke doel om onderscheid naar ras, levensovertuiging e.d. te maken. De Hoge Raad besloot in 2010 echter dat een foto een bijzonder persoonsgegeven betreft, aangezien men uit die foto het ras van de betreffende persoon kan afleiden; HR 23 maart 2010, LJN BK6331. Zie ook: Gellaerts & Jobse 2011, p. 53 en 54. Naar onze mening is de verwerking van het stemgeluid bij de aantoonplicht geen verwerking van een bijzonder persoonsgegeven. Het stemgeluid van de aantoonplichtige wordt opgeslagen en gebruikt in verband met het verrichten van een speaker recognition. Het betreft een taalonafhankelijke biometrische toets op afstand, die niet als doel heeft om onderscheid te maken naar ras e.d.

porter verboden is om zich in dat gebied te bevinden, van de burgemeester te verkrijgen. Het betreft hier gegevens die geen betrekking hebben op een natuurlijke persoon, noch hem identificeren. Op deze gegevens is de Wbp derhalve niet van toepassing.

Cell-ID en locatiegegevens

Om digitaal te surveilleren kan de politie gebruikmaken van een methode waarbij zij een Cell-ID zal verkrijgen. Strikt genomen is een Cell-ID geen gegeven over een natuurlijke persoon. Het betreft immers een gegeven over een publieke zendmast. Dat betekent echter niet dat een Cell-ID geen persoonsgegeven kan zijn. Indien het gebruik van Cell-ID's aanzienlijke gevolgen heeft voor een aantoonplichtige, dan kunnen deze gegevens ook als gegevens betreffende natuurlijke personen worden beschouwd.[175] Met het verkrijgen en gebruiken van een Cell-ID kan de politie nagaan of een verbannen supporter zich aan het stadiongebiedsverbod houdt. Of het hier een 'aanzienlijk' gevolg betreft, moet betwijfeld worden. Echter, in combinatie met de overige gegevens kan identificatie plaatsvinden. Derhalve is een Cell-ID ook een persoonsgegeven.

5.3.2 *Verwerking in de zin van de Wbp*

Nu is vastgesteld dat een deel van de voor de uitvoering van de aantoonplicht benodigde gegevens persoonsgegevens zijn, moet worden onderzocht of er sprake is van een verwerking in de zin van de Wbp. Onder 'verwerking' verstaat de Wbp elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Als voorbeelden worden genoemd het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Het betreft hier een niet-limitatieve opsomming.[176] Elke handeling met persoonsgegevens kan dus een verwerking van persoonsgegevens inhouden. Doorslaggevend is of men

175 Zie: Article 29 Data Protection Working Party 2007, p. 12.

176 Artikel 1 onder b Wbp en Kamerstukken II 1997/98, 25 892, nr. 3, p. 51.

enige feitelijke macht of invloed, al dan niet via een geautomatiseerd systeem, over de gegevens kan uitoefenen.[177] Daarbij is het irrelevant of men die invloed ook daadwerkelijk uitoefent.[178]

De Wbp vindt toepassing, indien een systeem persoonsgegevens geheel of gedeeltelijk verwerkt. Een handmatige gegevensverwerking kan eveneens onder het bereik van de Wbp vallen. Daarvoor is vereist dat de gegevens in een bestand zijn vastgelegd of bestemd zijn om in een bestand te worden opgenomen.[179]

Bij de digitale aantoonplicht worden de benodigde gegevens vastgelegd, bewaard en gebruikt voor de controle op de naleving van het stadiongebiedsverbod. De gegevens zullen handmatig door een politieambtenaar in het systeem worden ingevoerd. Voor het overige is de gegevensverwerking vrijwel geheel geautomatiseerd. Bovendien kan de politie enige feitelijke macht of invloed over de gegevens uitoefenen. Hierdoor is er bij de digitale aantoonplicht duidelijk sprake van een verwerking in de zin van de Wbp.

5.3.3 *Uitzonderingen en territoriale begrenzing*

Ten slotte is van belang of de gegevensverwerking van de werking van de Wbp is uitgezonderd. Bepaalde situaties waarin persoonsgegevens (zullen) worden verwerkt, zijn van de werking van de Wbp uitgezonderd.[180] Op gegevensverwerking voor persoonlijk gebruik en/of huislijke kring is de Wbp bijvoorbeeld niet van toepassing. Tevens is verwerking op basis van bijzondere wetgeving van de werking van de Wbp uitgesloten.[181]

Bij de aantoonplicht doen zich ten aanzien van de verwerking van de naam,

---

177 Sauerwein & Linnemann 2002, p. 14.

178 Kamerstukken II 1997/98, 25 892, nr. 3, p. 52.

179 Om van een bestand te kunnen spreken is vereist dat de persoonsgegevens op grond van meer dan één kenmerk een samenhangend geheel vormen, systematisch toegankelijk zijn en betrekking hebben op verschillende personen. Bij de vraag of de persoonsgegevens systematisch toegankelijk zijn, is de methode van gegevensopslag en gegevensverwerking van belang. Waar het om gaat is of de inhoud van het bestand volgens bepaalde criteria is aangelegd. Kamerstukken II 1997/98, 25 892, nr. 3, p. 54.

180 Artikel 2 en artikel 3 van de Wbp.

181 Er zijn verschillende sectorale regelingen die een specifieke regeling over de verwerking van privacy gevoelige gegevens bevatten. De Wpg is bijvoorbeeld zo'n sectorale regeling.

het telefoonnummer en het stemgeluid van de aantoonplichtige en de verwerking van Cell-ID's geen situaties voor waarin deze gegevens van de werking van de Wbp zijn uitgezonderd.

Voor de reikwijdte van de Wbp is eveneens van belang of de gegevensverwerking plaatsvindt in het kader van activiteiten van een in Nederland gevestigde verantwoordelijke. In dat geval is de Wbp namelijk geheel van toepassing.[182]

5.3.4 *Wie is verantwoordelijk?*

In de Wbp is het begrip 'verantwoordelijke' belangrijk, aangezien de wet bij de verwerking van persoonsgegevens veel verplichtingen oplegt aan de verantwoordelijke. Verantwoordelijk is degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt.[183]

Om als verantwoordelijke te kunnen worden aangemerkt, is vereist dat men formeel juridische zeggenschap heeft of dat de gegevensverwerking op grond van de in het maatschappelijke verkeer geldende maatstaven is toe te rekenen.[184] Het laatste criterium is met name van belang als de juridische zeggenschap onvoldoende duidelijk is geregeld en/of persoonsgegevens onbevoegd zijn verwerkt.

In de publieke sector is de verantwoordelijke het bij of krachtens de publiekrechtelijke regeling bevoegde bestuursorgaan.[185] Bij de digitale aantoonplicht heeft de burgemeester formeel-juridisch de bevoegdheid het doel en de middelen van de gegevensverwerking vast te stellen. Hij is krachtens het eerste lid van artikel 172 Gemw belast met de handhaving van de openbare orde. Op grond van een verordening zou hij de bevoegdheid moeten krijgen om aan een stadiongebiedsverbod een aantoonplicht te koppelen. De burgemeester, die in Nederland is gevestigd, is dus als verantwoordelijke aan te merken.

---

182 Artikel 4 Wbp.

183 Artikel 1 onder de Wbp.

184 Volgens de Memorie van Toelichting dient te worden uitgegaan van de formeel-juridische bevoegdheid om het doel en de middelen van de gegevensverwerking vast te stellen en moet, in aanvulling daarop, worden afgegaan op de functionele inhoud van het begrip 'verantwoordelijke'. Kamerstukken II 1997/98, 25 892, nr. 3, p. 55.

185 Met het begrip 'bestuursorgaan' is in de Wbp aangesloten bij het begrip 'bestuursorgaan' in artikel 1:1 van de Awb. Kamerstukken II 1997/98, 25 892, nr. 3, p. 57.

De politie die de aantoonplichtige op de naleving van het stadiongebiedsverbod zal controleren en derhalve voor de burgemeester persoonsgegevens verwerkt, staat onder het gezag van de burgemeester.[186] Aangezien de politie in een hiërarchische verhouding staat tot de burgemeester, is er ten aanzien van de politie sprake van 'intern beheer'.

Geconcludeerd kan worden dat de Wbp op de verwerking van de naam, het telefoonnummer en het stemgeluid van de supporter en de verwerking van Cell-ID's van toepassing is. Het betreft immers persoonsgegevens die de politie 'verwerkt' en er doen zich geen situaties voor waarin toepassing van de Wbp is uitgesloten.

5.4 Rechtmatige gegevensverwerking

Niet elke verwerking van persoonsgegevens is per definitie toegelaten. Het verwerken van dergelijke gegevens is alleen rechtmatig, indien de gegevensverwerking aan de materiële normen van de Wbp voldoet. Die normen hebben allemaal betrekking op de toelaatbaarheid en de kwaliteit van de (verwerking van) persoonsgegevens. Zo dienen de gegevens op een behoorlijke en zorgvuldige wijze te worden verwerkt, mag men alleen op basis van een van de in de Wbp genoemde gronden gegevens verwerken en worden er specifieke eisen gesteld aan de kwaliteit van gegevens en het doel om deze te verwerken.

5.4.1 Behoorlijke en zorgvuldige gegevensverwerking

In het algemeen geldt dat persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze moeten worden verwerkt.[187] Met het begrip 'zorgvuldig' heeft de wetgever aangesloten bij de zorgvuldigheidsnorm uit artikel 6:162 van het Burgerlijk Wetboek (BW) en bij de in het bestuursrecht geldende algemene beginselen van behoorlijk bestuur.[188] Bij de interpretatie van de term 'behoorlijk' kan volgens Kranenborg en Verhey

186 Artikel 2 jo. artikel 12 Polw 1993.

187 Artikel 6 Wbp en Kamerstukken II 1997/98, 25 892, nr. 3, p. 78.

188 Hooghiemstra & Nouwt 2011, p. 40.

inspiratie worden geput uit de maatstaven die in het kader van de toepassing van de behoorlijkheidsnorm krachtens de Wet Nationale ombudsman zijn ontwikkeld.[189]

Voor de digitale aantoonplicht betekent dit, dat men conform de algemene beginselen van behoorlijk bestuur moet handelen. Zo rust er in verband met het beginsel van zorgvuldige voorbereiding op de burgemeester een informatieplicht en dient hij in samenwerking met de politie maatregelen te treffen om ervoor te zorgen dat de gegevens juist, nauwkeurig en van een voldoende kwaliteit zijn.

De Wbp bevat verschillende eisen waaraan de verantwoordelijke zich moet houden. Hiermee is gewaarborgd dat er bij de verwerking van persoonsgegevens geen belangrijke (geschreven en ongeschreven) beginselen worden veronachtzaamd. Wanneer de aantoonplichtige bijvoorbeeld heeft verzocht om een correctie van de gegevens, dan dient de politie bij een afwijzing van dat verzoek die weigering te motiveren. Dit volgt uit het motiveringsbeginsel. De Wbp waarborgt dit beginsel.[190]

5.4.2 *Doeleinden gegevensverwerking*

De Wbp stelt aan het doel om gegevens te verwerken verschillende voorwaarden.[191] Vereist is dat men persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omgeschreven en gerechtvaardigde doeleinden verzamelt.[192] Het doel moet duidelijk zijn omschreven, zodat kan worden getoetst of de verzameling van de gegevens in dat verband nodig is. De doelomschrijving mag derhalve niet zodanig vaag of ruim zijn, dat zij bij de beoordeling van de noodzakelijkheid geen

189 Kranenborg & Verhey 2011, p. 82.

190 Het tweede lid van artikel 36 van de Wbp bepaalt namelijk: 'Een weigering is met redenen omkleed'.

191 Tijdens het verwerkingsproces mag men het doel niet zomaar veranderen of uitbreiden. Zie: Sauerwein & Linnemann 2002, p. 20. Men mag persoonsgegevens die voor een bepaald doel zijn verzameld, alleen voor andere doeleinden verder verwerken, indien die verwerking verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verkregen; artikel 9 Wbp. Hoe gevoeliger het gegeven, hoe minder snel men mag aannemen dat er sprake is van verenigbaar gebruik; zie: Kamerstukken II 1997/98, 25 892, nr. 3, p. 90.

192 Onder het verzamelen van persoonsgegevens moet worden verstaan het verkrijgen van persoonsgegevens. Zie: artikel 1 onder o Wbp. Indien persoonsgegevens voor meerdere doeleinden worden verzameld, is niet vereist dat zij verband houden met elkaar.

handvatten kan bieden. Tevens is vereist dat het doel bepaald is voordat de politie overgaat tot het verzamelen van de gegevens.[193]

Bij de digitale aantoonplicht worden de gegevens verwerkt in verband met de handhaving van de openbare orde. Meer specifiek heeft de verwerking de controle van de naleving van het stadiongebiedsverbod en het voorkomen van voetbalgerelateerde verstoringen van de openbare orde tot doel. De burgemeester besluit op basis van een verordening tot het opleggen van een stadiongebiedsverbod en een digitale aantoonplicht. In dat besluit moet hij het doel duidelijk omschrijven. Bij de aantoonplicht is, mede in verband met de algemene beginselen van behoorlijk bestuur, voldoende gewaarborgd dat het doel welbepaald en uitdrukkelijk is omschreven.

De Wbp stelt tevens als voorwaarde dat het doel gerechtvaardigd is.[194] Het belang van de burgemeester, te weten handhaving van de openbare orde, meer in het bijzonder het voorkomen van voetbalgerelateerde verstoring van de openbare orde, is een dragend argument voor het verzamelen van de gegevens en is niet in strijd met de wet, openbare orde of goede zeden. Of het doel gerechtvaardigd is, is mede afhankelijk van de vraag of er voor de gegevensverwerking altijd een geldige rechtsgrond valt aan te wijzen. Van ieder gegeven moet worden onderzocht of de verwerking kan steunen op een van de in de Wbp aangegeven gronden.[195]

5.4.3 *Een geldige grondslag?*

Verwerking van persoonsgegevens is alleen toegestaan wanneer *iedere* verwerking van een gegeven op een of meer gronden uit artikel 8 van de Wbp kan worden gebaseerd.[196] Indien voor de verwerking geen grond is aan te wijzen,

193 Het doeleinde is pas uitdrukkelijk omschreven indien de verantwoordelijke het doel bij de melding aan het College bescherming persoonsgegevens of de functionaris voor de gegevensbescherming heeft aangeduid. De Wbp verplicht de verantwoordelijke om de gegevensverwerking bij het Cbp of de functionaris te melden, tenzij hij van de meldingsplicht is vrijgesteld. Zie voor de wijze waarop de melding plaats moet vinden het Meldingsbesluit Wbp. Het besluit is te vinden via http://wetten.overheid.nl. Zie ook het informatieblad 'Melden en vrijstellingen', dat is te downloaden via http://www.cbpweb.nl. Indien men van de meldingsplicht is vrijgesteld, geldt het doel dat bij het vrijstellingsbesluit is voorgeschreven. Voor informatie over vrijstelling wordt verwezen het Vrijstellingsbesluit Wbp en de Handreiking Vrijstellingsbesluit Wbp. Beide zijn te raadplegen via http://wetten.overheid.nl en http://www.cbpweb.nl.

194 Kamerstukken II 1997/98, 25 892, nr. 3, p. 78.

195 Kamerstukken II 1997/98, 25 892, nr. 3, p. 79.

is de gegevensverwerking onrechtmatig. Voor dit onderzoek zijn slechts de volgende gronden van belang:

1 Persoonsgegevens mogen worden verwerkt, indien de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;
2 Persoonsgegevens mogen worden verwerkt, indien de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
3 Persoonsgegevens mogen worden verwerkt, indien de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan, dan wel het bestuursorgaan waaraan de gegevens worden verstrekt;
4. Persoonsgegevens mogen worden verwerkt, indien de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Ondubbelzinnige toestemming

Artikel 8 onder a van de Wbp bepaalt dat de verwerking van persoonsgegevens geoorloofd is, indien degene van wie de gegevens verwerkt gaan worden met die verwerking instemt. Indien een verbannen voetbalsupporter ondubbelzinnige toestemming geeft voor de verwerking van zijn gegevens, is de aantoonplicht zonder meer uitvoerbaar.

