De Wet Vorderen Gegevens Telecommunicatie

Spanningsveld tussen opsporing en privacy

Auteur: Jean C.L.M.A.J. van Gemert
(ANR 44.22.32)

Scriptie in de strafrechtswetenschappen
Te verdedigen tegenover de Examencommissie
van de Faculteit der Rechtsgeleerdheid van de Universiteit van Tilburg
(mr. F.P.E. Wiemans, mr. J.B.H.M. Simmelink)
op

25 november 2004, om 16:00 uur

Inhoudsopgave

Voorwoord

Toen ik in 1996 een begin maakte met de opleiding technische natuurkunde had ik niet kunnen voorzien dat ik uiteindelijk niet als ingenieur, maar als jurist zou afstuderen. Het kiezen van een totaal andere richting en studieomgeving was geen gemakkelijke stap. Niet alleen omdat je een vertrouwde sfeer verlaat, maar ook omdat het opnieuw starten van een opleiding een enorme inzet van je vergt, wetende wat nog voor je ligt. Spijt van die wisseling heb ik absoluut nooit gehad, en met plezier kijk ik dan ook terug op de vier jaar en een kleine drie maanden die ik in Tilburg heb doorgebracht.

Hierbij wil ik mijn familie, in het bijzonder mijn grootvader Leo, en vrienden bedanken voor alle steun en vertrouwen. Daarnaast ben ik mr. Paul Wiemans uiteraard erkentelijk voor zijn begeleiding bij het schrijven van deze scriptie.

Eindhoven, november 2004

Jean van Gemert

Lijst van afkortingen

CBP	College Bescherming Persoonsgegevens
CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees verdrag voor de rechten van de mens
DPA 1998	Data Protection Act 1998
GW	Grondwet
ISP	Internet Service Provider
IP-adres	Internet Protocol adres
MvA	memorie van antwoord
MvT	memorie van toelichting
OvJ	officier van justitie
RIPA 2000	Regulations of Investigatory Powers Act 2000
Sv	Wetboek van Strafvordering
Sr	Wetboek van Strafrecht
Tw	Telecommunicatiewet
URL	Uniform Resource Locator
Wbp	Wet bescherming persoonsgegevens

Hoofdstuk 1. Opzet van de scriptie

1.1. Inleiding

Met de opkomst van de informatiemaatschappij laat de juridisering van allerlei belangen in de digitale omgeving haar sporen achter in de Nederlandse wetgeving, ook het strafrecht is hierbij in belangrijke mate niet onberoerd gebleven. Het belang van (digitale) gegevens die relevant kunnen zijn bij de opsporing van strafbare feiten is evident, maar hoe kan deze gegevensverstrekking nu het beste vorm worden gegeven en welke waarborgen staan hier tegenover?

Onder het oude recht waren de mogelijkheden voor wat betreft het vorderen van gegevens in zekere mate beperkt en zouden ze niet tegemoet komen aan de werkelijke behoefte aan gegevens die in de praktijk bestaat.[1] Deze situatie, voor de inwerkingtreding van het wetsvoorstel vorderen gegevens telecommunicatie, werd dan ook voor een belangrijk deel gekenschetst door een systeem van vrijwilligheid; men verschafte veelal gegevens op vrijwillige basis aan justitie indien men dit verantwoord achtte in de gegeven situatie.

1.2. Nieuwe strafvorderlijke bevoegdheden

De wet 'vorderen gegevens telecommunicatie' is tamelijk ingrijpend en ziet erop toe dat het voor justitie een stuk eenvoudiger is geworden om toegang te verkrijgen tot allerlei communicatiegegevens. Niet alleen zijn er nieuwe bevoegdheden gecreëerd voor de officier van justitie, maar ook de opsporingsambtenaar heeft nu de mogelijkheid om bepaalde identificerende gegevens op te vragen. Zelfs gegevens van niet verdachten kunnen worden gevorderd. Een machtiging voor dit alles van de rechter-commissaris is niet nodig, tevens blijft de notificatieplicht onder omstandigheden achterwege.

1.3. Probleemstelling

In deze scriptie staan deze nieuwe strafvorderlijke bevoegdheden die dienen tot het vorderen van telecommunicatiegegevens en gebruikersgegevens in het middelpunt. De concrete uitwerking van deze bevoegdheden zal worden getoetst op hun juridische consistentie en praktische handhaafbaarheid. Met name het EVRM zal bij deze beschouwing een belangrijke rol spelen. Het kernprobleem kan hierbij worden opgedeeld in twee deelvragen: Is het kennisnemen van verkeersgegevens per definitie minder ingrijpend dan van het kennisnemen van de inhoud van communicatie, en wat voor passend beschermingsregime kan hiermee samengaan? Hierbij zal tevens worden gekeken naar enkele van de randvoorwaarden waaronder verkeersgegevens en gebruikersgegevens kunnen worden opgevraagd. Bij deze analyse zal rekening worden gehouden met de belangen die gemoeid zijn met strafvordering, maar ook met de privacybelangen van het individu. Tussen beiden dient zowel een juridisch als maatschappelijk acceptabel evenwicht te bestaan.

De opzet van deze scriptie is als volgt. In het tweede hoofdstuk staat het begrip verkeersgegevens en hoe deze voorheen werden verkregen centraal. Ook wordt in dit kader een overzicht gegeven van de bevindingen van de commissie Mevis voor wat betreft het vorderen van gegevens in zijn algemeenheid. In het derde hoofdstuk komt de wet vorderen gegevens telecommunicatie zelf aan bod. Hierbij worden de meest belangrijke wijzigingen en vernieuwingen doorsproken die de wet met zich meebrengt. De nadruk zal hierbij voornamelijk liggen op het hoe en waarom vanuit het gezichtspunt van het kabinet. Het vierde hoofdstuk bevat een rechtsvergelijkend overzicht van de meest recente opsporingsbevoegdheden van politie in het Verenigd Koninkrijk die aldaar het vorderen van telecommunicatiegegevens mogelijk maken. Hoofdstuk 5 bevat een algemene beschouwing van de argumenten en uitgangspunten van het kabinet, en punten van kritiek op de nieuwe regeling alsmede de conclusies.

