

WRIKKEN EN WEGEN OVER GEGEVENS:

**EEN ANALYSE VAN DE WEGING VAN HET BELANG VAN DE BURGER BIJ DE
NIEUWE REGELING VOOR DE STRAFRECHTELIJKE GEGEVENSVERGARING.**

Master's Thesis Rechtsgeleerdheid, Universiteit van Amsterdam

Joris V.J. van Hoboken

Begeleider: dr. mr. Lodewijk F. Asscher

Tweede lezer: prof. dr. mr. Nico A.N.M. van Eijk

9 april 2006

Inleiding	2
Hoofdstuk 1 De Wet bevoegdheden vorderen gegevens	4
Voorgeschiedenis	4
Gegevens of informatie?	6
De nieuwe bevoegdheden	6
Gevolgen van de wet	8
De wet vanuit grondrechtelijk perspectief	10
De inbreuk van de bevoegdheden uit de wet op art. 8 lid 1 EVRM	11
Bij de wet voorzien	12
Noodzakelijk in een democratische samenleving	13
Toetsing van de wet aan de criteria van artikel 8 lid 2 EVRM	14
De noodzakelijkheid van de bevoegdheden	16
Conclusie	18
Hoofdstuk 2 De toegang tot persoonsgegevens in het kader	
van de strafvordering in de Verenigde Staten	19
Het Amerikaanse strafprocesrecht	19
Het verkrijgen van gegevens voor de opsporing	20
De bescherming van persoonsgegevens in de Verenigde Staten	21
Constitutionele bescherming van de privacy	22
Het <i>First Amendment</i>	23
Het <i>Fourth Amendment</i>	24
Ontwikkeling van het privacybegrip in het <i>Fourth Amendment</i>	25
Het <i>Fourteenth</i> en <i>Fifth Amendment</i>	28
Gevolgen voor de toegang tot persoonsgegevens voor de opsporing	30
Conclusie	33
Hoofdstuk 3 De juridische grondslag voor de bescherming van persoonsgegevens	34
Bescherming van persoonsgegevens: privacybescherming of machtsbeheersing	34
De informationele privacy en artikel 8 EVRM	36
De Wet bevoegdheden vorderen gegevens	36
Conclusie	40
Literatuurlijst	42

Inleiding

De ontwikkeling van de informatiemaatschappij heeft gezorgd voor een letterlijk en figuurlijk ongekende stroom aan persoonsgegevens in de private en de publieke sector. De burger laat deze gegevens in zijn dagelijks leven achter bij het contact met de overheid en het gebruik van diensten in de private sector. Hij is hier aan gewend geraakt, evenals aan het idee dat het ondoenlijk is bij te houden wie precies welke gegevens gebruikt voor welke doelen. De burger kan daarbij vertrouwen op een juridische regeling voor de verwerking van persoonsgegevens, de Wet bescherming persoonsgegevens, en de grondrechtelijke bescherming van de privacy. Op die basis heeft de burger onder meer rechten op inzage en verbetering en dienen verwerkers van persoonsgegevens zich te houden aan beginselen van behoorlijke gegevensverwerking, zoals het beginsel van transparantie en het beginsel van doelbinding.

De persoonsgegevens van burgers en in het bijzonder van verdachten van strafbare feiten, die in de maatschappij voor handen zijn, kunnen belangrijke aanknopingspunten bieden voor de opsporing. Waar opsporingsambtenaren echter toegang zoeken tot persoonsgegevens in de maatschappij, stuiten zij tot voor kort op de juridische regeling voor de verwerking van persoonsgegevens, die de toegang in veel gevallen juridisch blokkeerde. De wetgever heeft dit probleem onlangs opgelost door de introductie van een aantal nieuwe strafrechtelijke bevoegdheden voor het vorderen van gegevens. De in de maatschappij aan de verwerking van persoonsgegevens aanwezige informatiemacht is hiermee onder de voorwaarden van de nieuwe wetgeving ontsloten voor de opsporing van strafbare feiten.

De wetgever heeft bij het ontwerp van de regeling voor de toegang een belangenafweging gemaakt tussen het belang van de opsporing van strafbare feiten, het belang van de burger tegen inbreuken in zijn persoonlijke levenssfeer en een zorgvuldig gebruik van gegevens die op hem betrekking hebben, en het belang van de houder van de gegevens. In deze belangenafweging heeft het belang van de opsporing van strafbare feiten, ten gevolge van het gewicht dat de overheid momenteel aan het zorgen voor veiligheid toekent, de nodige nadruk gekregen. De veiligheid voor burgers omvat echter naast een leefomgeving vrij van criminaliteit, ook het belang van burgers voor onredelijke inbreuken door politie en justitie zelf behoed te zijn.

De nieuwe wet is tot stand gekomen met een stevige duw in de rug door de maatschappelijke ontwikkelingen op nationaal Europees en internationaal niveau. In de politiek wordt met succes de veiligheid voor de burger op de voorgrond gesteld en de publieke opinie verzet zich nauwelijks tegen verdere inbreuken op burgerrechten door verdergaande bevoegdheden voor de strafrechtelijke handhaving, welke gepresenteerd worden als wapens tegen terreur en criminaliteitsbestrijding. De regulering door de overheid van de informatiemaatschappij wordt door dit politieke klimaat, waarin misdaad- en terrorismebestrijding voorop staan, gekleurd.

De vraag in deze scriptie is hoe de wetgever het belang van de burger heeft gewogen. Wat is het aan dit belang gerelateerde normatieve kader voor de toegang tot persoonsgegevens voor de opsporing, en hoe is dit door de wetgever toegepast? Een belangrijke rol blijkt daarbij te zijn weggelegd voor de toets van artikel 8 van het Europese Verdrag voor de rechten van de mens; er zal bij deze toets dus uitvoerig stil worden gestaan, in het bijzonder bij de vraag of de bevoegdheden wel noodzakelijk zijn in een democratische samenleving. Veel aandacht zal ook uitgaan naar het beginsel van doelbinding. Dit beginsel schrijft immers voor dat gegevens niet mogen worden gebruikt voor andere doelen waarvoor ze zijn verzameld. Het doorbreken van dit beginsel behoeft een zelfstandige rechtvaardiging. De vraag is hoe de wetgever hier invulling aan heeft gegeven.

Om een ander licht te werpen op het in Nederland geldende normatieve kader zal de toegang tot persoonsgegevens voor de opsporing in het Amerikaanse recht uiteen worden gezet. Het Amerikaanse recht vertoont op het punt van het opsporingsonderzoek en de bescherming van persoonsgegevens aanzienlijke verschillen met het Nederlandse recht. Aan de andere kant zijn ontwikkelingen in de Verenigde Staten van grote invloed op de situatie in Europa en Nederland. Naast het begrip privacy zelf, zijn ook veel opsporingstechnieken en nieuwe informatietechnologie afkomstig uit de VS.

In het laatste hoofdstuk zal worden stilgestaan bij de beperkingen die vastzitten aan het conceptualiseren van het gebruik van persoonsgegevens als een inbreuk op de persoonlijke levenssfeer. Er zal daar worden ingegaan op een alternatieve grondslag voor het gegevensbeschermingsrecht. De vraag is vervolgens hoe deze alternatieve grondslag kan worden toegepast op de casus van de toegang tot persoonsgegevens voor de opsporing. Het geheel zal daarna worden afgerond met een conclusie.

Hoofdstuk 1 De Wet bevoegdheden vorderen gegevens

Centraal in deze scriptie staat de nieuwe Wet bevoegdheden vorderen gegevens, in dit hoofdstuk kortweg aangeduid met de wet.¹ Deze wet introduceert een aantal voor de strafvordering nieuwe bevoegdheden. Bevoegdheden die opsporingsambtenaren in staat stellen gegevens te vorderen bij bedrijven en instellingen in Nederland. De bevoegdheden zijn afgestemd op persoonsgegevens; juist elektronische verzamelingen met persoonsgegevens moeten voor de opsporing toegankelijker worden. Het vorderen van andere gegevens staat echter ook open.

De wet staat niet op zichzelf. Hiervoor waren er al de Wet vorderen gegevens financiële sector² en de Wet vorderen gegevens telecommunicatie³, met vergelijkbare bevoegdheden. De specifieke bevoegdheden voor de financiële sector zijn met de wet vervallen. Ondertussen ligt ook een wetsvoorstel ter herziening van de wetgeving die de verwerking van persoonsgegevens voor de opsporing regelt ter behandeling bij de Tweede Kamer.⁴

In dit hoofdstuk zal ik de wet bespreken aan de hand van de wetgevingsgeschiedenis en de discussie in de rechtsgeleerde literatuur. Het gaat er in deze scriptie om hoe de bescherming van de informationele privacy normatieve invloed heeft gehad op de regeling van de toegang tot persoonsgegevens voor de opsporing. De toets van artikel 8 van het Europees Verdrag voor de rechten van de mens (EVRM) speelt in dat kader een grote rol en heeft ook voor de wetgever in grote mate het normatieve kader bepaald, waarbinnen de bevoegdheden zijn ingevoerd en in de toekomst zullen worden uitgeoefend.⁵ Sommige commentatoren hebben echter gesteld dat niet voldoende aangetoond is dat de wet de toets van art. 8 EVRM kan doorstaan. Speciale aandacht zal daarom uitgaan naar artikel 8 EVRM.

Voorgeschiedenis

Aan de basis voor de wet ligt het rapport Gegevensvergaring in strafvordering van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, kortweg de Commissie Mevis.⁶ De regering had deze commissie ingesteld naar aanleiding van gesignaleerde knelpunten bij de vergaring van persoonsgegevens in het kader van de strafvordering.⁷ Bij het vergaren van persoonsgegevens bij

¹ Wet van 16 juli 2005 tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens), *Stb.* 2005, 390.

² *Stb.* 2004, 109.

³ *Stb.* 2004, 105.

⁴ Wetsvoorstel Politiegegevens, *Kamerstukken II* 2005/06, 30 327. De Wet politiegegevens houdt een verruiming in van de mogelijke verwerkingen door de politie en de bewaartermijnen voor gegevens. Het moge duidelijk zijn dat een verruiming van de toegang tot gegevens in combinatie met de verruiming van de mogelijke verwerkingen justitie een krachtig middel is voor de opsporing.

⁵ Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden, *Trb.* 1951, 154.

⁶ Commissie Mevis 2001.

⁷ Instellingsregeling, 2 maart 2000, nr. 501455/00/6, *Stcrt.* 17 maart 2000, nr. 55.

een houder van deze gegevens was justitie in de meeste gevallen afhankelijk van een afweging van deze houder. Dit was slechts anders indien er een wettelijke verplichting tot verstrekking van de gegevens aanwezig was maar dit was een uitzondering.⁸ De houder had op grond van artikel 43 van de Wet bescherming persoonsgegevens en daarvoor artikel 11 lid 2 van de Wet persoonsregistraties, de mogelijkheid gegevens, die niet voor het verstrekken aan justitie in het kader van strafrechtelijk onderzoek verzameld waren, toch rechtmatig te verstrekken. Het betreft hier een uitzondering op het beginsel van de doelbinding. De houder was dan wel gehouden te bezien of er voor de verstrekking een dringende en gewichtige reden aanwezig was. De wet diende op dit punt naar de bedoeling van de wetgever restrictief te worden uitgelegd. De rechter was in de weinige gevallen dat hij zich hierover heeft uitgesproken minder restrictief in zijn uitleg.⁹

Justitie was in de oude situatie dus afhankelijk van een afweging door de houder. Dit is voor justitie natuurlijk verre van ideaal. Voor justitie is het in het belang van het onderzoek vaak niet mogelijk alle informatie te verstrekken, die voor een goede afweging nodig is. Dit maakt een goede afweging onmogelijk, omdat het belang van justitie bij de verkrijging van de gegevens voor de houder dan niet kenbaar is. In de praktijk bleken houders de gegevens overigens in de meeste gevallen wel te verstrekken en bleek het geldende kader van de Wbp weinig normatieve invloed te hebben.¹⁰ Daarbij speelt mee dat de belangen van de opsporing en de houders van gegevens bij verstrekking vaak parallel lopen.¹¹ Opsporingsambtenaren deden het daarbij vaak lijken alsof de houder verplicht was de gegevens te verstrekken. Een opsporingsambtenaar had wel onder de daarvoor geldende voorwaarden van artikel 96a van het Wetboek van Strafvordering de mogelijkheid de gegevensdragers in beslag te nemen, welke bevoegdheid ook toekomt aan de rechter-commissaris ex artikel 105 Sv. Deze inbeslagname was echter in veel gevallen disproportioneel. Verder bestond voor de rechter-commissaris al de mogelijkheid tot uitlevering van computergegevens te bevelen tijdens het gerechtelijk vooronderzoek op grond van artikel 125i Sv.

Waarschijnlijk de belangrijkste aanbeveling van de Commissie Mevis was dat de afweging of er tot verstrekking overgegaan diende te worden, verplaatst moest worden van de houder van de gegevens naar de met de opsporing belaste ambtenaren. De Commissie Mevis stelde voor een reeks nieuwe strafvorderlijke bevoegdheden tot het vorderen van gegevens op te nemen in het Wetboek van Strafvordering. Zij kwam met een uitgewerkt voorstel, dat nu op enige uitzonderingen na in het wetboek is opgenomen. Op de voorstellen van de Commissie Mevis is uitgebreid gereageerd.¹²

⁸ Dit gold bijvoorbeeld voor de bevoegdheden tot inbeslagname en het bevel tot het verstrekken van computergegevens van art. 125i Sv.

⁹ Hoge Raad, 8 november 1994, *NJB* 27-2-1995; Rechtbank Zwolle, 24 april 1996, Politierechter Roermond, 15 mei 2000, *NJ* 2000, 527; Gerechtshof 's-Hertogenbosch, 8 november 2000, LJV AA8226, Hoge Raad, 20 november 2001, LJV AD4451.

¹⁰ Mac Gillavry 2004, p. 202-204.

¹¹ *Idem*, p. 203.

¹² Asscher & Koops 2004, Dommering 2001, Mac Gillavry 2001, Mac Gillavry 2002, Van Grinsven 2004, Kuitenbrouwer 2003, Mevis 2002, Prins 2004, Stevens, Koops & Wiemans 2004. Zie ook de website van Asscher en Koops, <http://www.gegeven.nl>.

Gegevens of informatie?

De wet gaat uit van het begrip gegevens. Gegevens zijn volgens de memorie van toelichting “*informatie die is vastgelegd of opgeslagen op een gegevensdrager, hetzij op schrift, hetzij in elektronische vorm*”.¹³ Deze definitie wijkt af van de definitie van de Commissie Mevis. Deze hanteerde de definitie “*iedere weergave van feiten, begrippen of instructies, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken*”.¹⁴ Deze laatste definitie is zorgvuldiger. Het begrip informatie is namelijk gangbaar gedefinieerd als “*de betekenis die een mens aan gegevens (data) toekent volgens de conventies die op de gegevens worden toegepast*”.¹⁵ Informatie bestaat dus uit gegevens die zijn vastgelegd op een informatiedrager volgens bepaalde overeengekomen regels.¹⁶ Gegevens zijn kortom een kaler begrip dan informatie. Het is dus onjuist het begrip informatie in de definitie van gegevens te gebruiken.¹⁷ Er worden hiervoor in de memorie van toelichting geen argumenten gegeven. Het kale begrip voor gegevens is van belang, omdat hierdoor in de strafrechtelijke systematiek aangesloten kan worden bij de bevoegdheden tot het uitleveren van voorwerpen. Dit is in de literatuur bekritiseerd als het verbloemen van de informatiewaarde van de gevorderde gegevens.¹⁸ De wetgever lijkt aan deze discussie te zijn voorbijgegaan.

Het onderscheid tussen het verstrekken van informatie en het verstrekken van kale gegevens is van groot belang in verband met het volgende. De systematiek van het Wetboek van Strafvordering gaat namelijk uit van het beginsel dat burgers op vrijwillige basis mogen meewerken aan de strafvordering. Burgers zijn behoudens uitzonderingen niet verplicht mee te werken en voor de opsporing van strafbare feiten interessante informatie te verstrekken. Voor zover met de wet een plicht ontstaat tot het verstrekken van informatie aan justitie breekt de wet met deze systematiek.¹⁹

De nieuwe bevoegdheden

De systematiek van de bevoegdheden in de wet gaat uit van een driedeling in soorten gegevens. De gegevens worden ondergebracht in drie categorieën: identificerende gegevens, andere gegevens en gevoelige gegevens. Voor de definitie van gevoelige gegevens is aangesloten bij de definitie van bijzondere gegevens uit de Wbp. De hoofdregel is dat het gaat om gegevens bij een houder die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt. De vordering mag niet gericht worden

¹³ *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7.

¹⁴ Commissie Mevis 2001, p. 16.

¹⁵ De omschrijving is ontleend aan de ISO/IEC-norm 2381-1.

¹⁶ Dommering 2000, p. 459.

¹⁷ Stevens, Koops & Wiemans trekken hier de conclusie uit dat het de wetgever juist gaat om de informatie, Stevens, Koops & Wiemans 2004. Het is overigens slordig dat terwijl in de definitie in de memorie van toelichting gegevens al ‘opgeslagen en vastgelegde informatie’ zijn, in de artikelen van de wet ook nog eens wordt gesproken over ‘opgeslagen of vastgelegde gegevens’.