Wanneer is er sprake van een ondubbelzinnige toestemming? Volgens de wetgever levert elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene de gegevensverwerking aanvaardt ondubbelzinnige toestemming op.[197] Om van een rechtsgeldige toestemming te kunnen spreken is vereist dat de burgemeester in zijn besluit tot oplegging van de digitale aan-

196 Het betreft een limitatieve opsomming.

197 Artikel 1 onder i Wbp. Met de term 'wilsuiting' is aangesloten bij het BW. Zie: Kamerstukken II 1997/98, 25 892, nr. 3, p. 65.

toonplicht voldoende en duidelijke informatie daarover geeft. Er moet namelijk sprake zijn van *informed consent*.

Het vereiste van informed consent betekent dat de aantoonplichtige voldoende en begrijpelijke informatie moet krijgen, zodat hij zich een goed oordeel kan vormen over de (toekomstige) gegevensverwerking. De burgemeester dient hier in beginsel voor te zorgen, maar ook op de persoon zelf rust een zekere onderzoeksplicht. De omstandigheden van het geval bepalen uiteindelijk in hoeverre op de burgemeester en/of de supporter een plicht rust. Volgens de Memorie van Toelichting bij de Wbp kunnen meerdere factoren een rol spelen, waaronder de aard van de gegevens, de manier waarop en de context waarin de persoonsgegevens verwerkt zullen worden en de positie en onderlinge verhouding tussen de burgemeester en de aantoonplichtige.[198]

Voorts is vereist dat de aantoonplichtige zijn wil daadwerkelijk heeft geuit en dat zijn wilsuiting specifiek betrekking heeft op een bepaalde verwerking of categorie van verwerkingen.[199] Dat de wilsuiting specifiek moet zijn, heeft tot gevolg dat ondertekening van een algemeen machtigingsformulier door de supporter niet volstaat. Alleen indien het formulier de (categorieën van) gegevensverwerkingen duidelijk omschrijft en er in het formulier een nadere specificatie over de derden aan wie men voornemens is de gegevens te verstrekken is opgenomen, kan ondertekening van het formulier worden aangemerkt als een specifieke toestemming om de gegevens te verwerken.[200]

Ten slotte is vereist dat de toestemming ondubbelzinnig is gegeven en niet onder druk tot stand is gekomen.[201] De burgemeester mag geen twijfel hebben over de vraag of de persoon voor de (categorie van) gegevensverwerking toestemming heeft verleend. Indien er bij hem wel twijfel bestaat, dient hij de toestemming te verifiëren De burgemeester moet namelijk kunnen bewijzen dat de verbannen voetbalsupporter met de verwerking van de gegevens heeft ingestemd en dat die toestemming rechtsgeldig is. Indien dat laatste niet het geval is, is de toestemming nietig.[202]

Indien de aantoonplichtige ondubbelzinnige toestemming geeft voor de verwerking van de gegevens, levert de verwerking in beginsel geen probleem

198 Kamerstukken II 1997/98, 25 892, nr. 3, p. 66.

199 In tegenstelling tot de Wpr hoeft de betrokkene de toestemming niet per se schriftelijk te geven.

200 Kamerstukken II 1997/98, 25 892, nr. 3, p. 65.

201 Voor het verwerken van bijzondere persoonsgegevens is vereist dat de betrokkene uitdrukkelijk toestemming geeft. Dat betekent dat er meer eisen aan de toestemming worden gesteld. De betrokkene dient in dat geval zijn wil expliciet te hebben geuit.

202 Zie: artikel 3:40 lid 1 BW.

op.[203] Wel dient opgemerkt te worden dat de supporter zijn toestemming te allen tijde mag intrekken.[204] Een dergelijke intrekking heeft geen terugwerkende kracht, waardoor verwerkingen die voor de intrekking hebben plaatsgevonden rechtmatig zijn.

Gezien het bovenstaande kunnen we met betrekking tot de digitale aantoonplicht tot de conclusie komen dat de politie met toestemming van de supporter persoonsgegevens kan verwerken. Er kan zich echter ook een situatie voordoen waarin de voetbalsupporter geen toestemming wil geven voor de verwerking van de gegevens. In dat geval moet worden gekeken of een onvrijwillige verwerking kan worden gebaseerd op een van de andere gronden uit de Wbp.

Wettelijke verplichting

Is de gegevensverwerking bijvoorbeeld noodzakelijk in verband met een wettelijke verplichting die op de burgemeester rust? Artikel 8 onder c van de Wbp vereist dat de burgemeester bij of krachtens wettelijk voorschrift met de uitvoering van een verplichting is belast. Daarbij geldt dat iedere, bij algemeen verbindend voorschrift opgelegde verplichting als 'wettelijke verplichting' kan worden aangemerkt.

De verplichting hoeft geen expliciete opdracht tot de verwerking van de gegevens te bevatten. Dat betekent echter niet dat iedere verwerking van persoonsgegevens zonder meer gerechtvaardigd is.[205] De wettelijke verplichting die op de burgemeester rust, moet namelijk de verwerking noodzakelijk maken. Het uitvoeren van de wettelijke taak moet niet goed mogelijk zijn zonder persoonsgegevens te verwerken, wat inhoudt dat er een evident verband dient te bestaan tussen de verwerking van de gegevens en het (uitvoeren van) de wettelijke verplichting.[206] Verder mogen er geen andere en/of minder ingrijpende mogelijkheden bestaan om de wettelijke taak uit te voeren.[207]

---

203 De verwerking kan in dat geval worden gebaseerd op artikel 8 onder a van de Wbp. In dat geval is nog wel vereist dat de gegevensverwerking noodzakelijk is met het oog op het voorkomen van wanordelijkheden en strafbare feiten. De verwerking dient aan het subsidiariteits- en proportionaliteitsvereiste te voldoen. Zie ook: HR 9 september 2011, NJ 2011/595.

204 Artikel 5 Wbp.

205 Kamerstukken II 1997/98, 25 892, nr. 3, p. 83.

206 Kamerstukken II 1997/98, 25 892, nr. 3, p. 82.

207 Bij de aanpak van voetbalvandalisme is dat naar onze mening (nog) niet het geval.

Krachtens het eerste lid van artikel 172 van de Gemw is de burgemeester belast met de handhaving van de openbare orde. In een verordening zou een burgemeester verplicht kunnen worden om aan een voetbalsupporter die zich heeft schuldig gemaakt aan een ernstige verstoring van de openbare orde een stadiongebiedsverbod op te leggen en bij een minder ernstige verstoring van de openbare orde naar keuze een aantoonplicht op te leggen.

Het opleggen van een aantoonplicht betreft dan bij de minder ernstige ordeverstoringen een discretionaire bevoegdheid, met andere woorden, geen verplichting voor de burgemeester om tot de oplegging van de aantoonplicht over te gaan. Een expliciete opdracht tot gegevensverwerking is niet vereist, toch is het lastig om in dit geval van een verplichting krachtens wettelijk voorschrift te spreken. Op z'n minst zou de burgemeester in zo'n geval moeten motiveren waarom hij zich gezien zijn wettelijke taak inzake de handhaving van de openbare orde verplicht voelt om een aantoonplicht op te leggen. De reputatie van de supporter, de aankondiging het stadiongebiedsverbod niet te zullen naleven, kunnen hierin een rol spelen.

Komt aan de burgemeester geen beleidsvrijheid toe, dan vormt artikel 8 onder c van de Wbp een geldige grondslag om bij de digitale aantoonplicht gegevens te verwerken.[208]

Publiekrechtelijke taak

Op grond van artikel 8 onder e van de Wbp kunnen persoonsgegevens worden verwerkt als dat noodzakelijk is om een publiekrechtelijke taak goed te vervullen. Vereist is dat de gegevensverwerking plaatsvindt door een bestuursorgaan.[209] Een taak is publiekrechtelijk als de bevoegdheid speciaal voor het openbaar bestuur in het leven is geroepen en derhalve op een publiekrechtelijke grondslag berust.[210]

Bij de openbareorderechtelijke handhaving door middel van een gebiedsontzegging en een (digitale) aantoonplicht is sprake van een publiekrechtelijke

208 Over de vraag of artikel 172 Gemw al dan niet een toereikende grondslag vormt, is discussie mogelijk. Een combinatie van deze bepaling met een specifieke verordening, neemt veel van die twijfel weg.

209 Het bestuursorgaan kan de publiekrechtelijke taak zelf verrichten of door een ander bestuursorgaan laten verrichten. Met de begrippen 'publiekrechtelijke taak' en 'bestuursorgaan' heeft de wetgever aangesloten bij de systematiek van de Awb. Voor het begrip 'bestuursorgaan' wordt verwezen naar artikel 1:1 van de Awb.

210 Zie voor het begrip 'publiekrechtelijke taak' onder meer het besluitbegrip van artikel 1:3 van de Awb.

taak. Het betreft een taak van algemeen belang. Het eerste lid van artikel 172 Gemw belast de burgemeester met de handhaving van de openbare orde. Een verordening verschaft hem daartoe een specifieke bevoegdheid.[211] Bij de digitale aantoonplicht vindt de verwerking van persoonsgegevens plaats door een bestuursorgaan.[212] De burgemeester zal bij de uitoefening van deze taak gebruikmaken van de onder zijn gezag staande politie.

De vraag rijst of bij de digitale aantoonplicht de gegevensverwerking noodzakelijk is om de taak goed te kunnen vervullen. Het antwoord hierop hangt af van de vraag of aan de vereisten van subsidiariteit en proportionaliteit is voldaan. Dit betekent dat het doel waarvoor de politie de gegevens zal verwerken in redelijkheid niet op een voor de voetbalsupporter minder nadelige wijze kan worden gerealiseerd en dat de beperking van het privacyrecht van de supporter in een redelijke verhouding moet staan tot het doel.[213]

Bij de inrichting en de uitvoering dient men rekening te houden met het privacyrecht van de betrokkene. Het doel van handhaving van de openbare orde kan naar onze mening niet op een minder ingrijpende wijze worden bereikt. Om op afstand te controleren of de supporter het verbod naleeft, zal de politie meer persoonsgegevens moeten verwerken dan bij een fysieke meldingsplicht het geval is. Immers, er moet zekerheid bestaan dat het de juiste persoon is die de politie op afstand controleert.

De supporter moet zich eenmalig op het politiebureau legitimeren. Als gevolg hiervan kan worden volstaan met alleen de verwerking van de naam, het telefoonnummer en het stemgeluid van de voetbalsupporter en is het overbodig om voor de aantoonplicht ook zijn adres, woonplaats, geboortedatum en/of het burgerservicenummer e.d. te verwerken. Bij de inrichting van de digitale aantoonplicht is het belangrijk om te streven naar zo veel mogelijk minimalisatie van persoonsgegevens. Alleen gegevens die daadwerkelijk nood-

211 Wanneer er geen gedetailleerde wettelijke regels voor de taakuitoefening voorhanden zijn, verkrijgt de vraag of er sprake is van een rechtmatige taakuitoefening bijzondere aandacht. De Wbp spreekt van een 'goede vervulling van de taak'. Kan de burgemeester in dit geval zijn taak alleen goed vervullen door middel van een nalevingscontrole op afstand? Wij zijn van mening dat het antwoord op deze vraag bevestigend luidt. Met de huidige bevoegdheden kan men voetbalvandalisme niet effectief en efficiënt aanpakken. Er zijn weliswaar andere manieren om voetbalgerelateerde overlast te voorkomen, zoals de digitale meldzuil, maar deze alternatieven zijn niet minder ingrijpend dan een digitale aantoonplicht.

212 Zie voor de burgemeester artikel 1:1 lid 1 onder a Awb jo. artikel 2:1 BW en artikel 6 Gemw en voor de politie artikel 1:1 lid 1 onder a Awb jo. artikel 21 Polw 1993.

213 Kamerstukken II 1997/98, 25 892, nr. 3, p. 80.

zakelijk zijn om een digitale surveillance en de speaker recognition uit te voeren, dient de politie te verwerken, waardoor de aantoonplicht een maatregel is die zo min mogelijk ingrijpt in het privéleven van de supporter.

De beperking van het privacyrecht is niet onevenredig aan het met de verwerking te dienen doel. Een digitale aantoonplicht beperkt het privacyrecht slechts gering. Het subsidiariteits- en proportionaliteitsvereiste hoeven in de praktijk geen problemen op te leveren. Op basis van artikel 8 onder e van de Wbp kunnen bij de aantoonplicht derhalve persoonsgegevens worden verwerkt.

Gerechtvaardigd belang verantwoordelijke

Artikel 8 onder f van de Wbp kan wellicht ook een geldige grond opleveren voor het verwerken van de naam, het telefoonnummer en het stemgeluid van de aantoonplichtige en het verwerken van Cell-ID's.[214] Daarvoor is vereist dat de verwerking van deze gegevens noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de burgemeester. Of een belang gerechtvaardigd is en een verwerking toestaat, is een kwestie van interpretatie. Bij de aantoonplicht kan het belang van de burgemeester om de openbare orde te handhaven worden aangemerkt als een gerechtvaardigd belang.[215]

De vraag of de gegevensverwerking ook noodzakelijk is voor de behartiging van dat belang, wordt mede bepaald door het privacyrecht.[216] Alleen indien het privacyrecht van de aantoonplichtige niet prevaleert, is de verwerking van de gegevens met het oog op de openbareorderechtelijke handhaving geoorloofd.[217] Verwerking van de naam, het telefoonnummer en het stemgeluid van de aantoonplichtige beperkt diens privacyrecht. Beoordeeld moet worden of de verwerking van deze gegevens niet, afhankelijk van de ernst van de beperking,

214 Het betreft hier een restbepaling die de wetgever heeft opgenomen, aangezien het onmogelijk is om een sluitende regeling van gronden voor gegevensverwerking in de Wbp op te nemen.

215 De burgemeester dient zich echter altijd af te vragen of er in de desbetreffende situatie een belang is dat de verwerking van persoonsgegevens rechtvaardigt.

216 Het subsidiariteits- en proportionaliteitsbeginsel spelen wederom een belangrijke rol. Kamerstukken II 1997/98, 25 892, nr. 3, p. 87.

217 Er kan zich dus een situatie voordoen waarin de burgemeester voor de verwerking van persoonsgegevens wel een gerechtvaardigd belang heeft, maar waarin die gegevensverwerking desondanks niet is toegestaan.

achterwege moet blijven. Daarbij dient het algemene belang van openbare-orderechtelijke handhaving en het privacybelang van de supporter tegen elkaar te worden afgewogen.[218]

Of de verwerking van persoonsgegevens achterwege moet blijven, hangt af van de ernst van de inbreuk. Daarbij spelen de mate van gevoeligheid van te verwerken gegevens en de maatregelen die de verantwoordelijke of derde heeft genomen om een zorgvuldig gebruik van de gegevens te waarborgen een rol.[219]

Door bij de inrichting en de uitvoering van de aantoonplicht rekening te houden met het privacybelang van de aantoonplichtige, kan de beperking van diens recht zo gering mogelijk worden gehouden. Maatregelen die met het oog op het privacyrecht zijn genomen, zoals beveiligingsmaatregelen, beïnvloeden de afweging van de bij de aantoonplicht betrokken belangen. Het privacybelang van de supporter zal namelijk in mindere mate gewicht in de schaal leggen, indien er meer waarborgen voor een zorgvuldig gebruik van de gegevens zijn opgenomen.[220]

Bij de digitale aantoonplicht kan het oogmerk van openbareorderechtelijke handhaving niet op een minder ingrijpende wijze worden bereikt en de beoogde verwerking lijkt evenredig te zijn aan het nagestreefde doel. Artikel 8 onder f van de Wbp biedt derhalve eveneens een geldige grondslag voor de verwerking van de persoonsgegevens.