¹⁸ Stevens, Koops & Wiemans 2004, par. 2.4.

¹⁹ Zie voor deze interessante discussie of er sprake is van de introductie van een informatieplicht in het Wetboek van Strafvordering, het kritische artikel van Mac Gillavry over de voorstellen van de Commissie Mevis, Mac Gillavry 2002, en de scherpe reactie van de voorzitter van de Commissie, Mevis 2002.

tegen de verdachte en de verschoningsgerechtigden van artikel 96a Sv. De vordering is schriftelijk, maar kan bij dringende noodzaak mondeling worden gedaan.

De identificerende gegevens kunnen ex artikel 126nc Sv in het geval van een misdrijf door de opsporingsambtenaar in het belang van het onderzoek worden gevorderd bij een ieder die daar redelijkerwijs voor in aanmerking komt. Onder identificerende gegevens vallen NAW, geboortedatum en geslacht, en administratieve kenmerken. De vordering bevat een aanduiding van de persoon van wie gegevens gevorderd worden. Dit omvat de mogelijkheid op grond van een ander gegeven, identificerende gegevens te vorderen.²⁰ De vordering mag geen gevoelige gegevens betreffen.

Andere gegevens, met uitsluiting van gevoelige gegevens, kunnen ex art. 126nd Sv in het geval van een misdrijf waarvoor voorlopige hechtenis mogelijk is, in het belang van het onderzoek door de officier van justitie worden gevorderd van degene van wie redelijkerwijs vermoed kan worden dat deze toegang heeft tot deze gegevens. Dit kan ook indien de houder deze gegevens verwerkt voor persoonlijk gebruik. Indien het een minder zwaar misdrijf betreft, heeft de officier een machtiging van de rechter-commissaris nodig. Dezelfde categorie gegevens, maar dan toekomstige, kan onder dezelfde voorwaarden worden gevorderd ex artikel 126ne Sv. De vordering van gegevens bij de houder die de gegevens verwerkt voor persoonlijk gebruik is hier wel uitgesloten.

Gevoelige gegevens kunnen ex artikel 126nf Sv door de officier van justitie worden gevorderd in het geval van een misdrijf waarvoor voorlopige hechtenis mogelijk is en dat gezien de aard of de samenhang met de andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, indien het belang van het onderzoek dit dringend vordert, bij degene van wie redelijkerwijs vermoed kan worden dat deze toegang heeft tot deze gegevens. De officier heeft hiervoor een schriftelijke machtiging nodig van de rechter-commissaris.

Aan vorderingen op grond van de nieuwe bevoegdheden zijn steeds de volgende voorwaarden gesteld. De vordering bevat verplicht de titel van de vordering, een aanduiding van de persoon of een zo nauwkeurig mogelijke aanduiding van de groep van wie de gegevens worden gevorderd, evenals een de termijn waarbinnen en de wijze waarop de gegevens dienen te worden verstrekt. Er dient van elke vordering proces verbaal opgemaakt te worden door de officier van justitie of de opsporingsambtenaar in het geval van de identificerende gegevens.

Gezien de mogelijkheid dat de gegevens versleuteld zijn is er tevens een bevoegdheid tot het bevelen tot ontsleuteling van gegevens. Deze bevoegdheid, die toekomt aan de officier van justitie is

²⁰ *Kamerstukken II 2003/04*, 29 441, nr. 3, p. 20 (MvT). Dit lijkt mij gezien de systematiek van de wet onjuist. In dit geval zou namelijk de bevoegdheid gebruikt moeten worden tot het vorderen van andere of gevoelige gegevens. Er wordt immers van de personen van wie identificerende gegevens gevorderd worden ook het andere gegeven, op grond waarvan de groep aangeduid wordt, verkregen. In het geval dit gegeven een bijzonder gegeven is, zoals "is lid van de politieke organisatie X in plaats Y", dient volgens de memorie van toelichting ook de bevoegdheid tot het vorderen van bijzondere gegevens gehanteerd te worden, waarvoor machtiging van de rechter-commissaris vereist is. Indien dit gegeven een ander gegeven is, zoals "heeft in plaats Y een computer van merk X gekocht" dient mijns inziens ook deze redenering te worden gevolgd en de bevoegdheid tot het vorderen van andere gegevens aangewend te worden.

opgenomen in artikel 126nh Sv. Een bevoegdheid bevestiging van gegevens te bevelen wordt meegenomen in het wetsvoorstel Aanpassing van het Cybercrime Verdrag.²¹

De notificatieplicht voor justitie en de geheimhoudingsplicht voor de houder volgen uit artikel 126bb Sv. Dit artikel regelt de kennisgeving aan betrokkenen van de hantering van bijzondere opsporingsbevoegdheden. Kennisgeving is pas verplicht in het geval het belang van het onderzoek dit toelaat. In het geval van vordering van identificerende gegevens kan een kennisgeving uitblijven, gezien het volgens de wetgever beperkte karakter van deze bevoegdheid.²²

Voor een niet opschortend beklagrecht voor de belanghebbende, onder wie in elk geval de houder en degene op wie de gegevens betrekking hebben, is aangesloten bij artikel 552a Sv. De houder kan daarnaast op grond van artikel 592 Sv trachten de kosten, die gemaakt worden in verband met het voldoen aan de vorderingen, vergoed te krijgen.

Gevolgen van de wet

De wet grijpt in, in een rechtsverhouding tussen de houder van persoonsgegevens en de betrokkene. Deze rechtsverhouding houder-betrokkene kan vele vormen aannemen, zoals uitvoeringsinstantie-burger, bedrijf-consument, werkgever-werknemer, school-leerling, zorginstelling-zorgafnemer. Het recht normeert deze rechtsverhouding voor wat betreft het gebruik van persoonsgegevens middels de Wbp. De Wbp is er gekomen ter implementatie van de Europese privacyrichtlijn.²³ Deze richtlijn was gericht op het opheffen van barrières die verschillende regimes voor de bescherming van persoonsgegevens in de lidstaten opleverden voor de vrije handel. De Wbp is in 2001 in werking getreden en wordt dit jaar geëvalueerd. Voor de Wbp was er de Wet persoonsregistraties.

De rechtsverhouding houder-betrokkene wordt bij de vergaring van persoonsgegevens ten behoeve van de opsporing met de komst van de nieuwe bevoegdheden nog steeds genormeerd door de Wbp. De grondslag voor de verstrekking verschuift echter van aanhef en onder f van artikel 8 Wbp naar onder c; er is bij een rechtmatige vordering een wettelijke verplichting tot verstrekking over te gaan. Dit vereenvoudigt de zaak voor de houder aanzienlijk. De lastige afweging die op grond van artikel 43 Wbp van de houder werd verlangd, en waarmee de praktijk blijkens onderzoek ook niet veel raad wist, verdwijnt hiermee.

Een punt dat ik hier niet onbelicht wil laten, is de positie van onrechtmatige gegevensverzamelingen. De Wbp kent voor het verwerken van gegevens, met uitzondering van bijzondere gegevens, een open systeem van regulering, dat er op neerkomt dat gegevens mogen worden verwerkt, mits wordt voldaan aan de in de wet gestelde voorwaarden. Voor de verwerking van bijzondere gegevens geldt een gesloten systeem: deze mogen slechts worden verwerkt als dat op de

²¹ Wetsvoorstel computercriminaliteit II, *Kamerstukken II* 2004/05, 26 671.

²² *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 5 (MvT).

²³ De richtlijn 'betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens', 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995, *PbEG* 1999 L 281/31.

Wbp te baseren is. Indien niet aan de voorwaarden in de Wbp is voldaan, is de verwerking onrechtmatig. Dit geldt bijvoorbeeld in het geval de gegevens zo onzorgvuldig worden verzameld en opgeslagen dat er heel veel gegevens niet kloppen. Een andere mogelijkheid is dat de betrokkene in het geheel niet op de hoogte is van, of er geen grondslag is voor de verwerking. De hantering van de bevoegdheden ten aanzien van onrechtmatige gegevensverzamelingen is vanuit het belang van degene op wie de gegevens betrekking hebben problematisch te noemen.

Uit de jurisprudentie volgt dat de onrechtmatigheid voor justitie geen niet-ontvankelijkheid tot gevolg heeft, als niet *“opsporingsambtenaren of ambtenaren van het Openbaar Ministerie hiervan wetenschap of hiermee enige bemoeienis hebben gehad”*.²⁴ Bewijsuitsluiting is mogelijk indien het handelen van de houder van de gegevens *“zodanige schending van de beginselen van een behoorlijke procesorde of veronachtzaming van de rechten van de verdediging in de strafzaak tot gevolg heeft dat dit dient te leiden tot uitsluiting van bewijsmateriaal dat tengevolge van dat onrechtmatig handelen is verkregen”*.²⁵ De conclusie is gerechtvaardigd dat bewijsuitsluiting en zeker niet-ontvankelijkheid niet snel aan de orde is.²⁶ Bij de beoordeling zal de horizontale werking van het recht op de persoonlijke levenssfeer en het recht op respect voor het privé leven een rol kunnen spelen. Een grove inbreuk op dit recht zou mijns inziens tot bewijsuitsluiting moeten leiden. Interessant in dit verband is het antwoord van de minister op de door bibliotheken geuite bezorgdheid over het opvragen van bepaalde gegevens. Volgens de minister moeten zij zich eerst afvragen of zij deze gegevens überhaupt wel zouden moeten verzamelen.²⁷ Hoewel de minister hier gelijk in heeft maakt dit het gevaar voor de burger niet kleiner.

Er komt door de introductie van de bevoegdheden dus zeker meer druk te staan op de verhouding tussen de verantwoordelijke voor de verwerking en de betrokkene. De laatste heeft er een belang bij gekregen dat er slechts beperkt gegevens van hem worden verwerkt en dat dit zeer zorgvuldig geschied. Men moge aannemen dat de gemiddelde zware crimineel dit eerste al langer als motto hanteert. In veel gevallen zal deze toch zorgen dat er geen gegevens of juist onjuiste gegevens van hem verwerkt worden.

Indien de houder zou weigeren aan een rechtmatige vordering te voldoen, maakt hij zich schuldig aan wederspanning, een misdrijf ex artikel 180 van het Wetboek van Strafrecht. Houders en medewerkers bij houders zullen zich dus wel twee keer bedenken voor zij zich tegen een vordering verzetten. Van de houder mag wel verwacht worden dat deze controleert dat de vordering aan de wettelijke vereisten voldoet.

²⁴ Hoge Raad, 1 juni 1999, *NJB* 1999, afl. 25. Zie voor een bespreking van dit arrest en de problematiek van onrechtmatig handelen door particuliere opsporing Buruma 2000.

²⁵ Idem.

²⁶ MacGillavry 2004, p. 79-80.

²⁷ “De bibliotheken hebben gewaarschuwd voor het zoeken op profielen. Die bezwaren zijn echter niet aan mij gezonden, maar alleen de Kamer. Dit kan ermee samenhangen dat de bibliotheken in overtreding van de Wet bescherming persoonsgegevens zijn als zij dergelijke bestanden hebben. Als zij zich aan de wet houden, kan geen opsporingsinstantie deze gegevens daar opvragen. [...] *Handelingen I* 2004/05, 29 441, nr. 32, p. 1495.

De wet vanuit grondrechtelijk perspectief

De informatiele privacy is in Nederland, Europees verband en internationaal verband²⁸ grondrechtelijk beschermd. De Nederlandse grondwet kent het recht op bescherming van de persoonlijke levenssfeer in artikel 10 van de Grondwet. Dit artikel heeft voor de wetgever slechts een beperkte rol gespeeld, namelijk dat inbreuken op de persoonlijke levenssfeer een basis dienen te hebben in een wet in formele zin. In Europees verband is er de bescherming tegen inbreuken in het privé leven van artikel 8 EVRM. Artikel 8 EVRM luidt:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others.

Het Europese Hof voor de rechten van de mens interpreteert het begrip *private life* ruim. In de zaak *P.G. and J.H.* wordt deze ruime interpretatie met de verschillende elementen van het privé leven die beschermd worden, door het Hof uiteengezet.²⁹ Hier wordt, voor wat betreft de bescherming van de informatiele privacy, door het Hof het oordeel uit de zaak *Rotaru*³⁰ herhaald, waar wordt aangesloten bij het Data beschermingsverdrag van de Raad van Europa uit 1981:³¹

“1. The Court reiterates that the storing of information relating to an individual's private life in a secret register and the release of such information come within the scope of Article 8 § 1 [...].

Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings: furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of “private life” [...].

The Court has already emphasised the correspondence of this broad interpretation with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is “to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to

²⁸ Namelijk artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten, *Trb.* 1969, 99. Hier zal gezien de geringe betekenis van dit artikel naast artikel 8 EVRM geen aandacht aan worden besteed.

²⁹ EHRM 25 september 2001, *P.G and J.H. v. United Kingdom*, nr. 56 t/m 59.

³⁰ EHRM 4 mei 2000, *Rotaru v. Romania*.

³¹ Verdrag tot bescherming van personen in verband met de geautomatiseerde verwerking van persoonsgegevens, *Trb.* 1988, 7.

him” (Article 1), such personal data being defined in Article 2 as “any information relating to an identified or identifiable individual” [...].

Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.”³²

Bij het automatisch verwerken van persoonsgegevens is er dus al snel sprake van bescherming door artikel 8 EVRM. De precieze grens is overigens door de zeer grote en vage reikwijdte van het recht moeilijk te trekken.

Als artikel 8 EVRM van toepassing is moet bij de toetsing ten eerste worden gekeken of er sprake is van een inbreuk op het recht op het privé leven. Als er sprake is van een inbreuk moet deze inbreuk ex van artikel 8 lid 2 EVRM bij de wet voorzien zijn, een van de daar genoemde doelen dienen, en noodzakelijk zijn in een democratische samenleving. Over de materiële betekenis van deze criteria is in een reeks uitspraken door het hof meer duidelijkheid gegeven. Bij de eis dat de inbreuk een van de in lid 2 genoemde doelen moet dienen zal niet verder worden stilgestaan; het is immers duidelijk dat de opsporing hier onder valt.

De inbreuk van de bevoegdheden uit de wet op art. 8 lid 1 EVRM

Bij de uitoefening van de bevoegdheden tot het vorderen van persoonsgegevens is er niet per definitie sprake van een inbreuk op het recht op privé leven.³³ Wanneer er precies sprake is van een inbreuk is niet eenvoudig aan te geven.³⁴ Duidelijk is dat als gegevens met toestemming van de betrokkene door de overheid worden verkregen, deze verkrijging niet te kwalificeren is als inbreuk. In de zaak *Rotaru* legt het Hof dezelfde toets aan als in de zaak *Leander*:

“The Court points out that both the storing by a public authority of information relating to an individual's private life and the use of it and the refusal to allow an opportunity for it to be refuted amount to interference with the right to respect for private life secured in Article 8 § 1 of the Convention [...]”.³⁵

In de zaak *P.G and J.H.* noemt het Hof ook een criterium om te bepalen of er sprake is van een inbreuk op het recht op respect voor privé leven dat afkomstig is uit de Verenigde Staten. Het gaat om

³² EHRM 4 mei 2000, *Rotaru v. Romania*.

³³ Nieuwenhuis 2001, p. 139. Anders Mac Gillavry in Mac Gillavry 2004, p. 500: “De verzameling, opslag en het gebruik van persoonsgegevens maken inbreuk op dit recht.” Zie ook Trechsel 2005, p. 552-555.

³⁴ Relatief veel zaken over de vraag of er sprake is van een inbreuk zijn voorgelegd aan de Commissie voor de rechet van de mens, zie Nieuwenhuis 2001. Deze uitspraken bevatten dezelfde overwegingen als het Hof.

³⁵ EHRM 26 maart 1987, *Leander v. Sweden*.

de volgens het hof belangrijke maar niet doorslaggevende vraag of er sprake is van een “*reasonable expectation as to privacy*”.³⁶

Gezien de rechtspraak van het Europese Hof en de Commissie voor de rechten van de mens is er wel snel sprake van een inbreuk. De Commissie Mevis en de wetgever brengen hier naast de driedeling van de gegevens naar mogelijke inbreuk weinig nuance in. Beiden gaan er bij het ontwerpen van hun regeling vanuit dat er sprake kan zijn van een inbreuk en toetsen de regeling aan de overige criteria van artikel 8 lid 2 EVRM. Dit lijkt een gebrek. Juist het duiden van de inbreuk zou ook helderheid kunnen verschaffen over een eventuele rechtvaardiging hiervan. Nu blijft deze inbreuk een abstract gegeven. Het is overigens de vraag of dit de wetgever aangerekend kan worden. De door de wetgever gekozen systematiek wordt ook veelvuldig door het Europese Hof gehanteerd. De inbreuk, hoe licht ook, wordt zeer snel aangenomen en vervolgens getoetst aan de vereisten van het tweede lid van artikel 8 EVRM. Het nogal vaag begrensde recht op privacy, besloten in de bescherming van artikel 8 EVRM lijkt hier debet aan.

Van gewicht bij de kwalificatievraag of sprake is van een inbreuk zou mijns inziens ook moeten zijn dat het gaat om het gebruik van de gegevens in het belang van strafvorderlijk onderzoek. Dit soort onderzoek en het soort van maatregelen dat in dat verband wordt genomen heeft al snel de neiging een inbreuk te maken op de persoonlijke levenssfeer. Vordering van bijzondere gegevens zal vrijwel steeds een inbreuk opleveren. Deze gegevens betreffen naar hun aard nu eenmaal zaken die privé zijn of diep raken aan de persoonlijke autonomie. Ook bij de vordering van andere (persoons)gegevens is er snel sprake van een inbreuk. Hierbij zou nog wel een rol kunnen spelen wat voor gegevens het betreft en hoeveel gegevens er worden verkregen. De identificerende gegevens krijgen van de wetgever een aparte positie. Er wordt steeds vanuit gegaan dat deze gegevens slechts beperkt inbreuk kunnen maken. Voor de vordering van deze gegevens worden minder zware eisen voldoende geacht. Ook de notificatieplicht is er niet voor deze vordering. Ten gevolge hiervan ontbreekt praktisch ook de mogelijkheid zich tegen de verwerking door justitie te verzetten. Dit zou gezien de hierboven geciteerde overweging uit de zaak *Leander* de conclusie kunnen rechtvaardigen, dat ook in het geval van identificerende gegevens er sprake is van een inbreuk.

Bij de wet voorzien

Als er sprake is van een inbreuk, moet deze bij de wet voorzien zijn. In de zaak *Silver and others* en eerder in de zaak *Sunday Times* heeft het Hof uiteengezet hieruit volgt dat de inbreuk een basis moet hebben in de wet, en dat deze wet toegankelijk en voorzienbaar moet zijn.³⁷ Over de toegankelijkheid merkt het Hof op:

³⁶ EHRM 25 september 2001, *P.G and J.H. v. United Kingdom* nr. 57. Zie ook EHRM 15 juni 1992, *Lüdi*, NJ 1993, 711.

³⁷ EHRM 25 maart 1983, *Silver and others v. United Kingdom*.

“the law must be adequately accessible: the citizen must be able to have an indication that is adequate, in the circumstances, of the legal rules applicable to a given case.”³⁸,

en over de voorzienbaarheid:

“a norm cannot be regarded as a law unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.”

A law which confers a discretion must indicate the scope of that discretion. However the Court has already recognised the impossibility of attaining absolute certainty in the framing of laws and the risk that the search for certainty may entail excessive rigidity. [...]

In view of this considerations, the Court points out once more that “many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice”.³⁹

In de zaak *Malone* stelt het hof dat voorzien bij wet ook slaat op de kwaliteit van de wettelijke regeling, inhoudende dat de regeling zich moet verdragen met het beginsel van de rechtsstaat:

“The Court would reiterate its opinion that the phrase “in accordance with the law” does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention [] .⁴⁰

Deze kwaliteitseis omvat de bovengenoemde eisen van toegankelijkheid en voorzienbaarheid.⁴¹ Ook betekent dit dat de wet waarborgen moet bevatten tegen willekeur en misbruik.⁴²

Noodzakelijk in een democratische samenleving

De laatste eis is dat de inbreuk noodzakelijk moet zijn in een democratische samenleving. Waar bij de andere elementen zich meer lenen voor een toetsing in abstracto, kan deze proportionaliteits eis slechts worden uitgevoerd ten aanzien van een specifieke inbreuk.⁴³ In zijn uitspraak in de zaak *Silver and others* vat het Hof zijn eerder gedane uitspraken op dit punt samen.⁴⁴ Ten eerste geeft het hof aan waarbinnen de bandbreedte van de betekenis van het woord noodzakelijk moet blijven:

³⁸ Idem, nr. 87.

³⁹ Idem, nr. 88.

⁴⁰ EHRM 2 augustus 1984, *Malone v. United Kingdom*, nr. 67.

⁴¹ EHRM 16 februari 2000, *Amann v. Switzerland*, nr. 50.

⁴² EHRM 25 september 2001, *P.G and J.H. v. United Kingdom*, nr. 46 en 47.

⁴³ Trechsel 2005, p. 540.

⁴⁴ EHRM 25 maart 1983, *Silver and others v. United Kingdom*, nr. 97.

“(a) the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" [...].”⁴⁵

Dit betekent dus dat aan het woord noodzakelijk het nodige gewicht dient te worden toegekend. Het valt op dat de memorie van toelichting bij het wetsvoorstel Wet Politiegegevens op dit punt dit gehele spectrum hanteert.⁴⁶ Misschien dat daarbij al invulling gegeven is aan het volgende beginsel dat inhoudt dat de nationale overheden bij de vraag of een inbreuk noodzakelijk is, een zekere maar niet onbeperkte beoordelingsruimte heeft:

“(b) the Contracting States enjoy a certain but not unlimited margin of appreciation in the matter of the imposition of restrictions, but it is for the Court to give the final ruling on whether they are compatible with the Convention [...].”⁴⁷

Daarnaast geldt de eis dat de inbreuk moet plaatsvinden ten behoeve van een *pressing social need*, die proportioneel moet zijn aan het legitieme doel dat de inbreuk dient:

“(c) the phrase "necessary in a democratic society" means that, to be compatible with the Convention, the interference must, inter alia, correspond to a "pressing social need" and be "proportionate to the legitimate aim pursued" [...].”⁴⁸

Hiermee wordt door het Hof dus ook invulling gegeven aan het beginsel van proportionaliteit. Tenslotte moet het tweede lid, dat de voorwaarden geeft waarbinnen een inbreuk op het recht op het privé leven gelegitimeerd is, restrictief worden uitgelegd:

“(d) those paragraphs of Articles of the Convention which provide for an exception to a right guaranteed are to be narrowly interpreted[...].”⁴⁹

Toetsing van de wet aan de criteria van artikel 8 lid 2 EVRM

Uit de jurisprudentie van het Hof valt af te leiden dat naarmate de inbreuk een ernstiger karakter heeft, de eisen waarin deze inbreuk moet voldoen strenger zijn. Dat geldt niet slechts in het kader van de

⁴⁵ Idem.

⁴⁶ “De beoordeling van de noodzakelijkheid van de verwerking van politiegegevens brengt een beoordelingsmarge met zich mee, die ergens beweegt tussen «onmisbaar» als bovengrens en «normaal», «nuttig», «redelijk» en «wenselijk» als ondergrens.”, *Kamerstukken II 2005/06*, 30 327, nr. 3, p. 8.

⁴⁷ EHRM 25 maart 1983, *Silver and others v. United Kingdom*, nr. 97.

⁴⁸ Idem.

⁴⁹ Idem.

proportionaliteit, maar ook voor de eisen die gesteld worden in het kader van de kwaliteit van de wettelijke regeling. Zo zal een minder inbreuk makende regeling minder precies omschreven kunnen worden dan een regeling die een ernstige inbreuk maakt op het recht voor respect op het privé leven.

Om aan bovenstaande eisen tegemoet te komen zijn de nieuwe bevoegdheden in een trapsgewijs oplopend kader gegoten, is steeds aangegeven in welke gevallen, op welke gronden, door wie en wat kan worden gevorderd. De basis hierbij is de driedeling in identificerende gegevens, andere gegevens, en gevoelige gegevens. Naar het oordeel van de wetgever is er bij de categorie identificerende gegevens sprake van een beperkte categorie gegevens, die op zichzelf slechts in beperkte mate kan raken aan de persoonlijke levenssfeer⁵⁰. De andere gegevens zijn volgens de wetgever meeromvattend en kunnen meer blootleggen van iemands persoonlijk leven; de persoonlijke levenssfeer van de persoon op wie de gegevens betrekking hebben, kan verdergaand worden beperkt.⁵¹ De gevoelige gegevens zijn gegevens die gezien hun aard een indringende inbreuk kunnen maken op de persoonlijke levenssfeer.⁵²

Trapsgewijs van identificerende gegevens, via andere en toekomstige gegevens naar gevoelige gegevens, nemen de voorwaarden toe. Zo loopt de bevoegde ambtenaar trapsgewijs mee van opsporingsambtenaar, via de officier van justitie, tot de officier van justitie op machtiging van de rechter-commissaris. Daarnaast zijn de gevallen waarin de bevoegdheden kunnen worden toegepast steeds beperkter, namelijk van het ruime ‘in geval van een misdrijf’, via ‘in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten’, tot ‘in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten en dat gezien de aard of de samenhang met andere misdrijven een ernstige inbreuk op de rechtsorde oplevert’. In de eerste twee gevallen dient de vordering in het belang van het onderzoek plaats te vinden. Bij gevoelige gegevens dient het belang van het onderzoek de toepassing van de bevoegdheid dringend te vorderen. Een andere reden die de wetgever noemt voor het verzwaren van de voorwaarden is als een bevoegdheid een grotere inspanning vergt van de houder van de gegevens. Door Buruma is over deze precieze regeling mijns inziens terecht gesteld dat “[het] allemaal heel erg precies is opgeschreven, maar [dat] bijna alle remmen zijn verdwenen om gegevens op te vragen.”⁵³ De toepassing van alle criteria dient door de opsporingspraktijk invulling te krijgen.⁵⁴

De begrenzing van de groep op wie de gegevens betrekking hebben is minder precies. Deze begrenzing wordt gegeven door het belang van het onderzoek.⁵⁵ Alleen indien gegevens nodig zijn voor een goede afronding van het opsporingsonderzoek kunnen gegevens worden vergaard. Een van de aangelegde criteria is dat hier bij vordering van gegevens van niet-verdachte personen minder snel

⁵⁰ *Kamerstukken II 2003/04*, 29 441, nr. 3, p.7 (MvT).

⁵¹ *Idem*, p. 8.

⁵² *Idem*, p.10.

⁵³ Buruma 2004, p. 670.

⁵⁴ Zie ook de voorbeelden van de toepassing van de bevoegdheden in het “Handboek voor de opsporingspraktijk”, paragraaf 2.12, *Staatscourant* 2005, 252, pag. 56. Er wordt in deze voorbeelden slechts weinig invulling gegeven aan de materiële criteria. In het bijzonder worden geen voorbeelden gegeven dat gegevens niet gevorderd kunnen worden.

⁵⁵ *Kamerstukken II 2003/04*, 29 441, nr. 3, p. 8 (MvT).

sprake zal zijn en dat uit het beginsel van proportionaliteit volgt dat aan een dergelijke vordering hogere eisen te stellen zijn aan de motivering, aangezien een beperking van de persoonlijke levenssfeer van de verdachte eerder is gerechtvaardigd dan bij een niet-verdachte burger.⁵⁶

De bevoegdheden kunnen echter ook worden ingezet indien de groep personen onbepaald is. Dit houdt in dat er ook nog geen sprake hoeft te zijn van een bepaalde verdachte, daar anders de vordering in beginsel gericht zou dienen te worden op gegevens over deze verdachte. Justitie dient bij een dergelijke vordering van gegevens van een onbepaalde groep op een andere wijze een begrenzing aan te geven. Het is echter zeer goed voorstelbaar dat het aangeven van deze grens voor justitie moeilijk en tijdrovend is. Zo zou een dergelijke vordering van gegevens van een onbepaalde groep gemakkelijk kunnen leiden tot het verkrijgen van gegevens van een zeer grote groep. In het geval de groep onnodig groot is, is er mijns inziens niet voldaan aan de toets van artikel 8 EVRM. Hier komt nog bij dat het goed kan zijn dat de gegevens door de hoeveelheid praktisch onbruikbaar worden, ook al is duidelijk dat er gegevens van de dader bij de verzameling moeten zitten.

Er worden op twee manieren gegevens van niet-verdachte burgers gevorderd. Enerzijds kan de vordering er juist op gericht zijn gegevens van niet-verdachte burgers te verkrijgen, omdat deze persoon in een bepaalde verhouding tot de verdachte of het misdrijf staat. Anderzijds worden er gegevens over niet-verdachte personen verkregen in het kader van vorderingen van gegevens van een onbepaalde groep personen. Het vorderen van gegevens van niet-verdachte burgers die in geen relatie tot het misdrijf staan in is gezien artikel 8 EVRM slechts te rechtvaardigen als niet te voorkomen is dat deze gegevens worden verkregen. Anders is er immers strijd met het beginsel van proportionaliteit.

De noodzakelijkheid van de bevoegdheden

Ten aanzien van de noodzakelijkheid van de bevoegdheden in het kader van de toets van artikel 8 EVRM geeft de wetgever drie redenen. Bij deze redenen spreekt de wetgever overigens over nodig in plaats van noodzakelijk, terwijl hier, zoals hierboven is gebleken, in het kader van de afweging van artikel 8 lid 2 EVRM een verschil in zit.⁵⁷

De eerste reden is, dat er gegevens over personen en hun handelingen bij derden beschikbaar zijn, die van grote betekenis kunnen zijn voor de opsporing van strafbare feiten.⁵⁸ Dat dit zo is, moge duidelijk zijn.⁵⁹ Het lijkt me een typische nut-is-noodzaak-redenering. Dit nut is zeker een voorwaarde überhaupt de introductie van de bevoegdheden te kunnen rechtvaardigen, maar maakt de introductie van de bevoegdheden nog niet nodig, laat staan noodzakelijk. Dit argument, dat kortweg inhoudt dat de mogelijkheden die de informatiemaatschappij biedt ook in het kader van de opsporing van strafbare feiten moet kunnen worden benut, wordt door Dommering terecht scherp aangevallen als

⁵⁶ Idem, p. 6.

⁵⁷ *Kamerstukken II 2003/04*, 29 441, nr. 3, p. 3 (MvT).

⁵⁸ Idem.

⁵⁹ Fijnaut, niet de minste op het gebied van onderzoek over opsporing en opsporingstechnieken, stelt overigens dat het belang en de rol van informatietechnologie bij de opsporing zwaar wordt overschat, zeker wat betreft de effectiviteit van dergelijke opsporingsmiddelen. Zie Franken 2003, p. 74 e.v.

“*corrumperend voor ons denken over de rechtsstaat*”.⁶⁰ Stevens, Koops en Wiemans benadrukken in dit verband dat het gaat om “*een substantiële verruiming van justitie om informatie te verzamelen en daarmee een aanzienlijke verruiming van de mogelijke inbreuk op de persoonlijke levenssfeer van burgers*”.⁶¹ De wetgever had er goed aan gedaan, de vraag naar de noodzakelijkheid van deze verruiming los van het nut te beschouwen.

In het argument schuilt ook een ander gebrek. De toegenomen informatiemacht van bedrijven en instellingen kan zeker nuttig zijn voor de opsporing. Echter het aanwenden van deze informatiemacht doorbreekt de doelbinding van deze informatiemacht en dit is slechts gerechtvaardigd als dit noodzakelijk is in een democratische samenleving.⁶² Gegevensverzamelingen zijn er immers steeds met een welbepaald doel. Het is juist deze doorbreking, die een zelfstandige rechtvaardiging behoeft, zoals eerst op basis van de criteria van artikel 43 WBP gebeurde. Nu wordt het doorbreken van dit criterium blijkbaar mogelijk geacht omdat dat nuttig is. Hier geeft het algemene belang bij de opsporing van strafbare feiten blijkbaar de doorslag en wordt dit te dik aangezet in de afweging met andere belangen. Het belang bij de opsporing van strafbare feiten zou het beste worden gediend als de dader met een druk op de knop uit de computer rolt. Waar aan voorbij gegaan wordt is de onwenselijke structurering en versterking van de informatiemacht van de overheid en private partijen die dit mogelijk zou kunnen maken.

De tweede reden van de wetgever is sterker. Gesteld wordt dat gegevens steeds vaker nog slechts in elektronische vorm beschikbaar zijn. De inbeslagname van de gegevensdrager is disproportioneel omdat dit de houder zwaar treft en omdat er veel meer gegevens dan noodzakelijk worden verkregen.⁶³ Dit maakt het inderdaad noodzakelijk op deze nieuwe situatie afgestemde bevoegdheden voor justitie te introduceren. Het gaat hier om een aanpassing van de opsporingsbevoegdheden aan de verandering in de maatschappij van het papieren naar het elektronische tijdperk.

De derde reden is dat het recht op de bescherming van persoonsgegevens sterk is ontwikkeld en dat zonder de geïntroduceerde bevoegdheden deze persoonsgegevens niet zondermeer beschikbaar zijn voor de opsporing, terwijl ze dat wel zouden moeten zijn.⁶⁴ Dit is wederom geen echte reden. Een echte reden zou immers aangeven waarom de gegevens beschikbaar moeten zijn voor strafrechtelijk

⁶⁰ Dommering 2001: “Het meest fundamentele bezwaar dat ik er tegen heb is dat het ons denken over de rechtstaat corrumpeert. De redenering lijkt te zijn dat ICT het steeds beter mogelijk maakt om de gedragingen van individuen te registreren en te volgen en dat dus de overheid het recht heeft om van deze technische vooruitgang te profiteren door individuele vrijheden verdergaand te beperken dan in de papieren wereld mogelijk was. Verplichtingen waarover wij niet zouden piekeren om die in het papieren tijdperk in te voeren worden nu als noodzakelijke technische aanpassingen aan de ICT wereld zonder principiële discussie door een zijdeur naar binnen gefietst.”

⁶¹ Stevens, Koops & Wiemans 2004, p 1684.

⁶² Zo ook artikel 9 van het Databeschermingsverdrag van de Raad van Europa, supra noot 27.