5.4.4 *Kwaliteit van de gegevens*

Ingevolge de Wbp dienen de persoonsgegevens van voldoende kwaliteit te zijn.[221] Vereist is dat zij toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig zijn. Dat betekent dat te verwerken gegevens voldoende informatie moeten bevatten en dat er niet meer persoonsgegevens mogen worden verwerkt dan nodig is om het doel van de verwerking te realiseren.

Dat de gegevens juist en nauwkeurig moeten zijn, houdt niet in dat de burgemeester (en de politie) altijd de juistheid van de gegevens moet kunnen

---

218 In feite betreft het hier een tweede proportionaliteitstoets, waarbij het privacybelang van de aantoonplichtige een zelfstandig gewicht in de schaal legt. De burgemeester dient per geval te beoordelen of toepassing van de bevoegdheid proportioneel is.

219 Kamerstukken II 1997/98, 25 892, nr. 3, p. 86-88.

220 Zie: Kamerstukken II 1997/98, 25 892, nr. 3, p. 88.

221 Artikel 11 van de Wbp.

garanderen. Op hen rust slechts een inspanningsverplichting om de nodige maatregelen te treffen om de kwaliteit van de gegevens te waarborgen. Men dient alle maatregelen te treffen die redelijkerwijs kunnen worden gevergd om te waarborgen dat de gegevens zo juist en nauwkeurig mogelijk zijn. Het soort gegevens, de huidige stand van de techniek en de kosten die met het treffen van maatregelen gepaard gaan, stellen grenzen aan wat men van de burgemeester (en de politie) mag verwachten.[222]

5.4.5 *Overige verplichtingen*

Bij het verwerken van persoonsgegevens moet tevens aan een aantal andere verplichtingen worden voldaan. De burgemeester dient er bijvoorbeeld, in samenwerking met de politie, voor te zorgen dat er adequate, zowel technische als organisatorische, beveiligingsmaatregelen worden getroffen.[223] Belangrijk is dat deze verplichting voor alle onderdelen van het proces van gegevensverwerking geldt.[224]

De maatregelen dienen 'passend' en dus in overeenstemming met de huidige stand van de techniek te zijn. Tevens moeten zij risico's uitsluiten of in ieder geval beheersbaar maken. Bij het bepalen welke beveiligingsmaatregelen noodzakelijk zijn, kan men met de kosten die de tenuitvoerlegging van de maatregelen met zich meebrengt rekening houden.

Het niveau van beveiliging is afhankelijk van de aard van de persoonsgegevens en de risico's van de gegevensverwerking. Bij de ontwikkeling van een bepaald systeem en voordat men persoonsgegevens gaat verwerken, is het derhalve aan te bevelen om een risicoanalyse uit te voeren. Bij de keuze voor het beveiligingsniveau moet men rekening houden met de eis dat de verwerking niet bovenmatig mag zijn. De beveiligingsmaatregelen moeten er derhalve mede op gericht zijn onnodige verwerking van persoonsgegevens te voorkomen.

Bij het treffen van beveiligingsmaatregelen kan men denken aan het anoni-

222 Kamerstukken II 1997/98, 25 892, nr. 3, p. 97 en Hooghiemstra en Nouwt 2011, p. 67.

223 Artikel 13 van de Wbp. Organisatorische maatregelen zijn maatregelen zoals toekenning en deling van verantwoordelijkheden, bevoegdheden, instructies, trainingen en calamiteitenplannen. Technische maatregelen zijn logische en fysieke maatregelen in en rondom informatiesystemen, zoals toegangscontroles, vastlegging van gebruik en back-up. Zie: Borking 2010, p. 117.

224 Hooghiemstra & Nouwt 2011, p. 66.

miseren van bepaalde gegevens en het zo snel mogelijk vernietigen of door middel van cryptografische technieken loskoppelen van (tijdelijke) gegevens. Daarvoor kan men denken aan Privacy Enhancing Technologies.[225] Bovendien kan het informatiesysteem wellicht zo worden ingericht, dat de gegevensverwerking wordt af- of onderbroken als de verwerking in strijd met de Wbp of andere privacyregelingen plaatsvindt.[226]

De Wbp stelt verder eisen aan het bewaren van persoonsgegevens.[227] De bewaartermijn is in beginsel onbepaald, maar wel afhankelijk van het doel waarvoor de verantwoordelijke de persoonsgegevens verwerkt. Men mag de gegevens namelijk niet langer bewaren dan noodzakelijk is om het handhavingsdoel te verwezenlijken.[228] Wanneer die noodzaak ontbreekt, mag de politie de gegevens niet langer bewaren in een vorm die het mogelijk maakt om de betrokkene te identificeren. In dat geval dienen de gegevens te worden verwijderd of ontdaan van alle identificerende kenmerken.[229] Bij de inrichting van de digitale aantoonplicht is het raadzaam om zoveel mogelijk te streven naar gegevensminimalisatie. Dat betekent dat anonimiteit, het gebruik van zo min mogelijk gegevens en het tijdig verwijderen ervan worden beoogt.

De Wbp vereist voorts dat de burgemeester informatie, waaronder zijn identiteit en het doel van de gegevensverwerking, verstrekt aan de aantoonplichtige.[230] Het niet voldoen aan deze informatieplicht heeft als gevolg dat de gegevensverwerking onrechtmatig is. Op verzoek van de verbannen voetbalsupporter dient de burgemeester inzage te geven in de te verwerken gegevens. De aantoonplichtige heeft namelijk inzagerecht, correctierecht en recht van verzet.[231] Het kan derhalve voorkomen dat persoonsgegevens moeten worden gecorrigeerd, aangevuld of verwijderd. Wanneer de supporter gebruikmaakt van zijn verzetsrecht, moet men de gegevensverwerking beëindigen.

---

225 Voor meer informatie over Privacy Enhancing Technologies verwijzen wij naar Borking 2010 en Koorn, Van Gils, Ter Hart, e.a. 2004.

226 Zie: Borking 2010, p. 177 en 178.

227 Artikel 10 van de Wbp.

228 Dat een supporter wellicht in de toekomst opnieuw de fout in gaat, is geen reden om zijn gegevens langer te bewaren. Wanneer de supporter wederom de openbare orde voetbalgerelateerd verstoort en een stadiongebiedsverbod en aantoonplicht opgelegd krijgt, moet hij de procedure opnieuw doorlopen. In verband met het privacyrecht van de betrokkene zijn de eerdere gegevens dan al verwijderd.

229 Sauerwein & Linnemann 2002, p. 40.

230 Zie voor de inhoud van de informatieplicht de artikelen 33, 34 en 35 van de Wbp.

231 Zie onder meer de artikelen 35, 36, 40 en 41 van de Wbp.

5.5 Het besluit van de burgemeester

De burgemeester kan op grond van een verordening een besluit nemen tot het opleggen van een stadiongebiedsverbod en een aantoonplicht, indien de supporter de openbare orde heeft verstoord. Aangezien een aantoonplicht alleen in combinatie met een stadiongebiedsverbod kan worden opgelegd, kan de burgemeester beide gedragsaanwijzingen in één besluit opleggen.

Het is uiteindelijk aan de burgemeester om per geval te bepalen hoe de aantoonplicht eruit komt te zien. Voordeel hiervan is dat hij persoonlijke omstandigheden van de supporter bij de inrichting mee kan nemen en zodoende maatwerk kan leveren.

5.5.1 Inhoudelijke vereisten

Aan het besluit van de burgemeester worden verschillende eisen gesteld. In het algemeen geldt dat het besluit in overeenstemming met de algemene beginselen van behoorlijk bestuur moet zijn genomen en overeenkomstig de regels van artikel 3:41 Awb bekend moet zijn gemaakt. Wegens het combineren van een verblijfsverbod met een aantoonplicht zullen er zwaardere eisen aan de motivering van het besluit worden gesteld. Bovendien moet het besluit voldoen aan de vereisten van subsidiariteit en proportionaliteit.

De burgemeester dient in het besluit in ieder geval de volgende zaken te vermelden: de naam en het adres van de geadresseerde, dagtekening, de gedraging(en) waarmee de openbare orde voetbalgerelateerd is verstoord, alsmede de tijdstippen waarop en de plaats(en) waar die gedraging(en) heeft/hebben plaatsgevonden. In het besluit moet gemotiveerd zijn aangegeven waarom die gedraging(en) aanleiding is/zijn voor het opleggen van een gebiedsontzegging en een (digitale) aantoonplicht. Bovendien moet het besluit een omschrijving bevatten van het gebied en de periode waarvoor het verbod geldt.

Voorts moet de burgemeester in het besluit kort maar duidelijk het doel en de inhoud van de (digitale) aantoonplicht aangeven en een omschrijving geven van de dagen en de tijdstippen waarop de supporter dient aan te tonen niet in het verboden gebied aanwezig te zijn. Ten slotte mag een rechtsmiddelenclausule in het besluit niet ontbreken.

5.5.2 *Verstrekking politiegegevens*

Om een besluit te kunnen nemen, dient de burgemeester over verschillende gegevens, waaronder persoonsgegevens, te beschikken. Voor het opleggen van een stadiongebiedsverbod en een digitale aantoonplicht moet de burgemeester bewijzen dat de supporter de openbare orde heeft verstoord. Veelal zal hij daarvoor gebruikmaken van processen-verbaal van de politie. In het kader van dit onderzoek is de uitzonderingsgrond 'ten behoeve van de uitvoering van de politietaak […]' uit de Wbp van belang.[232] Een proces-verbaal bevat persoonsgegevens die in het kader van de uitoefening van de politietaak zijn verwerkt. De verwerking van deze gegevens valt buiten de reikwijdte van de Wbp. Het betreft politiegegevens en op het verstrekken van dergelijke gegevens is de Wpg van toepassing.

Ondanks dat de Wpg een gesloten systeem van verstrekkingen kent, worden aan burgemeesters steeds op basis van artikel 16 van de Wpg politiegegevens verstrekt. Dat artikel bevat een wettelijke grondslag, waarbij de mogelijkheid om gegevensverstrekking te weigeren ontbreekt.[233] Ook mag de verstrekking van politiegegevens aan de burgemeester niet aan beperkende voorwaarden worden onderworpen.[234] In het kader van de digitale aantoonplicht kan de burgemeester de politiegegevens derhalve altijd verkrijgen. Uit het proces-verbaal van de politie zal de burgemeester vervolgens de gegevens halen die nodig zijn voor het geven van de gedragsaanwijzingen.

5.6 *Concluderende opmerkingen*

In dit hoofdstuk zijn de materiële normen van de Wbp onderzocht. Gebleken is dat de Wbp alleen op de verwerking van de naam, het telefoonnummer en het stemgeluid van de aantoonplichtige, evenals op de verwerking van Cell-ID's van toepassing is. Op het verkrijgen van politiegegevens is niet de Wbp, maar de Wpg van toepassing. Deze gegevens heeft de burgemeester nodig om een stadiongebiedsverbod en aantoonplicht op te leggen.

---

232 Artikel 2 lid 2 sub c Wbp.

233 Zie artikel 16 lid 1 sub d onder 2 van de Wpg en de 'Verstrekkingenwijzer Wpg', p. 8. Op basis van dit artikel kan bij handhaving van de openbare orde veel informatie worden uitgewisseld tussen de burgemeester en de politie.

234 Zie voor meer informatie over de verstrekking van politiegegevens de 'Verstrekkingenwijzer Wpg', die landelijk wordt gebruikt.

De verwerking van de naam, het telefoonnummer en het stemgeluid van de aantoonplichtige en de verwerking van Cell-ID's moet rechtmatig zijn. Daarvoor is vereist dat de politie de persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt. Tevens worden er aan het doel van de gegevensverwerking verschillende eisen gesteld. Men mag de gegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzamelen. Of het doel gerechtvaardigd is, hangt onder meer af van de vraag of de gegevensverwerking op een of meer gronden van de Wbp kan worden gebaseerd.

Uit ons onderzoek blijkt dat er voor de verwerking van de naam, het telefoonnummer en het stemgeluid van de aantoonplichtige en de verwerking van Cell-ID's een geldige grondslag valt aan te wijzen. Verwerking is mogelijk in verband met een ondubbelzinnige toestemming van de voetbalsupporter. Gegevensverwerking kan echter ook geoorloofd zijn omdat dit noodzakelijk is voor de burgemeester om zijn publieke taak te vervullen. Daarnaast kan het noodzakelijk zijn voor de behartiging van een gerechtvaardigd belang van de burgemeester.

De Wbp vereist voorts dat men ervoor zorgt dat de gegevens van voldoende kwaliteit zijn. Het betreft hier een inspanningsverplichting. Men dient de nodige maatregelen te treffen om de kwaliteit van de gegevens te waarborgen. Dat betekent onder meer het treffen van adequate, zowel technische als organisatorische, beveiligingsmaatregelen.

Daarnaast stelt de Wbp eisen aan het bewaren van de gegevens. Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is om het doel te verwezenlijken.

6

Meerwaarde digitale aantoonplicht dagelijkse politiepraktijk

6.1 Inleiding

Voetbalgerelateerde verstoringen van de openbare orde betreffen een landelijk probleem met een decentraal vertrekpunt. Om die problemen het hoofd te bieden, heeft de wetgever in artikel 172a Gemw de burgemeester de bevoegdheid toegekend om een uit het stadion verbannen persoon een meldplicht op te leggen. Burgemeesters en de politie ondervinden echter problemen met die meldingsplicht. In dit hoofdstuk onderzoeken we daarom in hoeverre een digitale aantoonplicht die problemen kan oplossen. Heeft een digitale aantoonplicht daadwerkelijk toegevoegde waarde?

6.2 Voor- en nadelen van een digitale aantoonplicht

Stadionverboden worden slecht nageleefd. De meldingsplicht had hierin verandering moeten brengen, maar dat valt in de praktijk tegen. Kan een digitale aantoonplicht deze problemen oplossen? Waarschijnlijk zal het enthousiasme bij burgemeesters van gemeenten met een bvo groot zijn. Elk instrument waarmee efficiënt het voetbalvandalisme kan worden bestreden, wordt toegejuicht. Een aantoonplicht zou in een verordening kunnen worden opgenomen, zo zagen we hiervoor. Hij zou vanzelfsprekend ook deel kunnen uitmaken van een herziene Wet mbveo.

Een digitale aantoonplicht op het niveau van een plaatselijke verordening heeft voor- en nadelen. Zeker is dat een digitale aantoonplicht sneller en goedkoper kan worden ingevoerd bij een gemeentelijke verordening dan via een wet in formele zin. Een herziening van de Wet mbveo zal naar verwachting jaren in beslag nemen, aangezien het om een complexe en electoraal gevoelige materie gaat.

Een belangrijk nadeel van een aantoonplicht op gemeentelijk niveau is dat de territoriale reikwijdte van de bevoegdheid beperkt blijft tot het grondgebied van de gemeente. Dat dit een groot nadeel is, bewijst de bevoegdheid van het

huidige artikel 172a Gemw.[235] Om een verbannen persoon op basis van een bevoegdheid in een verordening gedurende een periode uit alle stadiongebieden in Nederland te weren, is een samenspel van burgemeesters van verschillende gemeenten nodig. Een tweede nadeel is dat een verordening geen ruimte biedt om personen te beletten wedstrijden in het buitenland te bezoeken. Burgemeesters zijn immers alleen 'baas' in hun eigen gemeente.

Een meldplicht voor uitwedstrijden zou in die gevallen een uitkomst zijn, maar juist hiervoor biedt artikel 172a Gemw nu geen mogelijkheid. Voor thuiswedstrijden biedt een aantoonplicht bij autonome verordening weer veel meer soelaas.

6.2.1 Knelpunten die de aantoonplicht oplost

Een digitale aantoonplicht neemt (een groot deel van) de knelpunten waar men bij de toepassing van artikel 172a Gemw tegen aanloopt weg. Een verordening kan zodanig worden opgesteld dat de burgemeester na een eenmalige verstoring van de openbare orde een aantoonplicht kan opleggen.

Daarnaast hoeft de burgemeester bij een stadiongebiedsverbod en een digitale aantoonplicht op grond van een verordening niet af te wachten of de officier van justitie een maatregel gaat nemen, zoals thans bij artikel 172a Gemw het geval is. Beide trajecten kunnen naast elkaar, gelijktijdig, worden gevolgd.

De verordening kan zodanig worden ingericht dat een gedragsaanwijzing effectief is. Men kan rekening houden met de omstandigheid dat een verbannen voetbalsupporter slechts eenmaal in de twee weken enkele uren wordt belast met het stadiongebiedsverbod en de aantoonplicht. Ook kan men in een verordening de optie bieden om de winter- en zomerstop, interlandwedstrijden en wijzigingen in het wedstrijdprogramma te verdisconteren. In de verordening kan tevens de lengte van de sanctie, en daarmee ook die van de aantoonplicht, aanzienlijk worden opgeschroefd. Hierdoor komt er een redelijke verhouding tussen het aantal wedstrijden waarvoor de gedragsaanwijzing gaat gelden en de inspanningen die de burgemeester en de politie zich moeten getroosten.

235 De burgemeester van Helmond heeft de bevoegdheid van artikel 172a Gemw bijvoorbeeld ook toegepast bij wedstrijden van Helmond Sport in een andere gemeente; een dergelijke toepassing is echter niet toegestaan. De burgemeester is exclusief belast met de handhaving van de openbare orde in zijn eigen gemeente. Hij kan geen meldingsplicht opleggen om ordeverstoringen in een andere gemeente te voorkomen. De burgemeester van de gemeente Helmond handelde derhalve in strijd met de Gemw.

Indien er bij de uitvoering van de digitale aantoonplicht gebruik wordt gemaakt van een geavanceerd systeem, levert dit een besparing voor de politie-inzet alsook lagere administratieve lasten op. Nog belangrijker is echter dat met een aantoonplicht de naleving van een stadiongebiedsverbod veel beter kan worden afgedwongen. De politie kan, gedurende de zes uren per wedstrijd waarvoor het stadiongebiedsverbod geldt, op elk gewenst moment geautomatiseerd controleren of de supporter het verbod naleeft.

Bovendien lost een digitale aantoonplicht het probleem van het 'importeren' van hooliganisme op. Vanwege de beperkte openingstijden van politiebureaus komt het voor dat in een regio een voetbalsupporter zich uitsluitend fysiek kan melden op een politiebureau in de gemeente van de bvo. Een burgemeester dwingt een voetbalsupporter die in de regio woont, als het ware om zich te melden in de voetbalstad, terwijl hij die persoon daar nu juist liever kwijt dan rijk is.

6.2.2 *Privacy en bewegingsvrijheid*

De meldingsplicht van artikel 172a Gemw is pas werkelijk effectief als de supporter zich op een locatie moet melden die kilometers is verwijderd van het gebied waaruit hij is verbannen. Dat is eigenlijk alleen het geval indien de verbannen voetbalsupporter niet in de gemeente woont waar zijn club speelt. In zo'n geval is het zinvol om gebruik te maken van de intergemeentelijke meldingsplicht. Een voetbalsupporter van Ajax moet zich dan bijvoorbeeld in de rust van een thuiswedstrijd van Ajax melden in Zeist.

De meldingsplicht zou bij een inwoner van de gemeente waar zijn favoriete club speelt effectief kunnen werken, indien een persoon zich meerdere keren op een politiebureau moet melden. Men kan echter vraagtekens zetten bij de toelaatbaarheid daarvan. Artikel 172a Gemw bevat immers alleen een bevoegdheid om een vrijheidsbeperkende, niet een vrijheidsbenemende sanctie op te leggen. Wanneer een persoon zich meerdere malen op een bepaalde locatie moet melden, begint die maatregel toch sterke gelijkenis te vertonen met een vrijheidsbenemende sanctie.

Een meldingsplicht die inhoudt dat een persoon zich tijdens voetbalwedstrijden van zijn club meerdere malen op een politiebureau moet melden, legt een onevenredig beslag op zijn bewegingsvrijheid, met name wanneer de supporter zich op een ander dan het voor hem dichtstbijzijnde politiebureau moet melden. Dit kan een disproportionele sanctie zijn vanwege het tijdsbeslag en de kosten die hiermee gemoeid zijn.

Dit soort problemen doet zich bij een digitale aantoonplicht niet voor. De voetbalsupporter is in dat geval, met uitzondering van het verboden gebied, vrij om te gaan en staan waar hij maar wil. Hij kan in principe vanaf elke willekeurige plaats aantonen niet in het verboden gebied aanwezig te zijn. De aantoonplichtige kan gewoon zijn familie bezoeken of bijvoorbeeld naar het buitenland op vakantie gaan. Een digitale aantoonplicht beperkt de bewegingsvrijheid en het privacyrecht van de supporter derhalve veel minder dan een meldingsplicht krachtens artikel 172a Gemw. De aantoonplicht legt een klein beslag op de tijd van de supporter, hij zal slechts enkele minuten met de aantoonplicht worden geconfronteerd.

De digitale meldzuil waarmee de regiopolitie Twente momenteel experimenteert, lost de problemen die men thans bij de meldingsplicht ondervindt ten aanzien van de meldlocatie slechts gedeeltelijk op. De overheid zal in verband met de bewegingsvrijheid en het privacyrecht van de supporter een behoorlijk aantal zuilen moeten plaatsen.[236] Bovendien voorkomt men er niet mee dat men de supporters importeert naar de voetbalstad. Verder bestaat bij een eenmalige melding het risico dat de supporter zich alsnog naar het stadion begeeft. Hem meerdere keren verplichten zich te melden, kan weer leiden tot een ongerechtvaardigde beperking van zijn bewegingsvrijheid en privacy. Bovendien roept het gebruik van een gezichtsherkenningsmethode de nodige privacyvraagstukken op.

Een digitale aantoonplicht werkt beter, doordat de politie intensiever kan controleren of de voetbalsupporter het gebiedsverbod naleeft. Op de dag van de voetbalwedstrijd kan de politie tijdens de uren van het verbod op elk gewenst tijdstip digitaal surveilleren en een speaker recognition uitvoeren.[237] Doordat de aantoonplichtige tijdens de verboden uren op willekeurige momenten door een computer kan worden gebeld, wordt voorkomen dat de supporter zich alsnog ongemerkt in het verboden stadiongebied kan begeven.

Om te voorkomen dat de digitale surveillance disproportioneel is, moet strategisch gebruik worden gemaakt van de ter beschikking staande controlemiddelen. Bij het onophoudelijk digitaal surveilleren is er wellicht sprake van 'stelselmatig volgen', zij het dat alleen het systeem op de hoogte is van de verblijfplaats van de persoon. Om dat risico uit te sluiten, moet het systeem zoda-

236 Alleen dan zal de plicht om zich bij een digitale meldzuil te melden proportioneel zijn.

237 Uiteraard stelt het proportionaliteitsvereiste grenzen aan het herhaaldelijk ten aanzien van een persoon uitvoeren van een digitale surveillance en speaker recognition.

nig worden ingericht dat er gedurende de verboden uren slechts enkele keren wordt gecontroleerd. Een pilot zal moeten uitwijzen welke mate van intensiteit voor de nalevingscontrole het beste resultaat geeft. Een persoon hoeft wellicht niet bij elke wedstrijd te worden gecontroleerd. De wetenschap van effectieve controle en de hoogte van de sanctie op overtreding van het verbod, kan een supporter ervan weerhouden het stadiongebiedsverbod te overtreden.

Een digitale aantoonplicht hoeft niet privacygevoeliger te zijn dan een meldingsplicht. Het digitaal aantonen dat men zich niet in het verboden gebied bevindt, gebeurt betrekkelijk anoniem. Bij de meldingsplicht moet men zich telkens in persoon op het politiebureau melden. Bij een meldingsplicht bij een digitale meldzuil moet de supporter zelfs een pasfoto inleveren om de controle via gezichtsherkenning mogelijk te maken. In plaats van een foto wordt bij een digitale aantoonplicht een stemsample afgegeven.

6.2.3 *Voor- en nadelen van speaker recognition*

Voor het uitvoeren van een stemherkenningscheck is voorafgaand aan de digitale surveillance de opname van een stemfragment noodzakelijk. Door gebruik te maken van dit biometrische gegeven kan met een grote mate van waarschijnlijkheid worden vastgesteld of het daadwerkelijk de aantoonplichtige is die de telefoon beantwoordt.

Controle met behulp van speaker recognition heeft verschillende voordelen. Er zijn geen speciale lezers of scanners nodig. De kosten voor de hardware zijn daarom gunstig in vergelijking met andere biometrische persoonsherkenningssystemen, zoals een irisscan, gezichtsherkenning of het gebruik van vingerafdrukken. De kosten van de software voor speaker recognition zijn gemiddeld.[238]

Een ander voordeel van het ter controle gebruikmaken van speaker recognition, is dat het de mogelijkheid biedt om met mobiele telefoons te werken. Het gebruik van een mobiele telefoon is aantrekkelijk en men kan er betrouwbare resultaten mee verkrijgen.

Een enkeling schaalt de vereiste medewerking van een persoon aan speaker recognition als nadelig in.[239] Voor de digitale aantoonplicht maakt het echter niet uit of de supporter al dan niet (voldoende) meewerkt aan de speaker

238 Willemsen (red.) 2008, p. 24.

239 Zie bijvoorbeeld Willemsen (red.) 2008, p. 24.

recognition. Indien de aantoonplichtige zijn telefoon meerdere malen niet opneemt of bijvoorbeeld weigert om een fatsoenlijk gesprek te voeren, geeft het systeem door middel van een foutcode aan dat de uitkomst van de stemherkenningscheck negatief is. In dat geval is duidelijk dat de voetbalsupporter niet aan zijn aantoonplicht voldoet.[240] Hierop staat een strafrechtelijke en een bestuursrechtelijke sanctie. De aard en ernst van de sancties moet zodanig zijn, dat de bereidheid om het stadiongebiedsverbod na te leven groot is.

Aan het gebruikmaken van speaker recognition kleven ook nadelen. Zo bestaat er altijd een kans op fouten. Er zijn verschillende factoren die de betrouwbaarheid van de speaker recognition kunnen beïnvloeden. Het antwoord op de vraag in welke mate dit risico bestaat, hangt sterk samen met de kwaliteit van het gekozen systeem.

Ten slotte bestaat er altijd een risico dat de database wordt gehackt of dat politieambtenaren de gegevens voor andere doeleinden gebruiken. Deze risico's kunnen tot een aanvaardbaar niveau worden teruggebracht, door gebruik te maken van encrypties en een procedure via een streng protocol. De procedure moet zo strikt zijn, dat slechts een select aantal personen toegang heeft tot de database met de versleutelde gegevens en dat men een eenmaal gebruikte sleutel direct zal vervangen.

6.2.4 *Voor- en nadelen van digitaal surveilleren*

Digitale surveillance kan op verschillende manieren plaatsvinden, maar het versturen van sms-berichten in combinatie met het gebruik van gps en een speciale app geniet de voorkeur. Het gebruik van deze methode heeft als voordeel dat de politie op afstand na kan gaan of de telefoon van de supporter zich in het verboden stadiongebiedsverbod bevindt. In combinatie met de speaker recognition kan zo worden vastgesteld of de voetbalsupporter het verblijfsverbod naleeft. Daar komt nog bij dat digitale surveillance de bewegingsvrijheid en het privacyrecht van de supporter veel minder beperkt.

Digitaal surveilleren via gps en een speciale app heeft als nadeel dat de politie voor een deel afhankelijk is van de provider, aangezien zij toegang moet hebben tot of in het bezit moet zijn van een database met locaties van publieke

240 De verantwoordelijkheid voor het naleven van het stadiongebiedsverbod en het voldoen aan de digitale aantoonplicht ligt geheel bij de desbetreffende persoon.

zendmasten. Over het algemeen beschikt de politie echter over deze locatiegegevens. Een ander bezwaar is dat de politie deze methode niet bij elke mobiele telefoon kan toepassen.

6.3 Concluderende opmerkingen

De meldingsplicht van artikel 172a Gemw levert in de praktijk de nodige complicaties op. Een digitale aantoonplicht lost een groot deel van die problemen op. Hij neemt het probleem met de beperkte openingstijden van politiebureaus alsook het hiermee samenhangende probleem van hooliganimport weg.

Een digitale aantoonplicht is bovendien effectiever dan de huidige meldingsplicht van artikel 172a Gemw. De politie kan meer dan één keer, dus intensiever, controleren of de voetbalsupporter zich aan de gebiedsontzegging houdt. Bovendien beperkt een digitale aantoonplicht de bewegingsvrijheid van de supporter en diens privacyrecht veel minder. De voetbalsupporter kan vanaf elke willekeurige plaats aantonen dat hij zich niet in het verboden gebied bevindt en hij wordt slechts enkele minuten met de gedragsaanwijzing geconfronteerd.

Belangrijk is dat de verantwoordelijkheid om het stadiongebiedsverbod na te leven geheel bij de voetbalsupporter zelf ligt. Wanneer hij niet wil meewerken aan de speaker recognition of de digitale surveillance, heeft hij niet aan zijn aantoonplicht voldaan en kan hij met (zwaardere) sancties worden geconfronteerd.

Een digitale aantoonplicht heeft voor de aanpak van voetbalvandalisme door burgemeesters en de politie derhalve toegevoegde waarde.

7

Conclusie

7.1 Inleiding

Voetbalgerelateerde verstoring van de openbare orde is een zeer specifieke en complexe vorm van overlast, die een eigen aanpak en een eigen sanctionering verlangt. Om voetbalgerelateerde overlast efficiënter en effectiever te kunnen bestrijden, is in 2010 in de Gemw een nieuw artikel opgenomen. Op grond van artikel 172a Gemw kan de burgemeester aan een voetbalsupporter een gebieds- of groepsverbod en/of een meldingsplicht opleggen.

Ondanks deze nieuwe bevoegdheden lukt het nog altijd niet om doeltreffend tegen voetbalgerelateerde verstoringen van de openbare orde op te treden. Dit heeft verschillende oorzaken. Een niet goed functionerende meldingsplicht is er een van.

In dit onderzoek is daarom gekeken of het mogelijk is om in plaats van, dan wel naast de meldingsplicht, een systeem te ontwikkelen met behulp waarvan de politie tijdens een wedstrijd op elk gewenst moment kan controleren of de voetbalsupporter het stadiongebiedsverbod naleeft. Hierbij hebben twee uitgangspunten centraal gestaan: een dergelijk systeem zou de politie minder inspanningen moeten kosten en het zou om een waterdicht controlesysteem moeten gaan.

7.2 Problemen met betrekking tot de meldingsplicht

De meldingsplicht van artikel 172a Gemw blijkt in de praktijk (nog) niet goed te functioneren. Dat heeft met de toepassingsvoorwaarden van de bevoegdheid te maken. De voorwaarden zijn erg streng. De burgemeester dient aan te tonen dat de voetbalsupporter de openbare orde herhaaldelijk heeft verstoord en dat er sprake is van ernstige vrees dat de supporter dit opnieuw zal doen. Vanwege de aard van de verstoring en het feit dat voetbalsupporters opmerkelijk weinig registraties in de politiesystemen hebben, is het moeilijk om een gedocumenteerd dossier op te bouwen. In de praktijk is het voor de burgemeester derhalve

niet altijd makkelijk om te bewijzen dat het noodzakelijk en gerechtvaardigd is om de supporter een gedragsaanwijzing te geven.

Daarnaast blijkt de meldingsplicht een minder doeltreffend controlemiddel dan verwacht. De inhoud van de meldingsplicht is te beperkt en de duur van de gedragsaanwijzing te kort om een stadionbezoek door een verbannen supporter te verhinderen. De onmogelijkheid om de meldingsplicht op te leggen voor uitwedstrijden is een groot gemis, want juist hiervoor zou hij uiterst effectief kunnen zijn. De meldplek dient ver genoeg verwijderd te zijn van het verboden gebied, dit doet zich nu alleen voor bij toepassing van de intergemeentelijke meldingsplicht.