⁶³ Tweede Kamer, vergaderjaar 2003–2004, 29 441, nr. 3, p. 3. Bij dit argument wordt impliciet aangenomen dat het vorderen van medewerking door houders van gegevens aan de strafvordering minder inbreuk maakt op de rechten van de houder en/of degenen die de gegevens betreffen dan de inbeslagname van de gegevensdragers. E. Mac Gillavry oordeelt anders, zie Mac Gillavry 2001 en Mac Gillavry 2002.

⁶⁴ Tweede Kamer, vergaderjaar 2003–2004, 29 441, nr. 3, p. 3.

onderzoek. Als er geen juridische problemen waren de gegevens zonder de bevoegdheden te verkrijgen zou de introductie van de bevoegdheden immers niet nodig zijn. Met deze redenering diskwalificeert de wetgever de beperkingen die golden op grond van de informationele privacy. Ik lees in deze redeneving dat de wetgever de introductie van de nieuwe bevoegdheden ziet als een legitimering van een gerechtvaardigde, maar juridisch problematische praktijk.⁶⁵ Dit laatste is in lijn met de koers die de wetgever naar aanleiding van de IRT-affaire in het strafprocesrecht heeft gevolgd om juridisch problematische praktijken niet te beperken, maar wettelijk te normeren.⁶⁶

Het een en ander maakt op mij en bovengenoemde commentatoren een niet erg overtuigende indruk.⁶⁷ De noodzakelijkheid is door de wetgever meegewogen en in de hierboven uiteengezette, naar de mate van inbreuk die de gegevens kunnen maken op de persoonlijke levenssfeer zwaardere voorwaarden vertaald. Gezien de bovenstaande zwakke en zeer algemene argumentatie was het beter geweest als een zwaardere noodzakelijkheidstoets in de bevoegdheden zelf was opgenomen, met een uitbreiding van de mogelijkheid tot rechtelijke toetsing vooraf. Dit had een minder scherpe verandering opgeleverd ten aanzien van de nu geldende toets van artikel 43 Wbp dat er sprake moet zijn van een dringende en gewichtige reden.

Conclusie

De wet bevoegdheden vorderen gegevens is een fundamentele verruiming van de informatiemacht van de justitie bij de opsporing van strafbare feiten. De wetgever heeft om tegemoet te komen aan de bescherming van de informationele privacy door artikel 8 EVRM, een erg precieze regeling opgesteld, maar met de argumentatie over de noodzakelijkheid van de bevoegdheden is de wetgever niet veel verder gekomen dan het wijzen op het nut van de toegang tot deze informatiemacht voor de opsporing. Dit wijst op een sterke nadruk op het belang van de opsporing van strafbare feiten. De inbreuk die de bevoegdheden maken op de informationele privacy zijn door de wetgever niet helder gemaakt en slechts abstract meegewogen. Hier lijkt ook het nogal vage normatieve kader voor de bescherming van informationele privacy van artikel 8 EVRM debet aan. De vraag blijft gezien deze conclusie of met de nieuwe wet de juiste afweging is gemaakt, en in het bijzonder of bij de toepassing van de bevoegdheden voldaan is aan de vereisten van artikel 8 EVRM. Om de vernieuwde toegang voor justitie tot persoonsgegevens in Nederland vanuit een ander perspectief te kunnen bezien zal ik in het volgende hoofdstuk de geldende regeling voor de toegang tot persoonsgegevens in het kader van de opsporing in de Verenigde Staten bespreken.

⁶⁵ De introductie van de wetgeving als legitimering van doorgeschoten (Europese) privacy bescherming wordt toegejuicht door Y. Buruma, Buruma 2004, p. 670.

⁶⁶ Koops en Vedder 2001, p. 27.

⁶⁷ Zo ook op Stevens, Koops en Wiemans, die concluderen: “Nergens in de discussie over de voorstellen van de Commissie Mevis of in de kamerstukken is ook maar enigszins aannemelijk gemaakt dat de nieuwe bevoegdheden in hun totaliteit ook werkelijk ‘noodzakelijk zijn in een democratische samenleving’ in de zin van artikel 8 EVRM.”, Stevens, Koops & Wiemans 2004, p. 1686.

Hoofdstuk 2 De toegang tot persoonsgegevens in het kader van de strafvordering in de Verenigde Staten

In dit hoofdstuk zal ik een beschrijving geven hoe in de Verenigde Staten de toegang van justitie tot persoonsgegevens is geregeld. Gezien de complexiteit van het Amerikaanse recht en het feit dat dit onderwerp niet in één regeling te vinden is zal ik mij op verschillende manieren moeten beperken. Dit hoofdstuk zal ten eerste het karakter hebben van een vogelvlucht; een korte bespreking van de relevante rechtsgebieden. Verder zal alleen het federale niveau in de beschouwing worden betrokken. De situatie op het niveau van de staten blijft vrijwel onbesproken. De constitutionele bescherming zal de meeste aandacht krijgen, omdat veel van de te bespreken leerstukken van het strafprocesrecht en het recht op privacy door het *Supreme Court* zijn ontwikkeld in zijn rechtspraak over de constitutie. Na een bespreking van het geldende recht volgt een kort, meer op de praktijk van gegevensvergaring, gericht overzicht van justitiële gegevensvergaring, gevolgd door een conclusie. Daarin zullen ook de verschillen met de Nederlandse regeling aan bod komen.

Dit rechtsvergelijkende deel is bedoeld om een ander perspectief te krijgen op de nieuwe bevoegdheden in Nederland. Rechtsvergelijking in het algemeen kan verschillende doelen dienen.⁶⁸ Hier is het doel voornamelijk om de vanzelfsprekendheid van het Nederlandse recht betreffende de bescherming van persoonsgegevens, de daarbij horende systematiek, en de door het EVRM geboden bescherming van de informationele privacy, te doorbreken. Het wegvallen van deze vanzelfsprekendheid schept ruimte voor nieuwe ideeën over het Nederlandse recht.

Er zijn een aantal goede redenen juist voor Amerikaans recht te kiezen. Ten eerste zijn de Verenigde Staten de bakermat van de bescherming van de privacy. Daarnaast lopen de Verenigde Staten voorop in informatietechnologische ontwikkelingen en is ook de invloed op Europa groot waar het de bestrijding van criminaliteit en terrorisme betreft. Het publieke debat over dit onderwerp is verder ook sterk ontwikkeld. Dit blijkt bijvoorbeeld uit de hoeveelheid populair wetenschappelijke literatuur over dit onderwerp.⁶⁹ De bescherming van persoonsgegevens is tenslotte van een geheel ander karakter.

Het Amerikaanse strafprocesrecht

De studie van het strafprocesrecht in de Verenigde Staten bestaat voornamelijk uit de studie van het constitutionele recht. Vanaf de jaren zestig heeft zich een constitutionalisering van het strafprocesrecht voltrokken. Talrijke uitspraken van het Supreme Court normeren tegenwoordig elk belangrijk onderdeel van het strafproces.⁷⁰ Het Hof heeft daarmee in grote mate de grenzen bepaald waarbinnen het politieoptreden in het kader van de strafvordering dient te blijven. Ik zal dan ook veel aandacht

⁶⁸ Voor een beknopte bespreking in het kader van rechtsvergelijking in het strafrecht en het strafprocesrecht, zie Nijboer 2005, p. 5-15.

⁶⁹ Zie bijvoorbeeld Solove 2004, Dash 2004 en Garfinkel 2000.

⁷⁰ Israel & LaFave 1993, p.2.

besteden aan de normen die aan de hand van de constitutie van de Verenigde Staten, en dan in het bijzonder de *Bill of Rights*, door het Hof zijn ontwikkeld, en voor dit onderwerp relevant zijn.

De sterke invloed van het constitutionele recht op het strafprocesrecht is ingezet door het Supreme Court, onder voorzitterschap van Earl Warren (1953-1969). De progressieve meerderheid van het Hof in deze periode heeft toen gezorgd voor een *criminal justice revolution*. Deze komt er op neer dat een groot deel van de grondrechten ook op de Staten van toepassing werd en dat de individuele constitutionele waarborgen steeds extensief werden geïnterpreteerd. Na het “*Warren Court*” volgden het “*Burger Court*” en het “*Rehnquist Court*”. Tijdens deze laatste twee perioden is door het Hof een veel sterkere nadruk gelegd op het belang van misdaadbestrijding.

In het Amerikaanse strafproces bestaan geen formele stadia waarin het opsporingsonderzoek door de politie is ingedeeld.⁷¹ Het politieoptreden is functioneel in de Verenigde Staten betrekkelijk autonoom en niet ondergeschikt aan het Openbaar Ministerie zoals in Nederland. Een codificatie van het optreden van politieoptreden is er traditioneel gezien niet.⁷²

Naast de constitutie en de uitspraken van het Supreme Court als bron van strafprocesrecht zijn de *Federal Rules of Criminal Procedure* van belang.⁷³ Deze bevatten een codificatie van regels voor het federale strafproces. Naar deze regels wordt ook steeds verwezen in titel 18 van de *United States Code*, waarin de statutaire regelingen van het strafproces zijn opgenomen. Ten slotte zijn er richtlijnen van de *Attorney General* voor de opsporing door het *Federal Bureau of Investigation*.⁷⁴

Het verkrijgen van gegevens voor de opsporing

Het onderdeel van het federale strafprocesrecht dat voor het onderwerp van deze scriptie van belang is, is het opsporingsonderzoek door politie, waarbij politie informatie verzamelt ten behoeve van het oplossen van (federale) misdrijven. Het centrale leerstuk uit het Amerikaanse recht is dan het leerstuk van *searches* en *seizures* en de bescherming die hiertegen geboden wordt door het *Fourth Amendment* uit de *Bill of Rights*. Dit leerstuk omvat ondermeer de doorzoeking van plaatsen, de ophouding, het fouilleren en de arrestatie van personen, en de inbeslagname van voorwerpen en documenten.⁷⁵

Het federale vervolgingsapparaat heeft een aantal verschillende instrumenten om documenten, gegevens en/of informatie te verkrijgen. In dat verband is van belang welke bescherming er geboden wordt. Als er bescherming is van het Vierde Amendement, dan dient in beginsel een warrant verkregen te worden.⁷⁶ Het geldende recht voor de verkrijging van een warrant is gecodificeerd in

⁷¹ Dressler 2002, p.5. Recentelijk zijn door de *Attorney General* wel dit soort stadia geïntroduceerd in zijn richtlijnen voor de federale strafvordering, infra noot 74.

⁷² Fijnaut 1994, p. 5.

⁷³ U.S.C.A 18, appendix.

⁷⁴ *Attorney General's Guidelines on General Crimes, Racketeering and Terrorism Investigations*, Attorney General John Ashcroft, May 30, 2002, www.usdoj.gov/olp/generalcrimes2.pdf

⁷⁵ Zie voor een meerdelige verhandeling over dit onderwerp het actueel gehouden LaFave 1996.

⁷⁶ Infra p. 27 e.v.

regel 41 van de Federal Rules of Criminal Procedure. Als deze bescherming afwezig is, is er het middel van de *subpoena*. In dit kader is relevant de *subpoena duces tecum*. Dit is een bevel tot het uitleveren van bepaalde zaken. De subpoena duces tecum is, zoals later zal blijken, naast de vrijwillige verstrekking het geijkte middel voor justitie om gegevens, waaronder persoonsgegevens, te verkrijgen bij houders.

De subpoena duces tecum valt binnen de bevoegdheid van de *grand jury* of de openbare aanklager. Er is ook een administratieve variant voor specifieke onderdelen van het overheidsapparaat. Er vindt een beoordeling van de rechtmatigheid door de rechter plaats als degene tot wie de subpoena is gericht, zich verzet tegen de uitoefening. Dit verzet is dus mogelijk voordat er documenten worden uitgeleverd, maar is niet kansrijk; de subpoena is zeer makkelijk af te dwingen.⁷⁷ Het verzet is mogelijk op drie gronden. Ten eerste op de grond dat de uitoefening van de subpoena strijd oplevert met het recht niet te hoeven meewerken aan de eigen veroordeling. Ten tweede kan verzet aangetekend worden op de grond dat de *subpoena* te belastend is om aan te voldoen. Ten derde is verzet mogelijk op de grond dat het gevorderde onvoldoende relevantie heeft voor justitie. De drie gronden dienen beperkt te worden uitgelegd. Zo kan verzet op de grond dat de gevorderde documenten irrelevant zijn slechts succes hebben, als er geen redelijke mogelijkheid is dat de categorie van het gezochte materiaal voor het onderzoek relevante informatie op zou kunnen leveren.⁷⁸ Indien er gegevens over bepaalde voor een opsporingonderzoek relevante personen verkregen worden bij een houder, zoals een bank, valt de eerste grond overigens af, tenzij het de advocaat-cliëntrelatie betreft.⁷⁹

De bescherming van persoonsgegevens in de Verenigde Staten

De bescherming van persoonsgegevens is in de Verenigde Staten van een ander karakter dan in Europa. De grondwet biedt op een aantal onderdelen belangrijke bescherming van de privacy in brede zin - in het bijzonder geldt dat voor het Vierde Amendement- maar de informationele privacy wordt slechts zeer beperkt grondwettelijk beschermd. De constitutionele bescherming van het recht op privacy behandel ik later.

Er is voor wat betreft de bescherming van persoonsgegevens een groot onderscheid tussen het soort regulering dat geldt voor de overheid en de private sector. Dit onderscheid hangt samen met het karakter van de Amerikaanse samenleving: een traditioneel wantrouwen jegens de (federale) staat, en een grote weerstand tegen regulering van de private sector. Het verwerken van persoonsgegevens in de publieke sector wordt statutair gereguleerd door de *Privacy Act* uit 1974. Deze wet is er gekomen naar

⁷⁷ Slobogin 2005.

⁷⁸ *Unites States v. R. Enterpr., Inc.*, 498 U.S. 292 (1991), 301.

⁷⁹ Ook de advocaat kan slechts eenzelfde beroep doen op de grond van het verbod tegen gedwongen meewerking aan de eigen veroordeling van het Fifth Amendment, als de persoon zou kunnen doen. De persoon zelf heeft slechts beperkt de mogelijkheid zich te verzetten tegen de productie van documenten. Het Fifth Amendment biedt geen bescherming voor het feit dat het vertrouwelijke en persoonlijke documenten betreft, zie *Fischer v. United States*, 425 U.S. 391 (1976). De bescherming van het Fifth Amendment heeft het karakter van bescherming tegen dwang tot medewerking aan het (eigen) proces. Zie Slobogin 2005, p.820-821. Voor een bespreking van het Fifth Amendment en de bescherming van informationele privacy, zie infra p. 31 e.v.

aanleiding van de angst voor het ontstaan van een landelijke database met de persoonsgegevens van elke Amerikaan. De Privacy Act kent nogal wat uitzonderingen, bijvoorbeeld voor de verwerking van persoonsgegevens door de opsporing. Om die reden zal deze wet in het vervolg buiten beschouwing blijven.

Er is geen omnibuswet voor de bescherming van persoonsgegevens, zoals de Wbp in Nederland. De bescherming van persoonsgegevens door de private sector is grotendeels overgelaten aan zelfregulering. Voor bepaalde sectoren bestaat er statutaire bescherming. Dit geldt bijvoorbeeld voor elektronische communicatie,⁸⁰ gegevens bij banken,⁸¹ gegevens bij bedrijven die informatie verzamelen en verstrekken voor de beoordeling van kredietwaardigheid,⁸² bepaalde soorten mediagebruik, zoals het gebruik van kabeltelevisie⁸³ en de huur van videobanden⁸⁴, en medische gegevens in de zorgketen.⁸⁵ Deze wetten grijpen meestal niet aan bij het soort gegevens, maar reguleren het gebruik van bepaalde gegevens door bepaalde verwerkers.⁸⁶ Zo vallen bijvoorbeeld gegevens over kredietwaardigheid, indien deze verwerkt worden door verhuurders, niet onder de bovengenoemde bescherming. De statutaire regelingen bevatten in de meeste gevallen ook bepalingen over de mogelijke verstrekking aan, of vordering door justitie van persoonsgegevens in het kader van strafvordering. Deze bepalingen bevatten bijvoorbeeld eisen voor de gevallen waarin gevorderd kan worden, en de mate van verdenking en relevantie van de gegevens die vereist is.

Dit alles geldt voor het federale niveau. De verschillende staten hebben daarnaast elk hun eigen statutaire en soms ook constitutionele regelingen voor de informationele privacy. Tussen de staten bestaan grote verschillen.

Constitutionele bescherming van de privacy

De grondrechten in de Verenigde Staten zijn opgenomen als amendementen op de constitutie van 1787, in de vorm van de Bill of Rights. Een aantal van de *Amendments* uit de Bill of Rights kent een impliciet aspect van privacybescherming. De grondrechten hebben in beginsel geen horizontale werking en leveren geen positieve verplichtingen op voor de overheid.⁸⁷ Hoewel uit het volgende zal blijken dat de Bill of Rights praktisch van geringe betekenis is voor de vergaring van persoonsgegevens voor de opsporing, kan behandeling van de geschiedenis van met name het Vierde Amendement niet achterwege blijven. De discussie over de bescherming van informationele privacy in het kader van de opsporing is voor het grootste deel gevoerd aan de hand van uitspraken van het

⁸⁰ *Omnibus Crime and Control and Safe Streets Act* (1968), amended with the *Electronic Communications Privacy Act* (1986), 18 U.S.C. §§ 2510-22, §§ 2701-11, §§ 3121-27.