Op dit moment kan de meldingsplicht alleen voor thuiswedstrijden worden opgelegd. In zo'n situatie heeft hij echter te weinig toegevoegde waarde: de meldplek is veelal te dicht bij het verboden stadion. Een meldingsplicht zou in dat geval wel effectief kunnen werken, indien de voetbalsupporter zich meerdere keren op het politiebureau zou moeten melden. In verband met de bewegingsvrijheid en het privacyrecht van de supporter kan men echter vraagtekens zetten bij de toelaatbaarheid daarvan.

De inrichting en de uitvoering van de meldingsplicht leveren evenzeer problemen op. De administratieve lasten zijn hoog en hij vergt van de gemeente en de politie de nodige capaciteit. Door de beperkte openingstijden van politiebureaus 'importeert' de burgemeester met een meldingsplicht op een politiebureau bovendien soms ongewild hooligans in zijn gemeente.

7.3 Een digitale aantoonplicht

Om al deze redenen hebben we onderzoek gedaan naar een aantoonplicht naast of in plaats van de meldingsplicht. Het betreft een bevoegdheid van de burgemeester om een voetbalsupporter een bevel te geven voor, tijdens en na een wedstrijd aan te tonen dat hij zich niet op de verboden tijdstippen in het verboden gebied of in het stadion bevindt. Door het gebruik van speciale apparatuur en software kan die nalevingscontrole (vrijwel) geheel autonoom op afstand plaatsvinden. Een speciaal voor de aantoonplicht ontwikkeld systeem zal op willekeurige tijdstippen voor aanvang, tijdens en/of na afloop van de voetbalwedstrijd telefonisch contact opnemen met de supporter. Vervolgens zal er een digitale surveillance en een speaker recognition worden uitgevoerd.

7.3.1 Inrichting van het systeem

Bij de digitale aantoonplicht zijn er drie verschillende fasen te onderscheiden. De eerste fase is de voorbereidende fase. In deze fase verzamelt de politie de voor de digitale surveillance en de speaker recognition benodigde gegevens. Men moet hierbij denken aan gegevens als de naam, het telefoonnummer en stemgeluid van de voetbalsupporter, gegevens over de duur en de omvang van het aan hem opgelegde stadiongebiedsverbod en een aantal Cell-ID's die nodig zijn voor de digitale surveillance.

In de tweede fase vindt een digitale surveillance plaats. Hiermee kan het politiesysteem op afstand vaststellen dat de voetbalsupporter zich niet in het verboden gebied bevindt. Er zijn verschillende manieren denkbaar om digitaal te surveilleren. Het blijkt niet handig te zijn om door middel van een driehoeksmeting digitaal te surveilleren, het gebruik van deze methode stuit op onoverkomelijke bezwaren. Om te beginnen is de politie voor het verrichten van een driehoeksmeting geheel afhankelijk van de providers, terwijl deze over het algemeen juist minder bereid zijn om hieraan mee te werken. Verder is ons gsm-netwerk niet op het verrichten van driehoeksmetingen ingericht en blijkt uit de ervaringen van het KLPD dat deze plaatsbepalingsmethode niet altijd werkt.

Gedurende het onderzoek is de mogelijkheid onderzocht om met het versturen van zichtbare sms-berichten een Cell-ID te verkrijgen. In het strafrecht wordt een soortgelijke methode, bekend onder de naam stealth sms-berichten, reeds toegepast. Over het algemeen is daarvoor het plaatsen van een telefoontap noodzakelijk, waardoor het bij de digitale aantoonplicht onmogelijk lijkt om met het versturen van zichtbare sms-berichten een digitale surveillance te verrichten. Uit het onderzoek blijkt echter dat de politie door het gebruik van gps en een speciaal voor de digitale aantoonplicht ontwikkelde app wel een Cell-ID kan verkrijgen.

Voor het digitaal surveilleren via gps en een speciale app is vereist dat de voetbalsupporter over een telefoon beschikt die is uitgerust met een gps-ontvanger. De aantoonplichtige dient een speciaal voor de aantoonplicht ontwikkeld programma op zijn telefoon te installeren. Op de dag van de voetbalwedstrijd ontvangt de aantoonplichtige door het systeem een sms-bericht dat hij zich moet melden. Wanneer de supporter zich vervolgens aanmeldt, zorgt het programma ervoor dat de gsm-mast het Cell-ID opstuurt. De politie kan op deze manier binnen een paar seconden nadat een voetbalsupporter zich heeft aangemeld een Cell-ID verkrijgen en derhalve digitaal surveilleren.

In de derde en laatste fase vindt er een speaker recognition plaats, zodat de politie kan vaststellen dat het daadwerkelijk de aantoonplichtige is die zij op naleving van het stadiongebiedsverbod controleert. Het betreft een biometrische toets op afstand. Er zijn verschillende factoren die de betrouwbaarheid van de speaker recognition kunnen beïnvloeden, denk aan omgevingsgeluid, de verbinding of ziekte en verkoudheid. Het verdient derhalve aanbeveling om bij de ontwikkeling van het systeem rekening te houden met factoren die de betrouwbaarheid van de speaker recognition kunnen beïnvloeden. Een pilot kan inzage verschaffen in wat een acceptabel percentage EER is. Het verkrijgen van 100 procent zekerheid is alleen mogelijk, indien men de test een of twee keren herhaalt.

Het systeem geeft na het uitvoeren van de digitale surveillance en de speaker recognition op een duidelijke manier voor de eindgebruiker aan of de uitkomst bij identificatienummer X positief of negatief is. Het systeem kan zo worden ingericht, dat aan de gebruikerskant slechts zichtbaar is of het systeem geheel heeft kunnen draaien of dat identificatienummer X, vanwege een negatieve digitale surveillance of speaker recognition, uit het systeem is gegooid. Bovendien kan het systeem, indien nodig, tussentijds een signaal afgeven, zodat de politie andere maatregelen kan treffen. Belangrijk is dat het systeem zo wordt ingericht, dat het de voetbalsupporter en de politie zo min mogelijk belast.

7.3.2 *Een aantoonplicht bij autonome verordening*

De bevoegdheid om een aantoonplicht op te leggen, kan worden opgenomen in een plaatselijke verordening. Dat blijkt uit ons onderzoek. Het recht op privacy, zoals vastgelegd in artikel 10 Gw, staat hieraan niet in de weg.

In de rechtspraak wordt een uitzondering op de door de grondwetgever aangebrachte beperkingensystematiek toegelaten. Dat is het geval indien er slechts sprake is van een geringe inbreuk. Bij deze geringe-inbreuktoets kijkt de rechter naar de duur, intensiteit, plaats en het doel van de inbreuk. Toepassing van deze criteria op de aantoonplicht laat zien dat de plicht op alle criteria goed scoort en dat er derhalve slechts sprake is van een geringe inbreuk op het privacyrecht van de betrokkene.

Een digitale aantoonplicht kan bovendien de privacytoets van artikel 8 EVRM doorstaan. De plicht heeft een basis in nationaal recht en is voldoende accessible en foreseeable. De aantoonplicht dient een legitiem doel. Met het opleggen van de plicht beoogt de burgemeester wanordelijkheden en strafbare feiten te voorkomen. Een digitale aantoonplicht is een geschikt middel en voor

zover bekend zijn er geen minder ingrijpende alternatieve manieren om dat doel te verwezenlijken. De fysieke meldingsplicht van artikel 172a Gemw zien wij, evenals de digitale meldzuil waarbij men gebruikmaakt van gezichtsherkenning, als een ingrijpender middel.

Beperking van het privacyrecht is tevens noodzakelijk in een democratische samenleving. De huidige bevoegdheden zijn ontoereikend om voetbalvandalisme effectief en efficiënt te bestrijden. In de praktijk bestaat behoefte aan werkbare alternatieven en voor de invoering van digitale aantoonplicht bestaan relevante en voldoende redenen. De omstandigheden van het geval bepalen of de combinatie van een stadiongebiedsverbod en een digitale aantoonplicht proportioneel is. Pas bij de uitoefening van de bevoegdheden blijkt of het stadiongebiedsverbod en de opgelegde aantoonplicht daadwerkelijk proportioneel zijn. Voor de toepassing van de bevoegdheden kunnen in verband met de proportionaliteit echter verschillende waarborgen worden opgenomen. Hierdoor is voldoende gegarandeerd dat het opleggen van beide gedragsaanwijzingen noodzakelijk is, de burgemeester de bevoegdheden niet willekeurig zal gebruiken en er een behoorlijk evenwicht bestaat tussen het legitieme doel van de burgemeester en het privacyrecht van de voetbalsupporter.

7.3.3 *Privacywetgeving*

Er bestaan vanuit grondwettelijk perspectief geen bezwaren om de bevoegdheid tot het opleggen van een digitale aantoonplicht in een lokale verordening vast te leggen. Dit betekent echter niet dat er geen andere hindernissen te nemen zijn. De politie zal onder meer privacygevoelige informatie gebruiken. Dat vereist dat de aantoonplicht ook in overeenstemming is met de privacywetgeving. Alleen dan is de invoering van deze bevoegdheid juridisch gezien haalbaar.

De Wbp

In het onderzoek zijn de materiële normen van de Wbp geanalyseerd, zodat duidelijk is hoe men bij de digitale aantoonplicht met de verwerking van bepaalde gegevens dient om te gaan. Het gaat hierbij om open normen en in beginsel technologieonafhankelijke begrippen. Belangrijk is dat men telkens een zorgvuldige belangenafweging maakt. Bij die belangenafweging spelen de algemene beginselen van behoorlijk bestuur een rol.

De materiële normen gelden slechts, indien de Wbp daadwerkelijk van toepassing is op de verwerking van de bij de aantoonplicht benodigde gegevens. Het gaat hier om de reikwijdte van de Wbp. De naam, het telefoonnummer en het stemgeluid van de aantoonplichtige, evenals het Cell-ID blijken persoonsgegevens te zijn. Bovendien is er ten aanzien van die gegevens sprake van een verwerking in de zin van de Wbp en doen er zich geen situaties voor waarin de werking van de Wbp is uitgesloten. De Wbp is derhalve geheel van toepassing op de verwerking van deze gegevens.

Wanneer is er sprake van een rechtmatige verwerking van de gegevens? Daarvoor is allereerst vereist dat de politie de persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze verwerkt. Dat betekent dat men conform de algemene beginselen van behoorlijk bestuur moet handelen.

Verder worden er aan het doel van de gegevensverwerking verschillende eisen gesteld. Men mag de gegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzamelen. Bij het reguleren van de aantoonplicht kan, mede in verband met de algemene beginselen van behoorlijk bestuur, voldoende worden gewaarborgd dat het doel welbepaald en uitdrukkelijk is omschreven. Het doel dient tevens gerechtvaardigd te zijn. Bij de digitale aantoonplicht is het voorkomen van voetbalgerelateerde verstoring van de openbare orde een dragend en juridisch relevant argument voor het verzamelen van de gegevens. Dit doel is bovendien niet in strijd met de wet, openbare orde of de goede zeden. Of het doel gerechtvaardigd is, hangt tevens af van het antwoord op de vraag of de gegevensverwerking op een of meer gronden van de Wbp kan worden gebaseerd. Uit ons onderzoek blijkt dat er voor de verwerking van de naam, het telefoonnummer en het stemgeluid van de aantoonplichtige en de verwerking van Cell-ID's een geldige grondslag valt aan te wijzen.

Twee situaties kunnen worden onderscheiden. De eerste situatie is die waarin de voetbalsupporter vrijwillig meewerkt aan de aantoonplicht. In dat geval geeft hij voor de gegevensverwerking ondubbelzinnige toestemming en levert die verwerking in beginsel geen problemen op.

Bij de tweede situatie is er door de supporter, al dan niet bewust, geen toestemming gegeven voor de verwerking van de gegevens. Er is in dit geval sprake van een onvrijwillige verwerking van persoonsgegevens. Toch kan de politie ook in deze situatie de gegevens verwerken. Dit kan namelijk noodzakelijk zijn om de publiekrechtelijke taak van de burgemeester goed te vervullen dan wel ter behartiging van een gerechtvaardigd belang van de burgemeester. Opge-

merkt dient te worden dat het ook hier belangrijk is dat er een behoorlijke belangenafweging plaatsvindt. Het privacyrecht van de voetbalsupporter mag niet ondergesneeuwd raken, anders is de verwerking van de gegevens onrechtmatig.

De Wbp vereist voorts dat men ervoor zorgt dat de gegevens toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig, en derhalve van voldoende kwaliteit zijn. Het betreft hier een inspanningsverplichting. De burgemeester hoeft dus niet altijd de juistheid van de gegevens te garanderen. Wel dient hij de nodige maatregelen te treffen om de kwaliteit van de gegevens te waarborgen. Dat houdt onder meer in dat er voor alle onderdelen van het proces adequate, zowel technische als organisatorische, beveiligingsmaatregelen worden getroffen. Deze maatregelen moeten in overeenstemming zijn met de huidige stand van de techniek en risico's uitsluiten of in ieder geval beheersbaar maken.

Daarnaast stelt de Wbp eisen aan het bewaren van de gegevens. Men mag de gegevens niet langer bewaren dan noodzakelijk is om het handhavingsdoel te verwezenlijken. Het is aanbevelenswaardig om bij het inrichten van de digitale aantoonplicht zoveel mogelijk naar gegevensminimalisatie en derhalve naar anonimiteit te streven, alsook naar het zo min mogelijk gebruiken van de gegevens, en ze te verwijderen zo gauw als de maatregel is geëindigd.

Op de burgemeester rust overigens een informatieplicht. Hij dient bepaalde informatie, waaronder zijn identiteit en het doel van de gegevensverwerking, aan de aantoonplichtige te verstrekken. Bovendien heeft de aantoonplichtige een inzage- en correctierecht en het recht van verzet.

De Wpg

Ten slotte is onderzocht welke eisen er aan het besluit van de burgemeester om een stadiongebiedsverbod en een aantoonplicht op te leggen, moeten worden gesteld. Belangrijk is dat de burgemeester over de noodzakelijke gegevens beschikt. Hij dient immers aan te tonen dat een specifieke supporter de openbare orde voetbalgerelateerd heeft verstoord en dat het geven van een gedragsaanwijzing noodzakelijk is.

Voor het bewijs zal de burgemeester veelal gebruikmaken van processen-verbaal. Een proces-verbaal bevat persoonsgegevens die in het kader van de uitoefening van de politietaak zijn verwerkt. Op de verwerking en derhalve ook op het verstrekken van deze gegevens aan de burgemeester is niet de Wbp, maar de Wpg van toepassing. De Wpg bevat een wettelijke grondslag voor de gegevens-

verwerking, waardoor de burgemeester voor het opleggen van een aantoonplicht altijd de politiegegevens kan verkrijgen.

7.4 Conclusie

In dit onderzoek hebben wij gekeken of er ook minder arbeidsintensieve alternatieven inzetbaar zijn om de naleving van stadiongebiedsverboden praktisch waterdicht te maken. Onderzocht is of het mogelijk is om een digitale aantoonplicht in te voeren en, zo ja, hoe deze verplichting het beste kan worden ingericht.

Geconcludeerd moet worden dat de invoering van een digitale aantoonplicht technisch gezien goed haalbaar is. Juridisch gezien zijn er evenmin onoverkomelijk hindernissen in het geval van een autonome verordening. Voorwaarde is wel dat men de aantoonplicht zodanig inricht dat het geheel aan de privacywetgeving voldoet.

Een digitale aantoonplicht heeft toegevoegde waarde. Het lost een groot deel van de problemen met de huidige meldingsplicht op. Naar onze mening kunnen burgemeesters en de politie met een dergelijke gedragsaanwijzing voetbalvandalisme efficiënter en effectiever bestrijden.

Wij raden aan om, alvorens tot opname in de wet of een verordening over te gaan, een pilot te draaien met de digitale aantoonplicht om (nog) meer inzicht te verkrijgen in het functioneren van de aantoonplicht en hoe deze aan de systeemkant het beste kan worden ingericht.[241] In plaats van een pilot zouden we de digitale aantoonplicht ook kunnen testen door een eigen testomgeving, met een eigen doelgroep, in het leven te roepen. Op deze manier kan, in een beschermde testomgeving, de werking van de aantoonplicht misschien nog beter worden gecontroleerd.

241 Tijdens het onderzoek is met de regiopolitie Groningen over dit voornemen gesproken.

Lijst van afkortingen

AB	AB Rechtspraak Bestuursrecht (tijdschrift)
ABRvS	Afdeling Bestuursrechtspraak van de Raad van State
app	Applicatie, klein programma dat men op een telefoon kan installeren
APV	Algemene Plaatselijke Verordening
Awb	Algemene wet bestuursrecht
BVH	Basisvoorziening Handhaving
bvo	Betaald voetbal organisatie
BW	Burgerlijk Wetboek
Cbp	College bescherming persoonsgegevens
Cell-ID	Identificatienummer van een publieke zendmast
EER	Equal Error Rate
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
FAR	False Acceptance Rate
FDA	Football Disorder Act
FFR	False Rejection Rate
Gemw	Gemeentewet
GPRS	Global Packet Radio Service
gps	Global positioning system
gsm	Global system for mobile communication
Gw	Grondwet
Inspectie OOV	Inspectie Openbare Orde en Veiligheid
jo.	Juncto (samen met)
KLPD	Korps landelijke politiediensten
KNVB	Koninklijke Nederlandse Voetbalbond
LJN	Landelijk Jurisprudentie Nummer
NJ	Nederlandse Jurisprudentie
Polw 1993	Politiewet 1993

Pro Facto	Bureau voor bestuurskundig en juridisch onderzoek, advies en onderwijs
RFID	Radio Frequency Identification
VNG	Vereniging van Nederlandse Gemeenten
Wbp	Wet bescherming persoonsgegevens
Wet mbveo	Wet maatregelen bestrijding voetbalvandalisme en ernstige overlast
Wpg	Wet politiegegevens
Wpr	Wet persoonsregistraties
WvSv	Wetboek van Strafvordering

Bronnen

Literatuur

Article 29 Data Protection Working Party (2007). *Opinion 4/2007 on the concept of personal data, 01248/07/NL,WP 136*. 20 juni 2007.

Article 29 Data Protection Working Party (2011). *Opinion 13 on Geolocation services on smart mobile devices, 881/11/EN,WP 185*. 16 mei 2011.

Berkouwer, E.C. & J.H.A. van der Grinten (2012). 'De Wet MBVEO (of: Voetbalwet) en de roep om meer'. In: *Gemeentestem*, 2012/29.

Berkvens, C.J.M.A. & J.E.J. Prins (red.) (2007). *Privacyregulering in theorie en praktijk*. Deventer: Kluwer.

Borking, J.J.F.M. (2010). *Privacyrecht is code. Over het gebruik van Privacy Enhancing Technologies*. Deventer: Kluwer.

Bovend'Eert, P.P.T., J.L.W. Broeksteeg, D.E. Bunschoten & J.W.A. Fleuren (2009). *Tekst & Commentaar Grondwet, artikel 10*. Deventer: Kluwer.

Bröring, H.E. (2005). *De bestuurlijke boete*. Deventer: Kluwer.

Brouwer, J.G. & K. Jacobs (2010). 'Naar een Engelse voetbalwet'. In: *Nederlands Juristenblad*, 21.

Brouwer, J.G. & A.E. Schilder (2009). 'De Voetbalwet, Ongekende mogelijkheden'. In: *Tijdschrift voor Sport & Recht*, 2009-3.

Brouwer, J.G. & A.E. Schilder (2011). 'Wet maatregelen bestrijding voetbalvandalisme en ernstige overlast'. In: *Tijdschrift voor Constitutioneel Recht*, 2011-2.

Brouwer, J.G. & M. Vols (2010). 'Autonome verordeningen en artikel 10 Grondwet'. In: *Gemeentestem*, 2010/79.

Burkens, M.C., H.R.B.M. Kummeling, B.P. Vermeulen & R.J.G.M. Widdershoven (2012). *Beginselen van de democratische rechtstaat. Inleiding tot de grondslagen van het Nederlands staats- en bestuursrecht*. Deventer: Kluwer.

Commissie Grondrechten in het digitale tijdperk (2000). *Rapport: Grondrechten in het digitale tijdperk*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Het rapport is te raadplegen via http://www.ivir.nl/dossier/grondrechten/bronnen/rapport_gdt_5-00.pdf.
Corstens, G.J.M. (2011). *Het Nederlands strafprocesrecht*. Deventer: Kluwer.

De Bot, D. & S. Renette (2006). 'Employee, where are thou?'. In: *Privacy & Informatie*, 2006-5.
De Jong, M.A.D.W. (2011). 'De Wet MBVEO: mateloos maakt machteloos'. In: *Jurisprudentie Bestuursrecht Plus*, 79.

Engberts, A.B. (2010). 'Deze wet is een niet te missen kans'. In: *Nederlands Juristenblad*, 1272.

Ferwerda, H.B. & O.M.J. Adang (2005). 'Hooligans in beeld: Van informatie naar aanpak'. In: *Politiekunde*, 7.

Gellaerts, S.L. & C.M. Jobse (2011). *Inleiding ICT en recht*. Deventer: Kluwer.
Grijpink, J.H.A.M. (2009). 'Zinvol, betrouwbaar en veilig gebruik van biometrie'. In: *Privacy & Informatie*, 2009-6.

Henrard, K. (2008). *Mensenrechten vanuit internationaal en nationaal perspectief*. Den Haag: Boom Juridische Uitgevers.
Hijmans, H. (2012). 'Nieuwe Europese regels voor privacy: commissie stelt pakket voor om gegevens ook in het informatietijdperk te beschermen'. In: *Nederlands tijdschrift voor Europees recht*, 2012-4.
Holvast, J. (2004). *Jaarboek privacy 2004*. Aphen aan den Rijn: Kluwer.
Hooghiemstra, T.F.M. & S. Nouwt (2011). *SDU Commentaar Wet bescherming persoonsgegevens*. Den Haag: Sdu Uitgevers.
Huydecoper, S.M. (red.) (2006). *Wet bescherming persoonsgegevens en ICT. Monografieën Recht in Informatietechnologie*. Den Haag: Sdu Uitgevers.

Inspectie Openbare Orde en Veiligheid (2011). *Toepassing in de praktijk. Rapport van de IOOV, wet maatregelen bestrijding voetbalvandalisme en ernstige overlast*.

Jansen, M. (2011). 'Verwerking van persoonsgegevens een inbreuk op artikel 8 EVRM?'. In: *Privacy & Informatie*, 2011-6.

Kielman, H.H. (2010). *Politiële gegevensverwerking en Privacy. Naar een effectieve waarborging*, Den Haag.

Kikkers, H., B. Nienhuis & E.P. Rutkens (2009). 'Testen van informatiesystemen en het gebruik van (geanonimiseerde) persoonsgegevens'. In: *Compact*, 2009-3.

Knol, P.C. & G.J. Zwenne (red.) (2008). *Tekst en Commentaar Telecommunicatiewet*. Deventer: Kluwer.

Koorn, R., H. van Gils, J. ter Hart e.a. (2004). *Privacy Enhancing Technologies. Witboek voor beslissers*. Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Kranenborg, H.R. (2007). *Toegang tot documenten en bescherming van persoonsgegevens in de Europese Unie: over de openbaarheid van persoonsgegevens*. Deventer: Kluwer.

Kranenborg, H.R. & L.F.M. Verhey (2011). *Wet bescherming persoonsgegevens in Europees perspectief*. Deventer: Kluwer.

Minister van Justitie (2011). *Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens*. Den Haag: Ministerie van Justitie.

Minister van Veiligheid en Justitie (2012). *Voetbal en Veiligheid*. Den Haag: Directoraat-Generaal Rechtspleging en Rechtshandhaving, Directie Veiligheid en Bestuur, 4 september 2012.

Muijen, P.J.D.J. (2012). *Politie, informatie en privacy. De Wet politiegegevens toegelicht*. Zutphen: Uitgeverij Paris.

Nederlands Biometrie Forum (2009). 'Betrouwbaar en veilig gebruik van biometrie'. Position paper, Nederlands Biometrie Forum (NBF).

Pro Facto (2012). *Op doel? Evaluatie van de Wet maatregelen bestrijding voetbalvandalisme en ernstige overlast, in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Veiligheid en Justitie*.

Ruifrok, A.C.C. (2006). 'Biometrie: wondermiddelen bestaan niet'. In: *Justitiële verkenningen*, 2006-7.

Sauerwein, L.B. & J.J. Linnemann (2002). *Handleiding voor verwerkers van persoonsgegevens. Wet bescherming persoonsgegevens*. Den Haag: Ministerie van Justitie.

Terstegge, J.H.J. (2000). *De nieuwe Wet bescherming persoonsgegevens. Handleiding voor de praktijk. Reeks acuteel recht voor P&O*. Aphen aan den Rijn: Samsom.
Terstegge, J.H.J., H.H. de Vries, T.A.J. Reinders & I. van der Helm (2001). *Wet bescherming persoonsgegevens*. Deventer: Kluwer.
Titulaer-Meddens, J.M. (2011). 'Tien jaar Wbp. En hoe nu verder?'. In: *Privacy & Informatie*, 2011-5.
Thomassen, W. (2010). *Rapport Staatscommissie Grondwet*.

Van Blarkom, G.W. & J.J. Borking (2001). *Beveiliging van persoonsgegevens, Achtergrondstudies en Verkenningen* 23. Den Haag: Registratiekamer.
Vereniging van Nederlandse Gemeenten (2012). *Evaluatie Wet Maatregelen Bestrijding Voetbalvandalisme en Ernstige Overlast, kenmerk BABVI/U201200785*, 24 mei 2012.

Wessels, L. (2008). *Het vorderen van verkeersgegevens van mobiele telefoons. De hulpverlenende taal van de politie en de bescherming van de persoonlijke levenssfeer van de mobiele beller*. Tilburg: Celsus juridische uitgeverij.
Willemsen, C. (red.) (2008). *Biometrie wat is het, hoe werkt het: Rapport van het Programma Informatievoorziening Strafrechtsketen (Progis) en Justitie*. Den Haag: Ministerie van Justitie.
Winter, H.B. (2009). 'De werking van de Wbp in kaart gebracht: onbekend maakt onbemind'. In: *Regelmaat*, 2009-2.
Winter, H.B., P.O. de Jong, A. Sibma e.a. (2009). *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*. Den Haag: Boom Juridische uitgevers.

Kamerstukken en handelingen

Kamerstukken I 1999/00, 25 892, nr. 92c.
Kamerstukken I 2000/01, 25 892, nr. 200.
Kamerstukken I 2009/10, 31 467, nr. E.
Kamerstukken I 2011/12, 31 570, nr. A (bijlage).

Kamerstukken II 1997/98, 25 892, nr. 3.
Kamerstukken II 2001/02, 28 059, nr. 3.
Kamerstukken II 2007/08, 31 467, nr. 3.
Kamerstukken II 2008/09, 31 467, nr. 9.
Kamerstukken II 2010/11, 25 232, nr. 57.

Kamerstukken II 2011/12, 31 570, nr. 20.
Kamerstukken II 2011/12, 31 570, nr. 22.

Handelingen I 1999/00, nr. 34.
Handelingen I 2009/10, nr. 34.
Handelingen I 2011/12, nr. 18.

Handelingen II 1999/00, nr. 24.
Handelingen II 2008/09, nr. 62.

Jurisprudentie

ABRvS 28 augustus 1995, AB 1996, 204.
ABRvS 21 april 2010, JG 2010/0038, m.nt. L.D. Ruigrok.

EHRM 26 april 1979 (*Sunday Times v.* the United Kingdom).
EHRM 2 augustus 1984 (Malone), NJ 1988, 534.
EHRM 24 april 1990 (Kruslin), NJ 1991, 523.
EHRM 17 juli 2003, no. 44787/98 (P.G. and J.H. v. the United Kingdom).
EHRM 17 juli 2003, no. 63737/00 (Perry v. the United Kingdom).
EHRM 17 februari 2004 (Maestri v. Italy).
EHRM 12 januari 2010, no. 4158/05.

Hof Arnhem 24 januari 2012, LJN BV3076.

HR 9 januari 1987, AB 1987, 231 m. nt. F.H. Burg.
HR 20 januari 2009, LJN BF5603.
HR 23 maart 2010, LJN BK6331.
HR 9 september 2011, NJ 2011/595.

Rb. Amsterdam 18 februari 2011, LJN BP5057.
Rb. Amsterdam 18 februari 2011, AB 2011, 122 m. nt. J.G. Brouwer en A.E. Schilder.
Rb. Amsterdam 8 maart 2011, LJN BP7233.
Rb. Amsterdam 31 mei 2011, LJN BQ9049.
Rb. Amsterdam 3 april 2012, LJN BW1140.
Rb. Amsterdam 3 april 2012, AB 2012, 174 m. nt. J.G. Brouwer en A.E. Schilder.

Rb. Arnhem 8 november 2011, LJN BU3688.
Rb. Arnhem 4 januari 2012, LJN BV0086.
Rb. Breda 20 mei 2011, LJN BQ5217.
Rb. Haarlem 29 april 2011, LJN BQ3272.
Rb. Rotterdam 7 mei 2011, LJN BQ3848.
Rb. Rotterdam 18 mei 2011, LJN BQ5186.
Rb. Rotterdam 11 april 2012, LJN BW 3105.
Rb. 's-Gravenhage 23 juli 2012, LJN BX4292.

Elektronische bronnen

http://ec.europa.eu
http://wetten.overheid.nl
http://www.antenneregister.nl
http://www.biometrieforum.nl
http://www.cbpweb.nl
http://www.ioov.nl
http://www.itl.nist.gov
http://www.ivir.nl
http://www.nist.gov
http://www.njb.nl
http://www.recht.nl
http://www.rijksoverheid.nl
http://www.security.nl
http://www.touch2id.co.uk

Bijlagen

1 Expertmeetings

Bij het onderzoek betrokken personen

Bij het onderzoek is met verschillende personen, waaronder experts en ervaringsdeskundigen op het gebied van ICT en privacy, gesproken. Bij het onderzoek waren de volgende personen betrokken:

- De Jonge, E., Regiopolitie Groningen, projectmanager Research en Innovation;
- Jean Pierre, A., Dienst Uitvoering Onderwijs, functionaris voor de gegevensbescherming;
- Jensma, L., Rijksuniversiteit Groningen, docent Algemene Rechtswetenschap en masterstudent Recht & ICT;
- Klompmaker, J.L., Capgemini, consultant;
- ervaringsdeskundige ICT, Korps landelijke politiediensten;
- specialist in het gebruik van biometrie, Korps landelijke politiediensten;
- Venderbosch, A., Programmadirecteur Politie en Wetenschap.

Het Cbp is, ondanks het voornemen van de onderzoekers, niet bij het onderzoek betrokken. Als reactie op een daartoe formeel ingediend verzoek, liet het College weten dat het geven van adviezen op gespannen voet staat met zijn rol als handhavend toezichthouder en dat het derhalve niet mee kan werken aan het onderzoek naar een digitale aantoonplicht.

Gespreksnotitie Regiopolitie Groningen

Datum: 07-03-2012
Plaats: Rademarkt 12, Groningen
Onderwerp: aantoonplicht

Aanwezig: E. de Jonge (Regiopolitie Groningen), J.G. Brouwer (Rijksuniversiteit Groningen), C. Veen (Rijksuniversiteit Groningen)

Systeem ComProNet

Bij de regiopolitie Groningen zijn ze bezig met het ontwikkelen van een nieuw systeem, het Community Protection Network (ComProNet). Dit systeem maakt gebruik van social media, doordat aan ComProNet een Twitter Alarm Knop (TAK) is gekoppeld. Direct messages van Twitter zijn meer privé. Het systeem beoogt zowel burgers als de politie te helpen met de aanpak van incidenten en de kans op ontdekking op heterdaad te vergroten. Door middel van *real-time data* probeert men incidenten aan te pakken.