⁸¹ *Right to Financial Privacy Act* (1978), 29 U.S.C.A. §§3401 e.v., tot stand gekomen naar aanleiding van de uitspraak *Miller v. United States*, infra p. 27 e.v.

⁸² *Fair Credit Reporting Act* (1970), 15 U.S.C.A. § 1681.

⁸³ *Cable Communications Policy Act* (1984), 47 U.S.C. § 551.

⁸⁴ *Video Privacy Protection Act* (1998), 18 U.S.C. § 2710, tot stand gekomen nadat journalisten overzichten van de gehuurde banden van R. Bork, kandidaat voor het Supreme Court hadden verkregen.

⁸⁵ Deze zijn gereguleerd door de *Health Insurance and Accountability Act* (1996), 45 C.F.R. § 160-64.

⁸⁶ Hoofnagle 2004, p.9.

⁸⁷ Schwartz & Reidenberg 1996, p. 31.

Supreme Court. Het betreft in grote mate een klassieke discussie over hoe het recht technologische ontwikkelingen dient te volgen, en in het bijzonder of de constitutionele bescherming met deze ontwikkelingen dient mee te groeien. De uitspraken over de gegevensvergaring door justitie en het grotendeels ontbreken van constitutionele bescherming is sinds deze uitspraken bekritiseerd. De laatste jaren is deze discussie verhevigd naar aanleiding van de recente praktijk van de federale overheid bij de justitiële gegevensvergaring en het gesignaleerde tekort aan normering van de groeiende stroom van persoonsgegevens tussen de private en publieke sector. Daarbij komt dat de hoeveelheid persoonsgegevens die beschikbaar is toeneemt met de ontwikkelingen van de informatiemaatschappij. Critici lijken in de meeste gevallen te denken aan herziening van de rechtspraak door het Hof in zake de bescherming van het Vierde Amendement.⁸⁸ Ik zal hieronder de verschillende amendementen die privacybescherming bieden kort behandelen. Het Vierde Amendement zal daarbij de meeste aandacht krijgen.

Het First Amendment

Het Eerste Amendement, dat de vrijheid van meningsuiting, godsdienst en vereniging beschermt, bevat ook een privacybeschermend element. Dit komt tot uiting in de uitspraak *N.A.A.C.P. v. United States*.⁸⁹ Het gaat in deze zaak om de vordering door de staat Alabama van een grote hoeveelheid documenten in het bezit van de *National Association for the Advancement of Coloured People*, waaronder ook de ledenlijsten. De vordering is gedaan in het kader van een procedure aangespannen door deze organisatie tegen een door de staat Alabama afgedwongen verbod tot verdere activiteiten in Alabama. Het Supreme Court oordeelt dat het recht van de leden van de organisatie verschoont te blijven van een dergelijke inmenging door de staat, valt binnen de bescherming die het Veertiende Amendement biedt.⁹⁰ Het Hof concludeert vervolgens dat het opvragen van de ledenlijsten een schending van het recht op vrijheid van vereniging uit het Eerste Amendement oplevert. Het Hof overweegt daartoe dat in dit geval voldoende aannemelijk is dat de productie van deze ledenlijsten een substantiële beperking van de uitoefening van dit recht door de leden op zou leveren.⁹¹ Het Hof is van oordeel dat het belang bij de ledenlijsten onvoldoende is aangetoond door de staat. Verenigingen hebben dus in bepaalde gevallen een sterke bescherming richting de overheid om persoonsgegevens

⁸⁸ Zie Heffernan 2001, LaFave 1996, Solove 2001, 2002a, 2002b, 2004, 2005 Hoofnagle 2004. Deze auteurs geven allen een oplossing door middel van een extensievere interpretatie van het Vierde Amendement dan nu door het Hof gevolgd. De kritiek komt er daarmee op neer dat het Hof het Vierde Amendement niet juist toepast en onvoldoende inspeelt op nieuwe (technologische) ontwikkelingen. Een andere oplossing is dat de gaten gevuld dienen te worden met statutaire wetgeving. Dit wordt voorgestaan door Kerr. Zie Kerr 2004 en Kerr 2005.

⁸⁹ *N.A.A.C.P. v. Alabama*, 357 U.S. 449 (1958).

⁹⁰ *Idem*, 460-461: “Freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the “liberty” assured by the Due Process Clause of the Fourteenth Amendment.”

⁹¹ *Idem*, 463: “In the circumstances of this case, compelled disclosure of petitioner’s membership lists is likely to constitute an effective restraint on its members’ freedom of association.”

van hun leden niet prijs te geven.⁹² Dit geldt zeker waar zij maatschappelijk controversiële zaken voorstaan, zoals emancipatie van Afro-Amerikanen in het zuiden van de V.S. in de jaren vijftig. Indien deze specifieke lijsten zouden kunnen bijdragen aan de oplossing van een misdrijf zouden ze evenwel door middel van een warrant verkregen kunnen worden. Het Eerste Amendement is overigens vaak ook een grond voor het schenden van de informationele privacy. Zo worden persoonsgegevens met een beroep op het Eerste Amendement op het internet gepubliceerd.

Het Fourth Amendment

Het Vierde Amendement is voor de bescherming van privacy in de constitutie het belangrijkste.⁹³ Het luidt:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Het Vierde Amendement bevat een aantal elementen. Over de precieze samenhang daartussen is veel geschreven. Belangrijk in dit verband is dat steeds de vraag gesteld moet worden of er sprake is van een doorzoeking vallend onder het Vierde Amendement. Als dit het geval is moet gekeken worden of deze onredelijk is. Een doorzoeking kan in beginsel slechts met een *warrant* plaatsvinden, dat wil zeggen een (rechterlijk) bevel tot arrestatie of doorzoeking.⁹⁴ Om een warrant te verkrijgen is *probable cause* vereist. Dit is een redelijk zwaar vereiste. Bij een huiszoeking zal het er om gaan of er een redelijk vermoeden is dat het gezochte bewijsmateriaal dat tot oplossing van het misdrijf zal kunnen leiden op de te doorzoeken plek aanwezig is.⁹⁵ De warrant wordt verkregen van de rechter. Er is dus sprake van rechterlijke toetsing vooraf. Achteraf wordt het Vierde Amendement gehandhaafd via de weg van de uitsluiting van het bewijs - het leerstuk van de *exclusionary rule*⁹⁶-, en in beperktere mate door civiele aansprakelijkheid. In de praktijk spelen warrants een beperkte rol. Er zijn namelijk zo talrijke uitzonderingen op het vereiste van een warrant, dat er in veel gevallen doorzoekingen en arrestaties mogelijk zijn met een verdenking minder zwaar dan vereist voor *probable cause*.⁹⁷

⁹² Dit is anders indien het illegale activiteiten betreft, zoals in het geval van de K.K.K. Zie *Bryant v. Zimmerman*, 287 U.S. 63.

⁹³ LaFave stelt zelfs: "The basic interest that the Fourth Amendment protects is the right of privacy", LaFave 1996, Pocketpart 2004, p. 743.

⁹⁴ Blok 2002, p. 169. Zie voor een korte uiteenzetting over en allerlei uitzonderingen op het vereiste van een warrant het artikel van Bowman, Bowman 2001.

⁹⁵ Ferdico 1993, p. 94.

⁹⁶ *Weeks v. United States*, 232 U.S. 383 (1914), *Mapp v. Ohio*, 367 U.S. 642 (1961). Voor een overzicht van de bescherming door de exclusionary rule in het kader van het Vierde Amendement, zie Solove 2002, noot 211.

⁹⁷ Dressler 2002, p.6.

Ontwikkeling van het privacybegrip in het Fourth Amendment

Het is nu goed om wat preciezer stil te staan bij de ontwikkeling van het privacybegrip in het Vierde Amendement. De uitspraken waarin het oude op het eigendomsbegrip gebaseerde privacybegrip van het Supreme Court duidelijk naar voren komt zijn *Boyd v. United States*⁹⁸ en *Olmstead v. United States*.⁹⁹ In *Olmstead* oordeelt het Hof dat het af luisteren zonder binnentreden van de woning geen probleem is. Er is immers geen inbreuk gemaakt op het eigendom. Deze uitspraak is fel bekritiseerd, onder meer door rechter Brandeis in zijn beroemde *dissenting opinion* bij deze uitspraak. Hij komt met een interpretatie van het Vierde Amendement, die veel meer op het recht op privacy is gebaseerd.¹⁰⁰ Het Supreme Court was echter lange tijd niet gevoelig voor de gevaren voor de privacy en in het bijzonder de communicatie die de combinatie van zijn opvatting over het Vierde Amendement en nieuwe af luistertechnologie opleverde.

De doorbraak ten aanzien van het privacybegrip in het Vierde Amendement kwam in de jaren zestig met de uitspraak *Katz v. United States*.¹⁰¹ Het Hof gaat om ten opzichte van het eerder ingenomen standpunt in *Olmstead*. Het betreft dit keer het af luisteren van een telefoongesprek in een telefooncel door middel van het plaatsen van af luisterapparatuur aan de buitenkant van de telefooncel. Hoewel hier geen sprake is van het binnendringen van een beschermde plaats, oordeelt het Hof dat er toch sprake is van een handelen in strijd met het Vierde Amendement. De meerderheid stelt nu dat het niet gaat om de vraag of er sprake is van een plaats die beschermd wordt,

*“[...] for the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. [...] But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”*¹⁰²

De na *Katz* gevolgde toets of er sprake is van een *reasonable expectation of privacy* komt uit de *concurring opinion* bij deze uitspraak van rechter Harlan:

*“My understanding of the rule [...] is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable.”*¹⁰³

⁹⁸ *Boyd v. United States*, 116 U.S. 616 (1886).

⁹⁹ *Olmstead v. United States*, 277 U.S. 438 (1928).

¹⁰⁰ *Idem*, 478.

¹⁰¹ *Katz v. United States*, 389 U.S. 347 (1967)

¹⁰² *Idem*, 351.

¹⁰³ *Idem*, 387.

Toen er in latere jaren er meer nadruk kwam te liggen op het belang van de opsporing, is van *reasonable legitimate* gemaakt en zijn daarmee beroepen op het Vierde Amendement afgewezen. Er kan zelfs gesproken worden van een benadering waar alleen nog bescherming geboden wordt indien er sprake is van totale geheimhouding.¹⁰⁴ Het Hof is daarnaast, in het geval dat er sprake is van een *legitimate expectation of privacy*, het belang van de bescherming van de privacy gaan wegen tegen de andere in het geding zijnde belangen.¹⁰⁵

Een belangrijke uitspraak is de uitspraak *Miller v. United States* in 1976.¹⁰⁶ In deze zaak was door de bank van Miller op basis van een subpoena duces tecum, blanco afgegeven door de grand jury en aangevuld door de openbare aanklager, een groot aantal documenten geleverd die betrekking hadden op zijn financiële gegevens. Miller stelde het gebruik van deze documenten in de tegen hem aangespannen strafzaak ter discussie. Volgens hem had hij een *reasonable expectation of privacy* in deze gegevens bij de bank en diende de documenten uitgesloten te worden van het bewijs op grond van een schending van het Vierde Amendement. Een verdeeld Hof oordeelde echter, in afwijking van de rechten in eerste en tweede aanleg, dat een persoon geen privacybelang heeft in deze documenten. Het Hof overweegt als volgt.

“We think that the Court of Appeals erred in finding the subpoenaed documents to fall within a protected zone of privacy.

On their face, the documents subpoenaed here are not respondent's "private papers." Unlike the claimant in Boyd, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks.”¹⁰⁷

Het Hof valt hiermee terug op de eigendomsdoctrine en perkt hiermee de werking van het Vierde Amendement in. Het expliciete beroep van de verdachte op de toets uit *Katz* wordt door het Hof verworpen.

“[...] we perceive no legitimate "expectation of privacy" in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”

¹⁰⁴ Solove 2002, p. 1131.

¹⁰⁵ *Vernonia School District v. Acton*, <http://laws.findlaw.com/us/000/u10263.html>. Het Hof stelt: “As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is “reasonableness.” [...] whether a particular search meets the reasonableness standard is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.” [...] *Delaware v. Prouse*, 440 U.S. 648, 654 (1979)”.

¹⁰⁶ *United States v. Miller*, 425 U.S. 435 (1976).

¹⁰⁷ *Idem*, 460.

Het Hof wijst er hier op dat de informatie geen vertrouwelijke communicatie is maar gerelateerd aan het handelsverkeer en dat de informatie vrijwillig aan de bank is verstrekt. Het Hof haalt vervolgens ter ondersteuning van haar standpunt, dat het Vierde Amendement geen bescherming biedt voor iemands financiële gegevens bij zijn bank, een drietal eerdere uitspraken aan.

*“The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. United States v. White, 401 U.S. 745, 751 -752 (1971). This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. Id., at 752; Hoffa v. United States, 385 U.S., at 302 ; Lopez v. United States, 373 U.S. 427 (1963).”*¹⁰⁸

Het Hof haalt hier uitspraken aan, waarin het Hof de rechtmatigheid van het handelen van undercoveragenten en informanten had beoordeeld. Het betreft hier de *assumption of risk* doctrine.¹⁰⁹ In *Hoffa* oordeelde het Hof dat het vertrouwen van iemand die een ander vrijwillig laat kennismaken van zijn handelen en er vanuit gaat dat deze dat geheim houdt voor de politie niet beschermd wordt door het Vierde Amendement.¹¹⁰ In *United States v. White* oordeelt het Hof dat iemands verwachting dat zijn bondgenoten noch helpers van de politie zijn noch haar helpers worden, en met name dat zij de gesprekken die ze onderling voeren, niet overbrieven aan de politie, niet gerechtvaardigd is.¹¹¹ Het aansluiten bij deze doctrine in het geval van *Miller*, is zwaar bekritiseerd.¹¹² Ten eerste op de grond dat het vrijwillig kennis laten nemen, in het geval van een bank, helemaal niet zo vrijwillig is. In de huidige maatschappij kun je nu eenmaal niet functioneren zonder een bankrekening. Dit geldt natuurlijk ook voor vele andere derden die persoonsgegevens hebben, zoals verhuurders, scholen, ziekenhuizen, en aanbieders van telecommunicatie. Ten tweede op de grond dat de verdachten in deze zaken uitspraken hadden gedaan in het bijzijn van de informanten met concrete incriminerende informatie, terwijl hier in het geval van *Miller* geen sprake is. De bank heeft de onderliggende transacties slechts nodig voor de administratieve afhandeling en is verder niet geïnteresseerd in deze informatie.

Met een verwijzing naar *Miller* oordeelt de kleinste meerderheid van het Hof in de zaak *Smith v. Maryland* dat iemand ook geen bescherming van het Vierde Amendement heeft van de

¹⁰⁸ *Idem*, 462.

¹⁰⁹ Zie Solove 2002a, p. 1135-1138. Zie ook Feinaut 1993, p.11 e.v.

¹¹⁰ *Hoffa v. United States*, 385 U.S. 293 (1966), 302.

¹¹¹ *United States v. White*, 401 U.S. 745 (1971), Feinaut 1993, p. 9.

¹¹² Hoofnagle 2004, p.15, LaFave 1996, p. 628-638, Heffernan 2001, in het bijzonder p. 37-42 en p. 86-87. Solove is van oordeel dat deze doctrine vergelijkbare ernstige tekortkomingen heeft als de eigendomsgerelateerde doctrine zoals in *Olmstead*, Solove 2002a, p. 1137.

telefoonnummers die hij belt.¹¹³ In deze zaak is door de politie zonder een warrant een zogenaamd *pen register* geïnstalleerd bij de telefoonmaatschappij, om de nummers die de verdachte met zijn huistelefoon belde te registreren. Het Hof overweegt dat als iemand al een privacy verwachting heeft in de nummers die hij met zijn huistelefoon belt, deze verwachting in elk geval niet legitiem is. Telefoongebruikers weten namelijk dat deze informatie door de telefoonmaatschappijen voor legitieme doeleinden geregistreerd en gebruikt kan worden.¹¹⁴ Het Hof concludeert dat een persoon met het bellen het risico heeft genomen dat de telefoonmaatschappij de informatie zou doorspelen aan de politie.¹¹⁵

De rol van het Vierde Amendement in het normatieve kader voor de toegang tot persoonsgegevens voor de opsporing is gezien het bovenstaande dus slechts zeer beperkt. Persoonsgegevens gehouden door een derde krijgen geen bescherming van het Vierde Amendement. Het maakt daarbij dus niet uit of het zeer gevoelige gegevens betreft. Het Hof heeft de nieuwe, minder op eigendom gebaseerde toets van *Katz* niet verder uitgewerkt, maar met de assumption of risk doctrine beperkt tot een doctrine van totale geheimhouding. Alles waar vrijwillig de mogelijkheid tot kennisname voor politie van open wordt gelaten is niet beschermd.¹¹⁶ Om Vierde Amendement bescherming te krijgen moet je totale geheimhouding betrachten. Dit is een lezing van het Vierde Amendement die veel kritiek heeft gekregen.¹¹⁷ Er wordt in de literatuur door velen opgeroepen tot een herziening van deze jurisprudentie. De Amerikaanse wetgever heeft ondertussen het gat, dat door het uitblijven van bescherming is gevallen, in een aantal sectoren gedicht door middel van eerdergenoemde statutaire wetgeving.¹¹⁸

Het Fourteenth en Fifth Amendment

Deze amendementen bevatten beiden de *due process*-clausule “*no person shall be deprived of life, liberty or property, without due process of law.*” Het Vijfde Amendement is gericht tegen de federale overheid, het Vijftiende Amendement tegen de Staten. Het Vijfde Amendement bevat bovendien het *nemo tenetur* beginsel, het verbod iemand te dwingen medewerking te verlenen aan zijn eigen veroordeling. Dit verbod heeft een privacybeschermend aspect. Het moeten afstaan van bepaalde informatie of documenten uit de privé-sfeer zou hieronder kunnen vallen. Het Supreme Court heeft deze bescherming echter geminimaliseerd. Ten eerste heeft het geoordeeld dat het Vijfde Amendement

¹¹³ *Smith v. Maryland*, 442 U.S. 735 (1979).