Het systeem maakt gebruik van Trackr (gps en Google Maps) en kan slechts worden gebruikt als men beschikt over een telefoon met internet en gps-ontvanger. Via *open search* worden (delen van) zoekinformatie gedeeld. Het bedrijf FindWhere is een bedrijf dat zich bezighoudt met Location Based Service door middel van gps (licentie voor lokaliseren). ComProNet bevindt zich op dit moment nog in de testfase, maar binnen afzienbare tijd zal er een pilot gaan draaien.

Driehoeksmeting

Via Location Based Service (LBS) kan met een driehoeksmeting de plaats ook worden bepaald. Voordeel van dit systeem is dat het altijd aan staat, ook als men zich in een gebouw bevindt. De regiopolitie Groningen test dit systeem via simkaarten. Dit kost ongeveer € 3 per persoon. Belangrijk is dat er een backoffice wordt ingericht. KPN maakt gebruik van *fencing*, daarmee houd je het afstemmen redelijk anoniem.

Aantoonplicht

Na een korte inleiding over de Voetbalwet en de problemen die men in de praktijk ten aanzien van voetbalvandalisme ondervindt, is de aantoonplicht kort uiteengezet. Technisch gezien levert het geen probleem op en zijn er verschillende mogelijkheden om het systeem vorm te geven. Iedereen is het erover eens dat, wanneer we toestemming krijgen van de voetbalsupporter en het dus op basis van vrijwilligheid regelen, de privacy en dergelijke allemaal geen problemen opleveren. Lastiger ligt het wanneer de aantoonplichtige en/of de provider niet mee wil/willen werken.

Volgens De Jonge is het zaak om na te denken over de vraag of, en zo ja hoe, het systeem werkt als men geen medewerking van de voetbalsupporter aan de

aantoonplicht kan afdwingen. Het zou ideaal zijn als men er een wettelijke regel op zou kunnen zetten en zo de provider kan verplichten mee te werken. Het creëren van een formele wet neemt echter jaren in beslag. Wellicht kan op verordeningenniveau het een en ander geregeld worden en anders kan men een pilot als voorwerk op een formeel wettelijke regeling zien.

Kan je een voetbalsupporter en/of de provider verplichten om verkeersgegevens te overleggen? Een voetbalsupporter moet in dat geval, bijvoorbeeld via specificaties (opgevraagd bij de provider), aantonen dat hij zich niet in het verboden gebied bevindt. Volgens De Jonge zal dit niet werken, aangezien dit niet onder de service van telecombedrijven valt. Bij de Regiopolitie Groningen hebben zij dit, weliswaar in andere situaties, reeds ondervonden.

Kan een driehoeksmeting ook zonder toestemming van de aantoonplichtige? De Jonge zet hier een vraagteken bij. Plaatsbepaling ligt erg gevoelig in verband met privacy. Wij willen echter de exacte locatie van de supporter niet weten, maar slechts of hij zich niet in het verboden gebied bevindt. Volgens De Jonge zou het op deze manier omkeren van de bewijslast wellicht kunnen. Hij raadt aan om dit in de driehoek, in ieder geval met het Openbaar Ministerie, af te stemmen.

Vraag is in hoeverre providers (KPN, Vodafone en T-Mobile) bereid zullen zijn om mee te werken. De regiopolitie Groningen werkt met KNP, maar moet daar wel voor betalen.

In Groningen zijn ongeveer tien hooligans actief. Volgens Elle de Jonge is dit een mooi aantal om eventueel een pilot mee te draaien. Belangrijk is dat de aantoonplichtige gebeld moet worden, zodat misbruik zo veel mogelijk is uit te sluiten.

Gespreksnotitie KLPD Driebergen

Datum: 07-11-2012
Plaats: Hoofdstraat 54 Driebergen
Onderwerp: aantoonplicht
Aanwezig: A. Venderbosch (Programmadirecteur Politie en Wetenschap), ervaringsdeskundige ICT (Korps landelijke politiediensten), specialist in het gebruik van biometrie (Korps landelijke politiediensten), J.G. Brouwer (Rijksuniversiteit Groningen), C. Veen (Rijksuniversiteit Groningen), L. Jensma (Rijksuniversiteit Groningen)

Doel van het gesprek

Op 7 november 2012 heeft er een gesprek plaatsgevonden met het KLPD in Driebergen. Doel van het gesprek was om met elkaar van gedachten te wisselen over de wijze waarop de (digitale) aantoonplicht het beste kan worden ingericht. Voorafgaand aan het gesprek is er een lijst met vragen naar het KLPD gestuurd (zie Bijlage 2). Aan de hand van deze vragenlijst is door de betrokkenen over de inrichting van de aantoonplicht van gedachten gewisseld. Alle gesprekspartners keken positief tegen een dergelijke maatregel aan en waren van mening dat een aantoonplicht wellicht ook ingezet kan worden voor de aanpak van bijvoorbeeld grootschalige evenementen.

Stemherkenningscheck

Allereerst is de mogelijkheid van het verrichten van een stemherkenningscheck behandeld. Het KLPD is van mening dat het uitvoeren van een dergelijke check (voice recognition) zeker tot de mogelijkheden behoort. Uiteraard blijft het een statistisch middel dat wordt ingezet voor het voorkomen van overlastgevend gedrag.

Er zijn kort een aantal factoren besproken die de betrouwbaarheid van de voice recognition kunnen beïnvloeden. Er is wetenschappelijk onderzoek gedaan naar stemherkenning bij tweelingen. Omgevingsgeluid kan de stem vervormen. Het antwoord op de vraag of een stemherkenningscheck zal slagen, en de kans op vervorming van de stem door omgevingsgeluid, is afhankelijk van de locatie waar de aantoonplichtige zich bevindt. Bij de aantoonplicht mag men echter van de supporter verwachten dat deze persoon normaal praat en geen andere dingen doet die de stemherkenning negatief (kunnen) beïnvloeden.

Andere factoren die de stemherkenning kunnen beïnvloeden zijn een slechte verbinding met de telefoon en het communicatienetwerk van de provider. Ook ziekte en verkoudheid kan de betrouwbaarheid beïnvloeden. Het is echter onduidelijk in welke mate. Bij de digitale aantoonplicht hoeft dit geen probleem op te leveren. De desbetreffende persoon/supporter is namelijk gebaat bij een dergelijke plicht als alternatief voor de meldingsplicht. Zijn bewegingsvrijheid wordt veel minder beperkt dan bij een fysieke meldingsplicht. Indien blijkt dat een stemherkenning, bijvoorbeeld door een slechte verbinding, niet kan plaatsvinden, kan men verlangen dat de aantoonplichtige zelf terugbelt.

Tijdens het gesprek met het KLPD is eveneens de mogelijkheid van misbruik door spoofing besproken. Het schijnt mogelijk te zijn dat personen door middel van spoofing misbruik maken. De techniek om een computerstem zo men-

selijk mogelijk over te laten komen, kan gebruikt worden om te spoofen. De techniek hiervoor staat echter nog in de kinderschoenen. Het is bovendien onwaarschijnlijk dat de personen die een aantoonplicht opgelegd krijgen deze techniek inkopen, ze is namelijk zeer prijzig. Doorgaans zijn het criminelen met veel financiële middelen die deze techniek inkopen.

Het uitvoeren van een stemherkenningscheck is een statistisch middel, waarbij er een kans op fouten bestaat. Vroeger had men systemen waarbij de EER 7 procent was. Inmiddels zijn er systemen beschikbaar die een EER van 3 procent laten zien. De kans op fouten hangt af van de kwaliteit, die weer beïnvloed wordt door de lengte van het gesprek dat men met een persoon voert. De technologie is nog niet zover dat een EER onder de 3 procent haalbaar is. Een gesprek van ongeveer zeven à tien seconden zou genoeg kunnen zijn, maar (extern) onderzoek en ook de ervaringen van het KLPD met stemherkenning laten zien dat de kwaliteit bij een gesprek dat bijvoorbeeld een minuut of anderhalve minuut geduurd heeft vele malen beter is.

Een niet onbelangrijke vraag is hoe groot de kans is dat het systeem meerdere keren een persoon ten onrechte wel of niet herkent. Volgens het KLPD is dit statisch te berekenen. In dat geval heb je het wel over de meest optimale situatie, terwijl er altijd factoren zullen zijn die men niet onder controle kan hebben. Denk hierbij aan factoren als het communicatienetwerk van de provider, omgevingsgeluiden of bijvoorbeeld de vraag of een persoon al dan niet meewerkt aan de stemherkenningscheck. De kans dat het systeem meerdere malen een persoon ten onrechte wel of niet herkent zal waarschijnlijk minder dan 3 procent zijn.

Tegenwoordig is het niet meer zeker dat men door het verrichten van een stemherkenning met een vaste telefoon betere resultaten verkrijgt dan met een dergelijke check via een mobiele telefoon. Met een vaste telefoon had men vroeger een meer constant resultaat. De technologie met betrekking tot mobiele netwerken is wat betreft de kwaliteit wel verbetert, maar via een vaste telefoon is deze nog altijd beter. Door het maken van een speciale app kan men de aantoonplichtige wellicht een keuzemogelijkheid geven. Hij kan zich dan vanuit huis of via de op zijn smartphone geïnstalleerde app melden en dus aantonen dat hij het gebiedsverbod naleeft. Dan bestaat er een goede kans dat men goede informatie verkrijgt, waar men wat mee kan.

Wat betreft de kosten voor hardware en software, gaat het merendeel van de kosten niet zitten in de licentie van de leverancier voor stemherkenning. Het (willen) leveren van maatwerk is wel een kostbare zaak. Echter ook hier is niet uit te sluiten dat er bedrijven zijn die software waarmee maatwerk kan worden

geleverd reeds hebben ontwikkeld. Het KLPD gebruikt software van Agnitio. Dit bedrijf uit Madrid heeft drie soorten software ter beschikking. Allereerst is er software die verkocht wordt aan forensische laboratoria. Het betreft in dit geval ingewikkelde software, waarmee experts werken. Verder is er de BS3 die met JAVA is aan te sturen. Hierbij kan een een-op-een vergelijking worden gedaan. Ten slotte bestaat er nog software waarbij het systeem een spreker met heel veel sprekers uit een database vergelijkt.

Ten aanzien van de stemherkenningscheck kan worden geconcludeerd dat dit technisch haalbaar is, waarbij een combinatie van een smartphone met gps en een speciale app een mooi resultaat kan geven. Bovendien is de kans dat een persoon wil meewerken bij een digitale aantoonplicht waarschijnlijk groter, aangezien deze zich niet fysiek ergens hoeft te melden en dus een bepaald gedeelte van zijn dag hieraan kwijt is.

Digitale surveillance

Bij de aantoonplicht zal eveneens een digitale surveillance plaatsvinden. Het KLPD kijkt tegen een aantal methoden om digitaal te surveilleren wat kritischer aan.

Over sms-berichten

Bij het versturen van sms-berichten ben je afhankelijk van de provider. De politie maakt soms gebruik van deze methode in het kader van de hulpverleningstaak op grond van artikel 2 Politiewet 1993. Uit de ervaringen van de politie blijkt dat een aantal providers hun gsm-mastennetwerk open heeft staan of open zet. Een ander deel van de providers kan en/of wil dit niet doen. In de praktijk bestaat hier discussie over. Met verborgen stealth sms-berichten kan men slechts een Cell-ID terugkrijgen als er ook een telefoontap op staat. Als de provider de gsm-masten open heeft staan, kan het wel zonder tap, maar indien dit niet het geval is, werkt het niet. Veel providers hebben hun netwerken dichtgezet. In Amerika is dit zelfs bij wet geregeld en kan je op deze manier niemand lokaliseren.

Een contactpersoon bij het KLPD verkrijgt iedere maand een geüpdatedatabase met Cell-ID's. Deze wordt in het systeem ingevoerd. Het KLPD verkrijgt de database van de providers, maar mag deze niet aan iedereen verstrekken aan. De gegevens worden derhalve door de providers centraal aangeleverd, waarbij het KLPD deze weer middels invoering in het systeem voor bepaalde personen beschikbaar stelt. De gegevens worden alleen verstrekt aan personen die kunnen aantonen dat ze deze gegevens nodig hebben voor hun werk.

Driehoeksmeting

Het KLPD staat wat minder positief tegenover het digitaal surveilleren middels een driehoeksmeting. Er zijn proeven gedaan, waaruit blijkt dat het soms heel mooi kan werken, maar de volgende dag ineens niet meer werkt. Providers zijn over het algemeen minder bereid om mee te werken aan het verrichten van een driehoeksmeting. Bovendien is ons gsm-netwerk niet op het verrichten van driehoeksmetingen ingesteld.

Gps

Bij gps-tracking zou gebruik kunnen worden gemaakt van een speciaal ontwikkelde app. Hiermee kan men Cell-ID's verkrijgen, doordat het programma verbonden is met een gsm-mast. De app zorgt ervoor dat de gsm-mast de Cell-ID opstuurt. De dekking is over het algemeen goed en in steden (rondom stadions) zeer goed. Bij grote evenementen worden soms tijdelijk extra palen neergezet.

Door deze methode is de locatie van de aantoonplichtige niet exact te achterhalen. Voor de aantoonplicht maakt dit echter niet uit. Een ander voordeel van een dergelijke methode is dat men niet afhankelijk is van de provider. De aantoonplichtige moet wel met de installatie van de app op zijn smartphone instemmen.

De kans om deze app te kunnen manipuleren hangt af van de manier waarop het programma ontwikkeld is. Het is bij de app derhalve belangrijk om slim te programmeren. Er bestaat natuurlijk altijd een kans dat de app misbruikt wordt, maar ook hier geldt weer dat het inkopen van de techniek en het verlenen van opdracht voor manipulatie aan ICT'ers veel geld kost. Wel is het zo dat wanneer de app heel erg veel wordt gebruikt, de kans dat deze gemanipuleerd wordt groter is.

Een nadeel van gps is dat het in een gebouw niet werkt. Met een app die het identificatienummer van een gsm-mast doorstuurt, heb je hier minder last van. De aantoonplichtige krijgt bijvoorbeeld een sms-bericht dat hij zich moet aanmelden en binnen een paar seconden krijgt de politie een Cell-ID terug, zodat er een grove lokalisatie kan plaatsvinden.

Er bestaat een kans dat Cell-ID niet wordt herkend. De aantoonplicht kan zo worden ingericht, dat het systeem in dat geval een sms-bericht naar de aantoonplichtige stuurt met daarin het verzoek om zich even opnieuw aan te melden. Dit kan in de software/het programma worden ingebouwd.

Versleuteling

Het systeem kan zo worden ingericht, dat het op de hoogte is van bepaalde gegevens, maar dat de politieambtenaar deze niet kan zien. Dit kan door middel van versleuteling. Technisch is een dergelijk systeem te realiseren. Maar het zorgt ervoor dat het systeem wel tamelijk complex wordt. Bij een technische storing moet men uiteraard decoderen door gebruik te maken van een bepaalde sleutel. Deze sleutel kan na eenmaal te zijn toegepast niet opnieuw worden gebruikt. Er moet derhalve een strikte procedure zijn, zodat een eenmaal gebruikte sleutel direct wordt vervangen.

Een dergelijk systeem kan werken, maar daarbij is het wel belangrijk dat men goed logt en alles dus controleerbaar is. Indien men kan aantonen dat het systeem alleen tijdens de uren dat het gebiedsverbod van kracht is gedraaid heeft en dus bepaalde gegevens heeft ontvangen en/of gebruikt, zal het geen probleem opleveren. Als de politie kan aantonen wat men wanneer heeft gedaan, is er ook bij digitale surveillance middels een speciale app geen sprake van observatie. Ten aanzien van het versturen van stealth sms-berichten is inmiddels een zaak aanhangig met betrekking tot de vraag of er sprake is van stelselmatige observatie.