¹¹⁴ *Idem*, 742.

¹¹⁵ *Idem*, 744.

¹¹⁶ Dit geldt bijvoorbeeld ook voor zaken binnen hoge omheiningen die vanuit de lucht kunnen worden gezien, vuilniszakken die op straat worden gezet, de gezichtskenmerken waaronder het ras, het stemgeluid, gegevens over plaatsen in de openbare ruimte waar je je bevindt. Zie voor een overzicht Heffernan 2001.

¹¹⁷ Zie ook de dissenting opinions van rechter Marshall bij *Miller v. United States* en *Smith v. Maryland*. Zo is Marshall van mening dat “*it is idle to speak of “assuming” risks in contexts where, as a practical matter, individuals have no realistic alternative.*”, “*In my view, whether privacy expectations are legitimate within the meaning of Katz depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society.*”.

¹¹⁸ *Supra* noot 80 t/m 85.

niet van toepassing is op informatie die een burger verplicht is te verstrekken in verband met niet strafrechtelijke wetgeving, als het een algemene verplichting betreft, en het niet waarschijnlijk is dat de informatie zal worden gebruikt voor een strafrechtelijke vervolging.¹¹⁹ Het latere gebruik van deze informatie voor strafrechtelijke doeleinden is echter wel mogelijk.¹²⁰ Het Hof heeft in een latere uitspraak geoordeeld dat het Vijfde Amendement beschermd tegen “*compelled self-incrimination, not [the disclosure of] private information*”.¹²¹ Het Hof heeft het accent dus duidelijk weggelegd van de bescherming van privacy.

Het Veertiende Amendement richt zich tegen de Staten. De reeds besproken due process clause biedt niet slechts procedurele bescherming tegen staatsinmenging. Een deel van de rechten uit de Bill of Rights is via de due process bepaling op de Staten van toepassing. Hier valt ook de door de constitutie geboden bescherming van de privacy onder. De meeste uitspraken in dit verband gaan over de bescherming van fundamentele keuzevrijheid bij een aantal zaken, oftewel van persoonlijk autonomie. Deze jurisprudentie is bekritiseerd op dit onderbrengen van deze autonomie onder het recht op privacy.

Beroemd en controversieel zijn de uitspraken *Griswold v. Connecticut*¹²² en de hierop gebaseerde uitspraak *Roe v. Wade*.¹²³ In de zaak *Griswold* beoordeelt het Hof wetgeving, die de gebruik en de verschaffing van voorbehoedsmiddelen verbod, als ongrondwettig, want in strijd met een door het Hof ingelezen recht op privacy in de gezinssfeer. De staat kan dergelijke intimiteiten van het gezinsleven niet reguleren. In de zaak *Roe v. Wade* oordeelt het Hof dat het Texaanse verbod op abortus ongrondwettig is. Ook ditmaal gebeurt dit met een expliciete verwijzing naar een uit de Bill of Rights af te leiden recht op privacy. De zaak *Roe v. Wade*, maar nog meer de zaak *Griswold* speelt bij elke benoemingsprocedure voor nieuwe leden van het Supreme Court weer een rol.¹²⁴ Voor een uitvoerige bespreking van deze arresten verwijs ik naar het proefschrift van Blok.¹²⁵

De laatste hier te bespreken uitspraak over de bescherming van privacy door het Veertiende Amendement is de uitspraak van het Hof in de zaak *Whalen v. Roe*.¹²⁶ In deze uitspraak van het Hof is wel een recht op informationele privacy gelezen. Het ging hier om een wet van de staat New York. Deze wet gebod de centrale registratie van de persoonsgegevens van personen die door dokters medicijnen voorgeschreven kregen, die op de lijst van zwaardere narcotica voorkwamen. Het Hof noemt hier twee belangen die in het geding zijn. Ten eerste het belang bepaalde belangrijke beslissingen te nemen, zoals dat ook in de hiervoor genoemde zaken *Griswold* en *Roe v. Wade*

¹¹⁹ *Wilson v. United States*, 221 U.S. 361 (1911).

¹²⁰ *Garner v. United States*, 424 U.S. 648 (1976).

¹²¹ *Fisher v. United States*, 425 U.S. 391 (1976), 401.

¹²² *Griswold v. Connecticut*, 381 U.S. 479 (1965).

¹²³ *Roe v. Wade*, 410 U.S. 113 (1973).

¹²⁴ New York Times, 9 januari 2006, ‘Issues and (Possible) Answers: A Primer on the Alito Hearings’.

¹²⁵ Blok 2004, p. 178 e.v.

¹²⁶ *Whalen v. Roe*, 429 U.S. 589 (1977).

speelde.¹²⁷ Daarnaast noemt het Hof het individuele belang bepaalde persoonlijk zaken niet openbaar te maken.¹²⁸ Het Hof komt in deze zaak tot de conclusie dat de registratie voldoende beveiligd is tegen misbruik van de informatie en dat de geringe te achten mogelijkheid dat de informatie wordt gebruikt als bewijs in een strafproces niet voldoende is om de registratie ongrondwettig te verklaren.¹²⁹ Het Hof weerspreekt daarnaast dat de registratie personen af zou houden zich de medicijnen voor te laten schrijven, aangezien vast staat dat maandelijks zo'n 100.000 maal voorgeschreven bleek te zijn. Het Hof concludeert vervolgens dat de registratie een redelijke uitoefening van de ruime bevoegdheden van de staat is.¹³⁰ Het Hof heeft het aspect van de informationele privacy uit deze uitspraak niet verder uitgewerkt in latere jurisprudentie. De lagere rechtspraak heeft verdeeld gereageerd. Sommige lagere rechtbanken hebben een recht op informationele privacy ontwikkeld vanuit een focus van dit recht op de mogelijkheid tot participatie. Andere hebben het beperkter gehouden met een focus op afscherming, en beroepen op dit recht in de meeste gevallen afgewezen.¹³¹

Gevolgen voor de toegang tot persoonsgegevens voor de opsporing

Na deze behandeling van de bescherming van de informationele privacy kunnen we een aantal conclusies trekken. Ten eerste dat de bepaling die bij uitstek bescherming biedt tegen politieoptreden in de vorm van doorzoekingen en inbeslagnames, niet van toepassing is op het verkrijgen van (persoons)gegevens bij derden. Het warrant vereiste van het Vierde Amendement, of beter gezegd wat daarvan over is, is als gevolg daarvan hierop niet van toepassing. De due process bepaling uit het Vijfde en het Veertiende Amendement bevat een privacybeschermend element. De informationele privacy is door het Hof echter slechts in het kader van de beoordeling van de grondwettelijkheid van statelijke wetgeving in de constitutie ingelezen. Als er al bescherming is, dan is dat bescherming tegen het openbaar worden van bepaalde gegevens, die een rol spelen bij de persoonlijke autonomie. Het zal mijns inziens dan vooral gaan om gevoelige gegevens. Dit geldt ook voor de bescherming van het Eerste Amendement. Op grond van dit Amendement zullen de ledenlijsten van politiek actieve verenigingen in bepaalde gevallen wel bescherming krijgen van de constitutie, zij het afgeleide bescherming.

Het gat dat daarmee is ontstaan, is op onderdelen opgevuld door eerdergenoemde statutaire wetgeving. Deze wetgeving regelt in de meeste gevallen ook het gebruik van de gegevens voor strafvordering. Dit gebeurt door eisen te stellen aan de wijze van verkrijging en openbaarmaking in strijd met de regels te sanctioneren. In de meeste gevallen is verkrijging middels een subpoena of *court order* mogelijk.¹³² Een gebrek is dat deze wetgeving aangrijpt bij het soort houder van de

¹²⁷ Idem, 592-593.

¹²⁸ Idem, 599-600.

¹²⁹ Idem, 601-602.

¹³⁰ Idem, 596-598.

¹³¹ Schwartz & Reidenberg 1996, p. 77.

¹³² Solove 2002a, p. 1149.

gegevens. Indien dezelfde gegevens bij een houder aanwezig zijn die niet onder deze regels valt, dan geldt de regeling niet.

In de gevallen dat de gegevens geen statutaire bescherming genieten, is een subpoena of een court order voor justitie genoeg, om de gegevens te verkrijgen. Voor de rechtmatigheid van de subpoena is het genoeg dat de gegevens relevant zijn voor het strafproces. Er dient dus enig verband te zijn met het onderzochte misdrijf. Als voorbeeld kan dienen de regeling betreffende financiële gegevens. Om deze gegevens bij banken te verkrijgen dient justitie gebruik te maken van een warrant of een subpoena. Om de subpoena te verkrijgen dient er relevantie te zijn van de daarmee te verkrijgen gegevens voor een legitiem opsporingsonderzoek.¹³³ Er geldt een andere regeling voor gegevens bij kredietregistratiebureaus. De identificerende gegevens (*headers*) bij deze bureaus kunnen op verzoek verstrekt worden; er gelden daarvoor geen eisen.¹³⁴ Voor de andere gegevens dient justitie een grand jury subpoena of court order te verkrijgen. Als deze gegevens bij een andere derde berusten, valt de verstrekking aan justitie niet onder de statutaire regeling.

Persoonsgegevens kunnen in het geval dat er geen statutaire regeling van toepassing is, al naar gelang het privacy beleid van de houder van gegevens, ook vrijwillig verstrekt of verkocht worden. Dit is een veel voorkomende praktijk. Er zijn talloze bedrijven in de Verenigde Staten, waaronder het inmiddels beruchte Choicepoint, waarvan de handel in persoonsgegevens met justitie tot de kern van de bedrijfsactiviteiten behoort.¹³⁵ Deze *data brokers* beheren en bewerken deze gegevens tot voor hun klanten bruikbare informatie.¹³⁶ Één van deze klanten is justitie; justitie sluit miljoenencontracten met dit soort bedrijven om te kunnen profiteren van op maat gemaakte informatie.¹³⁷ Een interessante vraag is in welk deel van de behoefte aan persoonsgegevens door deze data brokers kan worden voorzien.

De bestrijding van terrorisme heeft de handel in persoonsgegevens en de ontwikkeling van technieken voor het gebruik van deze gegevens doen toenemen. Het *Department of Homeland Security* heeft jaarlijks vele miljoenen beschikbaar gesteld voor het benutten van private databases en de ontwikkeling van nieuwe zoektechnieken.¹³⁸ De informatievergaring ter bescherming van nationale veiligheid is relevant voor de strafvordering, omdat er weinig barrières zijn voor het gebruik van informatie van de veiligheidsdiensten voor de strafvordering.¹³⁹ Met de *USA PATRIOT Act*¹⁴⁰ zijn de

¹³³ 29 U.S.C. § 3407.

¹³⁴ 15 U.S.C. § 1681 f.

¹³⁵ Het betreft naast het hiergenoemde Choicepoint, bijvoorbeeld ook LexisNexis, Dun & Bradstreet, Experian Inc. Zie Hoofnagle 2004. Zie ook Solove 2002a, p. 1095-1101.

¹³⁶ Hoofnagle 2004, p. 16, Solove 2002b, p.1150-1152.

¹³⁷ Solove 2002b, p.1151.

¹³⁸ Dit gebeurde bijvoorbeeld in het kader van het programma *Total Information Awareness*. Dit programma is nu door het Congress gestopt. Vergelijkbare projecten lopen echter door. Zie Dempsey & Flint 2004. Voor een bespreking van de zoektechnieken die in het kader van de terrorismebestrijding ontwikkeld worden, zie Weiss 2004. De ontwikkelde technologie is natuurlijk ook voor het Nederlandse recht relevant.

¹³⁹ *In re Sealed Case*, 310 F.3d 717 (2002), 728 (United States foreign intelligence court of review).

¹⁴⁰ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (The USA PATRIOT Act)*, Pub. L. 107-56, 115 Stat. 272.

bestaande barrières voor de uitwisseling van informatie tussen de verschillende overheidsdiensten vrijwel verdwenen.¹⁴¹ In de richtlijnen van de Attorney General is rekening gehouden met de gewenste mogelijkheid van de toegang tot deze gegevens bij data brokers. De richtlijnen staan toe dat de gegevens worden geraadpleegd in elk stadium van het onderzoek.¹⁴² Dit betekent dat zelfs als er geen aanwijzing is, dat er een strafbaar feit is gepleegd, toegang gezocht kan worden tot persoonsgegevens in de private sector waar geen statutaire bescherming voor geldt.

Een groot deel van de persoonsgegevens wordt door de data brokers verzameld uit publiek toegankelijke persoonsgegevens.¹⁴³ Deze gegevens worden vrijgegeven om verschillende redenen.¹⁴⁴ De overheid legt hiermee bijvoorbeeld verantwoording af. Verder zijn veel gegevens publiek toegankelijk ten dienste van het private rechtsverkeer. Van bijna elke Amerikaan is uit deze publieke gegevens op eenvoudige en rechtmatige wijze een grote hoeveelheid data te verzamelen. Het gaat dan bijvoorbeeld om naam, adres, oud adres, huizenbezit, kredietwaardigheid, uitoefening van bepaalde geregistreerde beroepen, bijbehorende diploma's, telefoonnummer, *social security number*, en gegevens over strafrechtelijke veroordelingen.¹⁴⁵ Door het gemak waarmee deze publieke gegevens tegenwoordig te verzamelen zijn is er discussie over het zoeken naar een nieuwe balans tussen het publieke belang bij open toegang en het belang van de bescherming van persoonsgegevens.¹⁴⁶ Vroeger was dit soort data-aggregatie niet goed mogelijk door de bestaande *practical obscurity*; de gegevens waren verspreid over het hele land in kleine lokale administraties.¹⁴⁷ Het online beschikbaar maken van publieke databases heeft de toegang nu gemakkelijk en dus zelfs exploiteerbaar gemaakt.

Naast het verzamelen van publieke gegevens verkrijgen deze bedrijven gegevens uit de particuliere sfeer. Dan valt bijvoorbeeld te denken aan gegevens over betalingen met creditcard, bestedingspatronen, internetgedrag, belgedrag, medische gegevens die iemand heeft ingevuld om online medisch advies te krijgen, en een keur aan andere gegevens. De data brokers weigeren vaak enig belang van de betrokkene te onderkennen en stellen slechts verplichtingen te hebben jegens hun klanten. Goede informatie over wat met de gegevens wordt gedaan, en rechten op inzage en verbetering zijn afwezig. Het verkeerd geregistreerd staan in dit soort bestanden heeft menig Amerikaan al opgebroken bij het vinden van een nieuwe baan.

¹⁴¹ Weiss 2004, p. 260.

¹⁴² *Attorney general guidelines, Introduction*, paragraaf C, en hoofdstuk IV.

¹⁴³ Hoofnagle 2004, p. 15. Solove 2002b, p.1139-1141.

¹⁴⁴ Zie voor een uitvoerige bespreking Raul 2002.

¹⁴⁵ Solove 2002b, p. 1142-1149

¹⁴⁶ Zie onder meer Raul 2002, en Solove 2002b, p. 1173 e.v.. In de discussie over de problemen van het gemak waarmee zoveel persoonsgegevens te verzamelen zijn speelt de opkomst van *identity fraud* een centrale rol. Zo heeft Choicepoint zich moeten excuseren tegen meer dan 100.000 burgers van Californië, omdat criminelen een bestand met gegevens hadden verkregen en daarmee *identity fraud* pleegden.

¹⁴⁷ Raul 2002, p. 53 e.v.

Conclusie

In de Verenigde Staten is de toegang van tot persoonsgegevens voor de opsporing van strafbare feiten niet genormeerd door een zelfstandig grondrecht op informationele privacy. Deze situatie is verschillend van Nederland waar grondrechtelijke bescherming van de informationele privacy bestaat op grond van artikel 10 Gw en artikel 8 EVRM. Het grondrecht dat hiervoor in de Verenigde Staten in aanmerking zou komen, namelijk het Fourth Amendment, biedt geen bescherming. De reden hiervoor is dat de gegevens door de betrokkene vrijwillig zijn vrijgegeven. De betrokkene heeft daarmee zijn reasonable expectation of privacy verspeelt. Van een inbreuk op de privacy van de betrokkene kan daarom geen sprake zijn. Er kan wel sprake zijn van constitutionele bescherming in het geval het gebruik van de gegevens inbreuk maakt op andere grondrechten, zoals het recht op vrijheid van vereniging, maar deze bescherming is dus afgeleid van andere grondrechten.

De toegang tot gegevens is juist vanwege de afwezigheid van constitutionele bescherming binnen een aantal sectoren gereguleerd door statutaire wetgeving. In dat geval kan justitie persoonsgegevens gegevens verkrijgen middels een subpoena of court order. In het geval er geen statutaire wetgeving is, en de houder van de gegevens niet vrijwillig wil meewerken, is de subpoena ook het geëigende middel om gegevens te verkrijgen. De eisen die aan de subpoena worden gesteld zijn niet zwaar. Ze worden vaak blanco afgegeven en enig belang voor het onderzoek is genoeg om de subpoena rechtmatig te maken. Er is ten aanzien van de uitoefening van de subpoena wel een mogelijkheid van rechterlijke toetsing vooraf, maar dit verzet biedt weinig materiële bescherming.

Een groot deel van de stromen van persoonsgegevens is dus in het geheel niet genormeerd door het federale recht. Een aantal data brokers maakt van deze situatie gebruik om gegevens te verzamelen en te verkopen aan justitie. Dit is een groot verschil met Nederland, waar alle persoonsgegevens zijn genormeerd gezien de algemene regels van de Wbp, en artikel 10 Gw en artikel 8 EVRM.

Hoofdstuk 3 De juridische grondslag voor de bescherming van persoonsgegevens

Om een beter inzicht te krijgen in de afweging van de wetgever tussen het belang van de opsporing en het belang van de bescherming van persoonsgegevens zal in dit laatste hoofdstuk worden stilgestaan bij de grondslagen van de bescherming van informationele privacy. Er zal hier worden ingegaan op een alternatieve grondslag voor het gegevensbeschermingsrecht. Dit is de grondslag zoals door Blok verdedigd, onder meer in zijn proefschrift “Het recht op privacy”.¹⁴⁸ Vanuit deze grondslag zal worden gereflecteerd op het normatieve kader dat is toegepast bij de nieuwe regeling van het vorderen van gegevens door justitie en de bezwaren die door de verschillende commentatoren ten aanzien van de nieuwe bevoegdheden zijn opgeworpen.

Bescherming van persoonsgegevens: privacybescherming of machtsbeheersing

Het gegevensbeschermingsrecht is ontstaan als een reactie op groeiend gebruik van registraties van persoonsgegevens door de overheid. De opkomst van informatietechnologie en de automatisering van persoonsregistraties vanaf de jaren zestig van de vorige eeuw was gericht op een grotere efficiëntie van de overheid, maar bracht ook bepaalde gevaren met zich mee. De reactie vanuit de wetenschap en het publieke debat wezen op een toename van macht van de gegevensverwerkers ten opzichte van het individu. De overheid zou door middel van de aan persoonsregistraties ontleende informatiemacht haar greep op het individu vergroten en de private sector zou net zo haar positie ten opzichte van de consument kunnen versterken. De nadruk in de commentaren lag in eerste instantie op de noodzaak deze aan persoonsregistraties ontleende macht van de noodzakelijke controlemechanismen te voorzien.¹⁴⁹

Bij de zoektocht in het recht naar de juiste aanknopingspunten voor een regeling van het gegevensbeschermingsverkeer werd de keuze aan te knopen bij het grondrecht op de persoonlijke levenssfeer al snel dominant in de discussie.¹⁵⁰ Dit grondrecht moest de grondslag gaan bieden voor het gegevensbeschermingsrecht en de wetgever heeft deze opvatting gevolgd op advies van de Commissie Koopmans. De regering had deze commissie in 1972 ingesteld om een advies te geven over de problematiek van de bescherming van de persoonlijke levenssfeer in verband met persoonsregistraties. De Commissie Koopmans concludeerde dat het klassieke recht op privacy, dat slechts bescherming biedt voor de intieme levenssfeer van het huis en de familie, diende te worden aangepast aan de behoeften van de informatiemaatschappij.¹⁵¹ De Commissie Koopmans overweegt als volgt: *‘Kon men de persoonlijke levenssfeer tot voor kort bij uitstek associëren met de strikte privé-sfeer (huisrecht, correspondentiegeheim, gezinsleven, e.d.), de nieuwe opvattingen betreffen de*

¹⁴⁸ Blok 2002.

¹⁴⁹ Idem, p. 117.

¹⁵⁰ Idem, p. 120.

¹⁵¹ Idem, p. 121.

bescherming van de persoon ook als deelnemer aan het maatschappelijk verkeer'.¹⁵² Daarmee is het gegevensbeschermingsrecht dus in essentie de bescherming van privacy geworden, met een uitbreiding van reikwijdte van dit privacybegrip als noodzakelijk gevolg.

Blok beargumenteert overtuigend dat het recht op privacy een ongeschikte grondslag biedt voor beperking van de gevaren die samenhangen met de verwerking van persoonsgegevens.¹⁵³ De ratio van een regeling van de stromen van persoonsgegevens is vooral gelegen in de behoefte aan bescherming tegen de aan de verwerking van persoonsgegevens ontleende informatiemacht. Aanvankelijk was het uitgangspunt in de discussie over gegevensbeschermingsrecht dan ook dat er behoefte was aan controlemechanismen, die de aan persoonsregistraties te ontleenen informatiemacht zouden normeren. Deze regels moesten er voor zorgen dat burgers inzicht zouden hebben in de verwerking van hun persoonsgegevens, moesten waarborgen bevatten tegen de gevaren van het gebruik van onjuiste gegevens, en dienden burgers een bepaalde mate van zeggenschap te geven over de verwerking van hun persoonsgegevens.

Persoonsgegevens kunnen betrekking hebben op de persoonlijke levenssfeer in strikte zin maar hebben dit veelal niet. Blok concludeert dat het recht op privacy is verwaterd door de rol die het gevraagd wordt te spelen bij de bescherming van persoonsgegevens. Het is met betrekking tot de bescherming van persoonsgegevens verworden tot een aantal beginselen van behoorlijk gegevensbeheer en daarmee van een geheel ander karakter dan de onschendbaarheid van de huiselijke sfeer of het briefgeheim. Het recht tot bescherming van de informationele privacy bevat voornamelijk regels die inbreuken op de persoonlijke levenssfeer legitimeren en reguleren.¹⁵⁴ Het gaat er dus in dit rechtsgebied om de informatiestromen in goede banen te leiden en niet om deze te blokkeren. Met een omweg en gebaseerd op een verkeerde grondslag is wel gekomen tot de nodige controlemechanismen voor de aan verwerking van persoonsgegevens ontleende informatiemacht, aldus Blok.¹⁵⁵ Het beheersen van informatiemacht had echter ook tot stand gebracht kunnen worden door aan te knopen bij al in het recht bestaande mechanismen van machtsbeheersing. De nodige transparantie, verantwoording en toezicht en de rechten van inspraak waren op die manier ook zonder het zeer onduidelijke recht op informationele privacy mogelijk geweest.

Blok pleit daarom voor een herziening van het gegevensbeschermingsrecht en de grondrechtelijke bescherming van persoonsgegevens. Volgens Blok had men voor wat betreft het publiekrecht beter kunnen aansluiten bij de al bestaande rechtsstatelijke eisen en beginselen van behoorlijk bestuur die de overheidsmacht reguleren en beheersen. Voor wat betreft het privaatrecht had een regeling voor de hand gelegen die gericht is op ongelijkheidscompensatie, zoals bijvoorbeeld bestaat in het arbeidsrecht of het consumentenrecht. Voor een zelfstandig grondrecht op informationele privacy is vanuit deze visie geen plaats. De rechtstatelijke eisen geven wel aanleiding

¹⁵² Commissie Koopmans 1974, p.7.

¹⁵³ Zie Blok 2001, en Blok 2002, p. 128.

¹⁵⁴ Schreuders 2001, p. 87

¹⁵⁵ Blok 2002, p. 128.

voor een van de al geldende grondrechten afgeleid grondrecht op bescherming van persoonsgegevens. Daar is immers aanleiding toe als de gegevensverwerking raakt aan de persoonlijke levenssfeer in striktere zin, of andere grondrechten, zoals het recht op vertrouwelijke communicatie, of de vrijheid van meningsuiting of vereniging.

De informatiele privacy en artikel 8 EVRM

Blok besteedt in zijn proefschrift weinig aandacht aan artikel 8 EVRM. Het Europese Hof voor de Rechten van de Mens lijkt echter stevig te hebben bijgedragen aan een grondslag voor het gegevensbeschermingsrecht in het grondrecht op privacy. Het Hof heeft in de loop der jaren een zeer ruim recht op bescherming van het privé-leven erkend, inclusief een ruime bescherming van de informatiele privacy. Het Hof heeft daarbij weinig moeite gedaan dit ruime recht op informatiele privacy te voorzien van een heldere afbakening. In de meeste jurisprudentie van het Hof gaat het er dientengevolge om of een inbreuk op het ruime recht van artikel 8 lid 1 EVRM, de toets van het tweede lid kan doorstaan. In het eerste hoofdstuk is reeds uitvoerig stilgestaan bij de verschillende eisen die uit de jurisprudentie van het Hof over artikel 8 lid 2 EVRM zijn af te leiden. Het komt er daarbij samengevat op neer dat de regeling die inbreuk maakt op de informatiele privacy moet voldoen aan de rechtstatelijke eis, dat de regeling kenbaar en voldoende precies dient te zijn. Daarnaast staat de proportionaliteitseis centraal. Om deze reden komt de bescherming van de informatiele privacy in het kader van het EVRM neer op een regulering en legitimering van stromen van persoonsgegevens. De aangenomen inbreuk op de persoonlijke levenssfeer voltrekt zich op de achtergrond en geeft weinig houvast bij de te maken afweging. Bij de afweging krijgen nationale overheden dan ook nog eens een behoorlijke beoordelingsvrijheid, die de bescherming van de informatiele privacy alleen nog maar onduidelijker maken.

De Wet bevoegdheden vorderen gegevens

Als uitgaande van het bovenstaande wordt gekeken naar de wetgevingsgeschiedenis van de Wet bevoegdheden vorderen gegevens, dan blijkt dat de wetgever is uitgegaan van de conventionele in de privacy gelegen grondslag van gegevensbescherming en weinig oog heeft gehad voor het perspectief van de verschuiving van macht van de burger naar de overheid. Het ontwerp van de regeling is gebaseerd op de aard van de gegevens. Dit is typisch een met de grondslag van de gegevensbescherming samenhangende conceptie: dat het bij de bescherming in verband met gegevensverwerking gaat om bescherming van gegevens. De aard en de gevoeligheid van de gegevens is daarmee in grote mate bepalend voor de mate van bescherming en niet het betreffende gebruik van de gegevens.

Er wordt nergens expliciet gesproken over de achterliggende ratio van de regeling, namelijk het versterken van de informatiemacht van justitie. De specifieke gevaren die aan het gebruik van persoonsgegevens uit het maatschappelijk verkeer voor de opsporing vastzitten worden daarnaast niet

nader geanalyseerd. Ook het soort gebruik door de instelling waar de gegevens worden gevorderd speelt in de regeling geen expliciete rol. De inbreuk op de persoonlijke levenssfeer wordt niet concreet gemaakt en is in veel gevallen, zoals in het geval van identificerende gegevens, ook moeilijk voor te stellen. Daarmee valt de afweging ten opzichte van het belang van de opsporing van strafbare feiten wel erg gemakkelijk uit in het voordeel van de opsporing.

Gezien het bovenstaande zal ik hier nog stilstaan bij de diverse bezwaren die de verschillende commentatoren op de introductie van de bevoegdheden tot het vorderen van gegevens hebben gemaakt. Deze wijzen steeds in de richting van het belang van geëigende en zwaardere controlemechanismen ter beteugeling van de informatiemacht van justitie en het gebruik daarvan.

Ten eerste betreft het bezwaren die raken aan een van de belangrijkste controlemechanisme uit het gegevensbeschermingsrecht, namelijk het vereiste van doelbinding. Waar het doorbreken van de doelbinding een uitzondering was, is het met de nieuwe bevoegdheden eerder de regel geworden. Dit is een politieke keuze die door de wetgever gerechtvaardigd is vanuit het belang van de opsporing van strafbare feiten. Het principe van doelbinding is daarmee echter vergaand uitgehold.¹⁵⁶ De burger moet er rekening mee houden dat alle op hem gerichte informatiemacht – die overigens op verschillende wijzen veelal ten dienste van hem bestaat en wordt uitgeoefend – ook voor de opsporing van strafbare feiten kan worden gebruikt. Justitie kruipt hiermee een flink stuk naar de burger toe door verwerkers van persoonsgegevens tot regulier tappunt te maken voor de strafvordering.¹⁵⁷ Op grond van artikel 9 van het Databeschermingsverdrag dient het verbreken van de doelbinding noodzakelijk te zijn in een democratische samenleving. Dat is vanuit de visie van Blok op gegevensbescherming en het recht op privacy, iets anders dan dat de inbreuk die op de persoonlijke levenssfeer wordt gemaakt ten gevolge van het doorbreken van het beginsel van doelbinding noodzakelijk moet zijn in een democratische samenleving.

Een ander bezwaar, dat vooral in het werk van MacGillavry is te vinden, is dat met de nieuwe bevoegdheden een vergaande informatieplicht in het leven wordt geroepen.¹⁵⁸ Er van uitgaande dat er inderdaad sprake is van een dergelijke informatieplicht breekt dit inderdaad met de systematiek van het strafprocesrecht waarin vrijwilligheid aan het meewerken een uitgangspunt is. Het feit dat medewerking vrijwillig geschied, maakt het voor burgers mogelijk een eigen belangenafweging te maken. Daarbij hoeft het in het geheel niet te gaan om het belang inbreuken op de persoonlijke levenssfeer te beperken maar kan het gaan om het voorkomen van schade door eventueel ingrijpen door justitie, de angst voor represailles, en andere nadelige gevolgen. De met opsporing belaste ambtenaren zijn moeilijk in staat deze belangen mee te wegen en ook de wetgever lijkt hier niet aan toegekomen. Dit tegenwicht dat vanuit de maatschappij - al dan niet terecht - aan het ingrijpende

¹⁵⁶ Zie in bijzonder Dommering 2001, Stevens, Koops & Wiemans 2004, en Van Grinsven 2004

¹⁵⁷ Vergelijk Dommering 2000, p. 495.

¹⁵⁸ MacGillavry 2002.

karakter van het strafrechtelijk apparaat met de bijbehorende sancties wordt geboden, is met de nieuwe wet geschiedenis geworden.

Een van de meest gehoorde bezwaren is het gevaar dat de vordering van gegevens van een bepaalde persoon van invloed zou kunnen zijn op de dienstverlening door de houder van de gegevens.¹⁵⁹ Het handelen van opsporingambtenaren kan een bepaald beeld van de betrokkene scheppen bij de houder, dat zou kunnen leiden tot aanpassing of beëindiging van de betreffende dienstverlening. Aan dit gevaar zou justitie deels tegemoet kunnen komen door een goede voorlichting in geval van gebruik van de bevoegdheden, in het bijzonder wanneer gegevens van niet verdachte personen worden gevorderd.

Een ander bezwaar is dat justitie de neiging zal krijgen beslissingen te baseren puur gebaseerd op persoonsgegevens.¹⁶⁰ Personen worden door het gebruik van persoonsgegevens gereduceerd tot een virtuele persoonlijkheid. Een gevaar dat daarmee samenhangt, is dat de gevorderde gegevens onjuist kunnen zijn, en daarmee ook het virtuele beeld dat van iemand ontstaat. Dit gevaar blijft in de gekozen regeling voor risico van de betrokkene en de houder van gegevens. Het beeld kan slechts achteraf worden betwist. Het heeft voor justitie in beginsel geen gevolgen als de gegevens of de conclusies die eruit getrokken worden onjuist zijn, behalve natuurlijk dat er verkeerde beslissingen worden genomen en dat daarmee kostbare middelen verkeerd worden ingezet. Dit ongewenste gevolg is niet ondenkbeeldig; justitie voorziet de bevoegdheden veel te gaan gebruiken. In het geval dat gegevens van banken verkregen worden, zullen de gegevens naar mag worden aangenomen over het algemeen accuraat zijn. Dit is heel anders bij bestanden waar geen enkele bestrijding van fraude wordt ingezet, zoals bij de gegevens die Albert Heijn verkrijgt via de bonuskaarten. In dat laatste geval is er geen enkele redelijke waarborg dat de gegevens juist zijn. In het geval van de georganiseerde misdaad en de bestrijding van terrorisme is de kans dat gegevens onjuist zijn alleen nog maar groter. Daarbij betrokkenen zullen immers waar mogelijk gebruik maken van valse identiteiten. Daarmee wijzen de gevorderde gegevens dus naar de verkeerde personen, met alle vervelende gevolgen van dien. Ten slotte dient in dit verband gewezen te worden op de aanzienlijke problemen die de betwisting van de juistheid van de verkregen gegevens voor de betrokkene kan opleveren.

Het toezicht door een onafhankelijke rechter is natuurlijk in het strafrecht het procedurele mechanisme bij uitstek om controle op de machtsuitoefening door justitie te bieden. Dit toezicht vindt echter met uitzondering van de vordering van bijzondere gegevens achteraf plaats. In dit verband moet nog eens opgemerkt worden dat de deuren van de toegang wagenwijd openstaan en dat het er bij de beoordeling van de rechtmatigheid er dus voornamelijk op neer zal komen dat de rechter beziet of de juiste vormvereisten voor de betreffende vordering en het proces-verbaal in acht zijn genomen. Dit is mijns inziens een gemiste kans. Zwaardere inhoudelijke criteria voor het doorbreken van de doelbinding waren met het oog op de zwakke argumentatie van de wetgever of de inbreuk op

¹⁵⁹ Zie bijvoorbeeld MacGillavry 2004, 489.