Het systeem kan zo worden ingericht, dat het tussendoor meldingen geeft ten aanzien van personen vanwie duidelijk is dat zij zich niet aan het stadiongebiedsverbod houden. Het is belangrijk om de alarmering dan ruim in te vullen.

2 Vragenlijst inrichting aantoonplicht

Stemherkenningscheck

1 Hoe zit het men de betrouwbaarheid van stemherkenning?
   a In hoeverre beïnvloedt ziekte/verkoudheid de betrouwbaarheid?
   b Kan omgevingsgeluid de stem vervormen en, zo ja, hoe groot is de kans daarop?
   c Zijn er nog andere factoren die een stemherkenning (kunnen) beïnvloeden?
   d Hoe zit het met misbruik/fraude bij stemherkenning (is er bijvoorbeeld een risico op spoofing)?
   e Hoe groot is de kans op fouten (FAR, FRR et cetera)?
   f In hoeverre kan spraakherkenning een waardevolle aanvulling zijn op een stemherkenning? Kan je met een spraakherkenning de betrouwbaarheid van de stemherkenning vergroten?
   g Verkrijgt men met een mobiele telefoon betere resultaten dan met een stemherkenning via de vaste telefoon?
2 Hoe snel kan een stemherkenning plaatsvinden?
3 Kosten:
   a Wat zijn de kosten voor hardware?
   b Wat zijn de kosten voor software?
4 Welke software en apparatuur e.d. gebruikt de organisatie voor de stemherkenning en wat zijn de ervaringen met de software/apparatuur?

Digitale surveillance algemeen

1 Kan de digitale surveillance geheel automatisch?

Sms-berichten

1 Is het mogelijk om sms-berichten zichtbaar te versturen en zo toch Cell-ID te verkrijgen?
2 Ben je bij sms-berichten afhankelijk van de provider?
3 Hoeveel sms-berichten kunnen worden verstuurd naar de supporter in verband met het recht op privacy?
4 Betrouwbaarheid/nauwkeurigheid?

Driehoeksmeting

1 In hoeverre is de politie bij een driehoeksmeting afhankelijk van de provider?
2 Betrouwbaarheid:
   a Hoe nauwkeurig is de plaatsbepaling? In gebieden met een behoorlijk aantal gsm-masten en dus een hoge dekkingsgraad zal de plaatsbepaling nauwkeuriger zijn, maar wat is ongeveer haalbaar?
   b In hoeverre is een driehoeksmering fraudegevoelig?
3 Organisatorisch:
   a Hoe snel kan een driehoeksmeting plaatsvinden?
   b Hoe vindt er binnen de organisatie een driehoeksmeting plaats?
   c Welke software levert goede resultaten op en hoe is het systeem opgebouwd?
   d Tegen welke problemen liep men bij het inrichten van het systeem aan?
   e Ondervindt men bij het verrichten van een driehoeksmeting wel eens problemen en, zo ja, tegen welke problemen loopt men dan aan?
   f Hoe wordt er omgegaan met technische storingen?

Gps

1 Bij het gebruik van gps is de plaatsbepaling nauwkeuriger dan bij een driehoeksmeting, maar hoe zit het met de betrouwbaarheid van gps-tracking?
2 Hoe wordt er binnen de organisatie omgegaan met gps-tracking? Hoe is het systeem ingericht, welke software e.d. wordt er gebruikt en wat zijn de positieve en eventueel negatieve ervaringen?
3 Hoe snel kan men de locatie van een persoon bepalen?

Leden Redactieraad Programma Politie & Wetenschap

Secretariaat Programmabureau Politie & Wetenschap
Politieacademie
Arnhemseweg 348
7334 AC Apeldoorn

Postbus 834
7301 BB Apeldoorn
www.politieenwetenschap.nl

Uitgaven in de reeks Politiekunde

1. ***Criminaliteit in de virtuele ruimte***
   P. van Amersfoort, L. Smit & M. Rietveld, DSP-groep, Amsterdam/ TNO-FEL, Den Haag, 2002
2. ***Cameratoezicht. Goed bekeken?***
   I. van Leiden & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2002
3. ***De 10 stappen van Publiek-Private Samenwerking (PPS)***
   J.C. Wever, A.A. van Pel & L. Smit, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002
4. ***De opbrengst van projecten. Een verkennend onderzoek naar de bijdrage van projecten aan diefstalbestrijding***
   C.J.E. In 't Velt, e.a., NPA-Onderzoeksgroep, LSOP, Apeldoorn, 2003
5. ***Cameratoezicht. De menselijke factor***
   A. Weitenberg, E. Jansen, I. van Leiden, J. Kerstholt & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem/TNO, Soesterberg, 2003
6. ***Jeugdgroepen in beeld. Stappenplan en randvoorwaarden voor de shortlist-methodiek***
   H.B. Ferwerda & A. Kloosterman, Advies- en Onderzoeksgroep Beke & Politieregio Gelderland-Midden, Arnhem, 2004 (vierde druk 2006)
7. ***Hooligans in beeld.Van informatie naar aanpak***
   H.B. Ferwerda & O. Adang, Advies- en Onderzoeksgroep Beke, Arnhem/ Onderzoeksgroep Politieacademie Apeldoorn, 2005
8. ***Richtlijnen auditieve confrontatie***
   J.H. Kerstholt, A.G. van Amelsfoort, E.J.M. Jansen & A.P.A. Broeders, TNO Defensie en Veiligheid, Soesterberg/Politieacademie, Apeldoorn/NFI, Den Haag, 2005
9. ***Niet verschenen***
10. ***De opsporingsfunctie binnen de gebiedsgebonden politiezorg***
    O. Zoomer, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2006
11. ***Inzoomen en uitzoomen op Zaandam***
    I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem 2006
12. ***Aansprakelijkheidsmanagement politie. Beschrijving, analyse en handreiking***
    E.R. Muller, J.E.M. Polak, C.J.J.M. Stoker m.m.v. M.L. Diepenhorst & S.H.E. Janssen, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag/Faculteit der Rechtsgeleerdheid Universiteit Leiden, 2006

13. ***Cold cases – een hot issue***
I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem, 2006

14. ***Adrenaline en reflectie. Hoe leren politiemensen op de werkplek?***
A. Beerepoot & G. Walraven e.a., DSP-groep BV, Amsterdam/Walraven onderzoek en advies, 2007

15. ***Tussen aangifte en zaak. Een referentiekader voor het aangifteproces***
W. Landman, L.A.J. Schoenmakers & F. van der Laan, Twynstra Gudde, adviseurs en managers, Amersfoort, 2007

16. ***Baat bij de politie. Een onderzoek naar de opbrengsten voor burgers van het optreden van de politie***
M. Goderie & B. Tierolf, m.m.v. H. Boutellier & F. Dekker, Verwey-Jonker Instituut, Utrecht, 2008

17. ***Hoeveel wordt het vandaag? Een studie naar de kans op voetbalgeweld en het veiligheidsbeleid bij voetbalwedstrijden***
E.J. van der Torre, R.F.J. Spaaij & E.D. Cachet, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2008

18. ***Overbelast? De administratieve belasting van politiemensen bij de afhandeling van jeugdzaken***
G. Brummelkamp & M. Linssen, EIM, Zoetermeer, 2008

19. ***Geografische daderprofilering. Een inventarisatie van randvoorwaarden en succesfactoren***
G. te Brake & A. Eikelboom, TNO Defensie en Veiligheid, Soesterberg, 2008

20. ***Solosurveillance. Kosten en baten***
S.H. Esselink, J. Broekhuizen & F.M.H.M. Driessen, Bureau Driessen, 2009

21. ***Onderzoek naar de mogelijke meerwaarde van AWARE voor de politie. Ervaringen met een nieuwe aanpak van belaging door ex-partners***
M.Y. Bruinsma, J. van Haaf, R. Römkens & L. Balogh, IVA Beleidsonderzoek en Advies, i.s.m. INTERVICT/Universiteit van Tilburg, 2008

22. ***Gebiedsscan criminaliteit en overlast. Een methodiekbeschrijving***
B. Beke, E. Klein Hofmeijer & P. Versteegh, Bureau Beke, Arnhem, 2008

23. ***Informatiemanagement binnen de politie. Van praktijk tot normatief kader***
V. Bekkers, M. Thaens, G. van Straten & P. Siep; m.m.v. A. Dijkshoorn, Center for Public Innovation, Erasmus Universiteit Rotterdam, 2009

24. ***Nodale praktijken. Empirisch onderzoek naar het nodale politieconcept***
H.B Ferwerda, E.J van der Torre & V. van Bolhuis, Bureau Beke, Arnhem/COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

25. *Rellen om te rellen. Een studie naar grootschalige openbare-ordeverstoringen en notoire ordeverstoorders*
I. van Leiden, N. Arts & H.B. Ferwerda, Bureau Beke, Arnhem, 2009

26a. *Verbinden van politie- en veiligheidszorg. Politie en partners over signaleren & adviseren*
W. Landman, P. van Beers & F. van der Laan, Twynstra Gudde, Amersfoort, 2009

26b. *Politiepolitiek. Een empirisch onderzoek naar politiële signalering & advisering*
E.J.A. Bervoets, E.J. van der Torre & J. Dobbelaar m.m.v. N. Koeman, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

27. *De politie aan zet: de aanpak van veelplegers in Deventer*
I. Bakker & M. Krommendijk, IPIT, Enschede, 2009

28. *Boven de pet? Een onderzoek naar grootschalige ordehandhaving in Nederland*
O.M.J. Adang (redactie), S.E. Bierman, K. Jagernath-Vermeulen, A. Melsen, M.C.J. Nogarede & W.A.J. van Oorschot, Politieacademie, Apeldoorn, 2009

29. *Rellen in Ondiep. Ontstaan en afhandeling van grootschalige ordeverstoring in een Utrechtse achterstandswijk*
G.J.M. van den Brink, M.Y. Bruinsma (redactie), L.J. de Graaf, M.J. van Hulst, M.P.C.M. Jochoms, M. van de Klomp, S.R.F. Mali, H. Quint, M. Siesling, G.H. Vogel, Politieacademie, Apeldoorn, 2010

30. *Burgerparticipatie in de opsporing. Een onderzoek naar aard, werkwijzen en opbrengsten*
A. Cornelissens & H. Ferwerda (redactie), met medewerking van I. van Leiden, N. Arts & T. van Ham, Bureau Beke, Arnhem, 2010

31. *Poortwachters van de politie. Meldkamers in dagelijks perspectief*
J. Kuppens, E.J.A. Bervoets & H. Ferwerda, Bureau Beke, Arnhem & COT, Den Haag, 2010

32. *Het integriteitsbeleid van de Nederlandse politie: wat er is en wat ertoe doet*
M.H.M. van Tankeren, Onderzoeksgroep Integriteit van Bestuur, Vrije Universiteit Amsterdam, 2010

33. *Civiele politie op vredesmissie. Uitzendervaringen van Nederlandse politiefunctionarissen*
H. Sollie, Universiteit Twente, Enschede, 2010

34. *Ten strijde tegen overlast. Jongerenoverlast op straat: is de Engelse aanpak geschikt voor Nederland?*
M.L. Koemans, Universteit Leiden, 2010

35. ***Het districtelijk opsporingsproces; de black box geopend***
R.M. Kouwenhoven, R.J. Morée &. P. van Beers, Twynstra Gudde, Amersfoort, 2010

36. ***Balanceren tussen alert maken en onrust voorkomen. Publiekscommunicatie over seriële schokkende incidenten (casestudy Lelystad)***
A.J.E. van Hoek, m.m.v. P.F. van Soomeren, M.D. Abraham & J. de Kleuver, DSP-groep, Amsterdam, 2011

37. ***Sturing van blauw. Een onderzoek naar operationele sturing in de basispolitiezorg***
W. Landman, m.m.v. M. Malipaard, Twynstra Gudde, Amersfoort, 2011

38. ***Onder het oppervlak. Een onderzoek naar ontwikkelingen en (a)select optreden rond preventief fouilleren***
J. Kuppens, B. Bremmers, E. van den Brink, K. Ammerlaan & H.B. Ferwerda, m.m.v. E.J. van der Torre, Bureau Beke, Arnhem/COT, Den Haag, 2011

39. ***Naar eigen inzicht? Een onderzoek naar beoordelingsruimte van en grenzen aan de identiteitscontrole***
J. Kuppens, B. Bremmers, K. Ammerlaan & E. van den Brink, Bureau Beke, Arnhem/COT, Den Haag, 2011

40. ***Toezicht op zedendelinquenten door de politie in samenwerking met de reclassering***
H.G. van de Bunt, N.L. Holvast & J. Plaisier, Erasmus Universiteit, Rotterdam/Impact R&D, Amsterdam, 2012

41. ***Daders over cameratoezicht***
H.G.A. van Schijndel, A. Schreijenberg, G.H.J. Homburg & S. Dekkers, Regioplan Beleidsonderzoek, Amsterdam, 2012

42. ***Aanspreken op straat. Het werk van de straatcoach in al zijn verschijningsvormen***
L. Loef, K. Schaafsma & N. Hilhorst, DSP-groep, Amsterdam, 2012

43. ***De organisatie van de opsporing van cybercrime door de Nederlandse politie***
N. Struiksma, C.N.J. de Vey Mestdagh & H.B. Winter, Pro Facto, Groningen/Kees de Vey Mestdagh, Groningen, 2012

44. ***Politie in de netwerksamenleving. De opbrengst van de politiële netwerkfunctie voor de kerntaken opsporing en handhaving openbare orde en de sturing hierop in de gebiedsgebonden politiezorg***
I. Helsloot, J. Groenendaal & E.C. Warners, Crisislab, Renswoude, 2012

45. ***Tegenspraak in de opsporing.Verslag van een onderzoek***
R. Salet & J.B. Terpstra, Radboud Universiteit Nijmegen, 2012

46. ***Tunnelvisie op tunnelvisie? Een verkennend en experimenteel onderzoek naar de besluitvorming door VKL-teams met betrekking tot het onderkennen van tunnelvisie en andere procesaspecten***
I. Helsloot, J. Groenendaal & B. van 't Padje, Crisislab, Renswoude, 2012

47. ***M.-waarde. Een onderzoek naar de bijdrage van Meld Misdaad Anoniem aan de politionele opsporing***
M.C. van Kuik, S. Boes, N. Kop, M. den Hengst-Bruggeling, T. van Ham & H. Ferwerda, Politieacademie, Apeldoorn/Bureau Beke, Arnhem, 2012

48. ***Seriebrandstichters. Een verkennend onderzoek naar daderkenmerken en delictpatronen***
Y. Schoenmakers, A. van Wijk & T. van Ham, Bureau Beke, Arnhem, 2012

49. ***Van wie is de straat? Methodiek en lessen voor de politie om ongrijpbare veiligheidsfenomenen grijpbaar te maken – op basis van vijf praktijkcasus***
H. Ferwerda, T. van Ham, B. Bremmers, K. Tijhof & M. Grotens, Bureau Beke, Arnhem, 2013

50. ***Recherchesamenwerking in de Euregio Maas-Rijn. Knooppunten, knelpunten en kansen***
H. Nelen, M. Peters & M. Vanderhallen, Politieacademie, Apeldoorn/ Universiteit Maastricht, 2013

51. ***De operationele politiebriefing onderzocht. Een onderzoek naar de effectiviteit van de operationele politiebriefing***
A. Scholtens, J. Groenendaal & I. Helsloot, Crisislab, Renswoude 2013

52. ***Sociale media: factor van invloed op onrustsituaties?***
R.H. Johannink, I. Gorissen & N.K. van As, Politieacademie Apeldoorn/ VDMMP, Houten, 2013

53. ***De terugkeer van zedendelinquenten in de wijk***
C.E. Huls & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen/Centrum voor Openbare Orde en Veiligheid, Groningen, 2013