¹⁶⁰ Buruma 2004, p. 669.

de persoonlijke levenssfeer en het doorbreken van de doelbinding wel noodzakelijk is in een democratische samenleving, een grote verbetering geweest.

Conclusie

De wet bevoegdheden vorderen gegevens introduceert een aantal bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering. Gezien de potentiële zware inbreuk die deze bevoegdheden geacht worden te kunnen maken op de persoonlijke levenssfeer zijn de bevoegdheden zeer precies omschreven met een systematiek van oplopende voorwaarden naar gelang de gevorderde gegevens meer blootleggen van of dichter raken aan de persoonlijke levenssfeer. De systematiek is er op gericht om zoveel mogelijk gegevens toegankelijk te maken voor de opsporing.

De concrete inbreuk op de persoonlijke levenssfeer die het toepassen van de bevoegdheden zouden opleveren is door de wetgever niet onderzocht. De mogelijke inbreuk is aangenomen en vervolgens gelegitimeerd door bij het ontwerp rekening te houden met de eisen van artikel 8 lid 2 EVRM. Dit wordt ingegeven door het ruime en onduidelijke recht van artikel 8 lid 1 EVRM, dat de bescherming tegen inbreuken op de informationele privacy omvat. Het nadeel van zo'n ruim recht is, dat de bescherming die het biedt noodzakelijkerwijs beperkt is, en in gevallen een symbolische waarde krijgt; hoe ruimer het recht, hoe meer inbreuken immers noodzakelijk worden. Dit leidt dan wel tot zeer gedetailleerde regelingen, maar blokkeert bepaalde inbreuken niet.

Op de argumentatie van de wetgever dat de bevoegdheden noodzakelijk moeten zijn in een democratische samenleving, is de nodige kritiek te leveren. Deze kritiek, die voor een deel samenvalt met de vraag naar de rechtvaardiging van het doorbreken van het beginsel van doelbinding van de verwerking van persoonsgegevens, is op onderdelen zelfs overtuigend te noemen. Uitspraken van het Europese Hof in concrete gevallen zullen moeten uitwijzen of dit zal worden onderkend.

Waar in Europa de werking van de grondrechten, en in het bijzonder het recht op de persoonlijke levenssfeer is aangepast aan de technologie van geautomatiseerde gegevensverwerking is dit in de Verenigde Staten niet het geval. De toegang van opsporingsambtenaren tot persoonsgegevens bij houders is niet genormeerd door de constitutie. Het Supreme Court heeft met betrekking tot het Vierde Amendement een doctrine ontwikkeld die betrokkenen iedere legitieme privacyverwachting ten aanzien van aan derden afgestane persoonsgegevens ontzegt. Om die reden is de toegang tot persoonsgegevens slechts genormeerd door statutaire en statelijke wetgeving voor verschillende sectoren waar het uitblijven van bescherming door de wetgever onacceptabel werd geacht. De gaten die overblijven zijn aanzienlijk en worden te gelde gemaakt door bedrijven die persoonsgegevens verzamelen en verkopen aan justitie. Die praktijk is aan discussie onderhevig. De meeste commentatoren denken bij het zoeken naar een oplossing aan herziening van de rechtspraak van het Supreme Court, waarbij via het recht op privacy wel constitutionele bescherming wordt toegekend aan persoonsgegevens bij derden. Er is echter geen aanwijzing dat deze aanbevelingen zullen worden opgevolgd. De oplossing voor het gebrek aan normering zal eerder moeten komen van de wetgever dan de rechter.

Indien wordt stilgestaan bij de achtergrond en de juridische grondslag van het gegevensbeschermingsrecht en de opgeworpen bezwaren tegen de nieuwe bevoegdheden dan is de visie van Blok verhelderend. Het had in het ontwerp van de wetgever en in de voorafgaande discussie over de toegang tot persoonsgegevens voor de opsporing meer moeten gaan over de regulering en beheersing van overheidsmacht, dan over het voorkomen van inbreuken op de persoonlijke levenssfeer. Zo krijgen de beginselen van behoorlijke gegevensverwerking, zoals het beginsel van doelbinding, ook een zelfstandige waarde, in plaats van dat zij alleen worden gepercipieerd als mechanismen ter bescherming van een uitgebreide en onduidelijke bescherming van deze persoonlijke levenssfeer.

De conclusie van deze scriptie is gezien het bovenstaande dat de afweging die door de wetgever is gemaakt op een aantal punten gebrekkig is. Het betreft dan vooral de rechtvaardiging van het doorbreken van het beginsel van doelbinding en de argumentatie dat de bevoegdheden noodzakelijk zijn in een democratische samenleving. De verklaring hiervoor is ten dele te vinden in de grote nadruk die de wetgever legt op de bestrijding van misdaad. Voor een deel lijkt echter de systematiek en de grondslagen van het gegevensbeschermingsrecht hier dus zelf debet aan.

Het huidige juridische instrumentarium voor de weging van het belang van de burger geeft onvoldoende inzicht in de achterliggende belangen van de burger. Het extrapoleren van het klassieke vrijheidsrecht op respect van de persoonlijke levenssfeer naar een voldoende betekenisvol vrijheidsrecht in het gegevensbeschermingsrecht is dus niet geslaagd. Verder onderzoek naar de belangen van de burger bij beperking van gegevensverwerking, die niet uitgaan van de idee dat deze belangen gelegen zijn in de bescherming van de persoonlijke levenssfeer, is daarom zeker op zijn plaats. Dit onderzoek zou zich tot doel kunnen stellen welke beperkingen een zinvolle bijdrage leveren aan de te onderscheiden belangen van de burger, vanuit een visie op een fundamenteeler niveau over de gewenste machtsverdeling in de informatiemaatschappij tussen burgers, groeperingen, instellingen en de overheid. Met de resultaten van dit onderzoek zou vervolgens gereflecteerd kunnen worden op het bestaande juridische instrumentarium.

Literatuurlijst

Asscher & Koops 2004

L. Asscher B.-J.Koops, 'Een misstille revolutie in het strafrecht', Het Financieel Dagblad 1 april 2004, p. 10.

Asscher & Ekker 2003

L.F. Asscher & A.H. Ekker (redactie), met bijdragen van R. Hes, A.H. Ekker & B.J. Koops, *Verkeersgegevens: Een juridische en technische inventarisatie*, Amsterdam: Cramwinckel 2003.

Berkvens 2004

J.M.A. Berkvens, 'Van twee kanten - I. Ontvreemde privacy', *RMThemis* 2004-5, p. 267-269.

Blok 2001

P.H. Blok, 'De grondslagen van het privacyrecht herzien', *RM Themis* 2002-1, p. 17-26.

Blok 2002

P.H. Blok, *Het recht op privacy: Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, proefschrift, Boom Juridische Uitgevers 2002.

Bowman 2001

C.H. Bowman, 'The warrant requirement', *Georgetown Law Journal* (89) 2001, p. 1068-1084.

Buruma 2000

Y. Buruma, 'Particuliere opsporing', *Ars Aequi* (49) 2000-2, P. 117-121.

Buruma 2004

Y. Buruma, 'Acht nieuwe wetten : de zin en onzin van gegevens-bescherming', *Delikt en Delinkwent* (34) 2004-7, p. 665-675.

Cleiren & Nijboer 2003

C.P.M. Cleiren, J.F. Nijboer (red.), *Tekst & Commentaar: Strafvordering*, Deventer: Kluwer 2003.

Commissie Koopmans 1974

Commissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties, *Interim-rapport*, 's-Gravenhage: Staatsuitgeverij 1974.

Commissie Mevis 2001

Commissie Strafvorderlijke gegevensvergarig in de informatiemaatschappij, *Gegevensvergarig in strafvordering, Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*, Den Haag, 2001.

Corstens 2005

G.J.M. Corstens, *Het Nederlands strafprocesrecht*, Deventer: Kluwer 2005.

Dash 2004

S. Dash, *The intruders*, New brunswick, New Jersey and London: Rutgers University Press, 2004.

Dempsey & Flint 2004

J.X. Dempsey & L.M. Flint, 'Commercial data and national security', *George Washington Law Review* (72) 2004-6, p. 1459-1502.

Dommering 2000

E.J. Dommering (red.), met bijdragen van L. Asscher e.a., eindredactie door N. Sitompoel, *Informatierecht. Fundamentele rechten voor de informatiemaatschappij*, Amsterdam: Cramwinckel 2000.

Dommering 2001

E.J. Dommering, 'Het ongebreideld verzamelen van gegevens: de voorstellen van de commissie Mevis', *Netkwesties*, 1 november 2001.

Dressler 2002

J. Dressler, *Understanding criminal procedure*, Newark, San Fransisco: LexisNexis 2002.

Electronic Pivacy Information Center EPIC

<http://www.epic.org/privacy>

Ferdico 1993

J. N. Ferdico, *Criminal procedure for the criminal justice professional*, 5th edition, West Publishing Company, 1993.

Fijnaut 1994

C. Fijnaut, *De normering van het informatieve onderzoek in constitutioneel perspectief*, Preadvies uitgebracht voor de Nederlandse Vereniging voor Rechtsvergelijking, no. 49, Deventer: Kluwer 1994.

Franken 2003

H. Franken (ed.), *Zeven essays over informatietechnologie en recht*, Den Haag: Sdu Uitgevers, 2003.

Garfinkel 2000

S. Garfinkel, *Database nation: death of privacy in the 21st century*, O'Reilly, 2000.

Mac Gillavry 2001

E.C. Mac Gillavry, 'De voorstellen van de Commissie-Mevis - dwangmiddelen voor de informatiemaatschappij', NJB (76) 2001-30, p. 1411-1418.

Mac Gillavry 2002

E.C. Mac Gillavry, 'Gegevensvergaring in de informatiemaatschappij: een strafvorderlijke informatieplicht?', *I. de informatieplicht van de Commissie Mevis*, RM Themis 2002-1, p. 27-30.

Mac Gillavry 2004

E.C. Mac Gillavry, *Met wil en dank, Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven*, proefschrift, Wolf Legal Publishers 2004.

Van Grinsven 2004

M.P.J.M. van Grinsven, 'Grenzen aan gegevensvertrekking, reactie op de voorstellen van de commissie Mevis', www.gegeven.nl, 2004.

Heffernan 2001

C.M. Heffernan, 'Criminal law: Fourth amendment privacy interests', *The Journal of Criminal Law and Criminology* (82) 2001-1, p. 1-126.

Holvast Merkus & Michels 2004

J. Holvast, S. Merkus & G. Michels, 'De staat van de privacybescherming van de burger', *Privacy & Informatie* 2004-6, p. 242-249.

Hoofnagle 2004

C.J. Hoofnagle, 'Big brothers little helpers: How Choicepoint and other commercial databrokers collect, process and package your data for law enforcement', *29 N.C.J Int'l L. & Com. Reg.* 595, 2004.

Hustinx 2004

P.J. Hustinx, 'Van twee kanten – II. Bescherming van persoonsgegevens op koers', *RMThemis* 2004-5, p. 270-272.

Israel & LaFave 1993

J.H. Israel, W.R. LaFave, *Criminal procedure: constitutional limitations, in a nutshell*, Fifth edition, St. Paul, Minn.: West Publishing Co. 1993.

Jongeneel-van Amerongen 2005

M. Jongeneel-van Amerongen, 'Wet bevoegdheden vorderen gegevens', *Ars Aequi* (54), 2005-11, p. 954-961.

Kaplan, Skolnick & Feeley 1991

J. Kaplan, J.H. Skolnick & M.M. Feeley, *Criminal Justice: Introductory cases and materials*, fifth edition, Westbury, New York, The foundation press, 1991.

Kerr 2004

O.S. Kerr, 'The Fourth Amendment and new technologies: constitutional myths and the case for caution' *Michigan Law Review* (102) 2004. p. 801-888.

Kerr 2005

O.S. Kerr, 'Congress, the courts, and new technologies: a response to professor Solove', *Fordham Law Review* (74) 2205, p. 779-790.

Koops 2000

B.-J. Koops, *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?*, Deventer: Kluwer 2000.

Koops & Vedder 2001

B.-J. Koops & A. Vedder, *Opsporing versus privacy: de beleving van burgers*, Deventer: Sdu Uitgevers, 2001.

Kuitenbrouwer 2003

F. Kuitenbrouwer, 'Moderne inquisitie', reactie op de voorstellen van de Commissie Mevis, 2003.

LaFave 1996

W.R. LaFave, *A treatise on the Fourth Amendment*, Third edition, St. Paul, Minn.: West Publishing Co. 1996, actueel gehouden met Pocketpart, 2004.

Lodder Oskamp & Duker 2000

A.R. Lodder, A. Oskamp & M.J.A. Duker, *Informatietechnologische ondersteuning binnen het strafprocesrecht*, Den Haag: Sdu Uitgevers, 2000.

Mevis 2002

P.A.M. Mevis, 'Gegevensvergaring in de informatiemaatschappij: een strafvorderlijke informatieplicht?', *II Gegevensvergaring is iets anders dan een informatieplicht.*, RM Themis 2002-1, p. 30-35.

Meuwissen 1984

D.H.M. Meuwissen, *Grondrechten*, Utrecht/Antwerpen: Het Spectrum, 1984.

Nabben & Van de Luytgaarden 1996

P.F.B. Nabben & H.J.L.M. van de Luytgaarden, *De ultieme vrijheid: een rechtstheoretische analyse van het recht op privacy*, Deventer: Kluwer, 1996.

Nieuwenhuis 2001

A.J. Nieuwenhuis, *Tussen privacy en persoonlijkheidsrecht: een grondrechtelijk en rechtsvergelijkend onderzoek*, Nijmegen: Ars Aequi Libri, 2001.

Nijboer 2005

J.F. Nijboer, *Comparative criminal law & procedure, an introduction*, Deventer: Kluwer, 2005.

Overkleeft-Verburg 2005

G. Overkleeft-Verburg, 'Privacy en gegevensbescherming in de Europese Constitutie', *Privacy & Informatie* 2005-2, p. 50-56.

Pot-Donner 2001

Van der Pot – Donner, *Handboek van het Nederlandse Staatsrecht*, Deventer: W.E.J. Tjeenk Willink 2001.

Prins 2004

J.E.J. Prins, 'Vooraf - De stilzwijgend uitdijende opsporingsvergaarbak', *NJB* (79) 2004-16, p. 823.

Privacy international,

PHR2004-The United States of America, 16 november 2004, <http://www.privacy.org/pi>, last seen on 8 november 2005.

Raul 2002

A.C. Raul, *Privacy and the digital state: balancing public information and personal privacy*, Boston, Dordrecht, London: Kluwer academic publishers, 2002.

Rigaux 1990

F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles : Bruylant 1990.

Rhoden 2002

C. Rhoden, 'Challenging Searches and Seizures of Computers at Home or in the Office: From a Reasonable Expectation of Privacy to Fruit of the Poisonous Tree and Beyond', *American Journal of Criminal Law* (30) 2002, p. 107-135.

Schreuders 2001

Eric Schreuders, *Data mining, de toetsing van beslisregels & privacy. Een juridische Odyssee naar een procedure om het toepassen van beslisregels te kunnen toetsen*, Den Haag: Sdu Uitgevers, 2001.

Schwartz & Reidenberg 1996

P.M. Schwartz & J.L. Reidenberg, *Data privacy law: A study of United States data protection*, Charlottesville, Virginia: Michie Law publishers,

Slobogin 2005

C. Slobogin, 'Subpoenas and privacy', *DePaul Law Review* (54) 2005, p. 805-845.

Solove 2001

D.J. Solove, 'Privacy and power: computer databases and metaphors for information privacy', *Stanford Law Review* (53) 2001, p. 1393-1463.

Solove 2002a

D.J. Solove, 'Digital dossiers and the dissipation of Fourth Amendment privacy', *Southern Californian Law Review* 75, 2002, p. 1083-1168.

Solove 2002b

D.J. Solove, 'Access and aggregation: public records privacy and the constitution', *Minnesota Law Review* (86) 2002, p. 1137-1218.

Solove 2004

D.J. Solove, *The digital person: technology and privacy in the information age*, New York and London: NYU Press, 2004

Solove 2005

D.J. Solove, 'Fourth Amendment codification and professor Kerr's misguided call for judicial deference', *Fordham Law Review* (74) 2005, p. 747-777.

Stevens, Koops & Wiemans 2004

L. Stevens, B.J. Koops & P. Wiemans, 'Een strafvorderlijke gegevensvergaring nieuwe stijl', *NJB* (79) 2004-32, p. 1680-1686.

Van Stratum 2000

M.van Stratum, 'Privacy en opsporing II', *NJB* (75) 2000-43, p. 2087-2088.

Trechsel 2005

S. Trechsel, *Human rights in criminal proceedings*, Academy of European law of the European University Institute, Oxford University Press, 2005.

Weiss 2004

C. Weiss, 'the coming technology of knowledge discovery: a final blow to privacy protection', *Journal of Law Technology & Policy* 2004-2, p. 253-281.