Hoofdstuk 2. Communicatiegegevens en gegevensvergaring

2.1. Inleiding

Bij het gebruik van communicatiediensten ontstaan enorme hoeveelheden aan gegevens die door communicatieaanbieders worden geregistreerd en verwerkt. Deze 'verkeersgegevens' staan in deze scriptie centraal. Wat maakt een gegeven nu specifiek tot een verkeersgegeven? Men zou verkeersgegevens kunnen omschrijven als die elementen bij een communicatieproces die wat zeggen over het verloop van de communicatie. Om het begripskader wat nader te omlijnen werpen we een blik op enkele reeds bestaande definities, waarbij in dit verband het Besluit vorderen gegevens telecommunicatie in hoofdstuk 3 aan de orde zal komen.

2.2. Verkeersgegevens

Het begrip verkeersgegevens maakte haar eerste opwachting in de Europese ISDN richtlijn. Deze richtlijn geeft niet echt een eenduidige definitie. Uit artikel 6 lid 1 valt op te maken dat het zou moeten gaan om a) gegevens met betrekking tot abonnees en gebruikers welke b) worden verwerkt om oproepen tot stand te brengen en c) die worden opgeslagen door degene die een openbaar telecommunicatienetwerk en/of een algemeen beschikbare telecommunicatiedienst verzorgt.[2] Deze definitie omvat dus niet alle verkeersgegevens, maar alleen gegevens die worden opgeslagen.

De richtlijn privacy en elektronische communicatie geeft een techniekonafhankelijke definitie. Bij verkeersgegevens gaat het om "gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering daarvan".[3] De richtlijn geeft hierbij ook enkele voorbeelden, zoals de routering, de duur van een gesprek, tijdstip, het gebruikte protocol, etc.[4]

Het Cybercrime verdrag beperkt de definitie tot alleen computergegevens: "alle computergegevens die verband houden met communicatie door middel van een

computersysteem, voortgebracht door een computersysteem dat onderdeel vormde in de keten van communicatie, die de herkomst van de communicatie, de bestemming, de route, de tijd, de datum, de grootte, de duur of het type van de onderliggende dienst aangeven".[5]

Ekker meent dat de richtlijn betreffende privacy en elektronische communicatie het helderste is qua definitie en voor de praktijk het meest van belang zal zijn gezien dat de richtlijn het uitgangspunt vormt voor nationale wetgeving. Bepaalde elementen die alleen in het Cybercrime verdrag voorkomen, zoals de "herkomst" en "bestemming" van communicatie, zouden zonder veel problemen kunnen worden ondergebracht bij enkele algemenere begrippen die in de richtlijn worden genoemd. De opsomming in de richtlijn is tevens niet limitatief.[6]

2.3. Privacy bescherming op nationaal en internationaal niveau

Verkeersgegevens zijn privacygevoelig. Wanneer zij gekoppeld kunnen worden aan een persoon of aan andere gegevens wordt het mogelijk om (tot op zeker niveau) inzicht te krijgen in het handelen en wandelen van een persoon. Een inbreuk op iemands privacy is niet zonder meer toegestaan, zo beschermt artikel 10 GW de persoonlijke levenssfeer. Verkeersgegevens worden hiermee beschermd voor zover het persoonsgegevens betreffen.[7] Voor het moment lijkt men verkeersgegevens niet onder te brengen bij het brief-, telefoon- en telegraafgeheim van artikel 13 GW.

Op internationaal vlak speelt het EVRM een gewichtige rol. Artikel 8 van het verdrag biedt bescherming voor een ieder zijn "privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie". Lid 2 van artikel 8 geeft een aantal eisen waaraan een gerechtvaardigde inbreuk op dit privacyrecht moet voldoen. Het gaat hierbij voornamelijk om de kenbaarheid en voorzienbaarheid in de zin van rechtszekerheid en het feit dat een inbreuk noodzakelijk moet zijn in een democratische samenleving.[8] Dit noodzakelijkheidsbeginsel eist een dringende noodzaak en het in acht nemen van proportionaliteit en subsidiariteit. Verder geeft lid 2 een aantal doelen (zoals het voorkomen van strafbare feiten) waarmee een inbreuk op artikel 8 kan worden gerechtvaardigd. Bij de invulling hiervan behouden de lidstaten een eigen beleidsvrijheid, onder toezicht van het EHRM.[9]

2.4. Gegevensvergaring en strafvordering

Het bemachtigen van gegevens speelt een belangrijke rol bij het strafrechtelijk opsporingsonderzoek. In zijn algemeenheid kan in dit kader een onderscheid worden gemaakt tussen vrijwillige medewerking enerzijds, en de verplichte medewerking (naar aanleiding van strafvorderlijke dwangmiddelen) anderzijds. De algemene opsporingsbevoegdheid van opsporingsambtenaren vindt men in artikel 141 Sv. De reikwijdte van deze algemene opsporingsbevoegdheid wordt begrenst in het geval dat er sprake is van een inbreuk op een grondrecht. Er dient dan immers een specifieke wettelijke basis voorhanden te zijn die een dergelijke inbreuk legitimeert.[10] Een inbreuk moet niet al te snel worden aangenomen, zo is volgens het EHRM een niet-stelselmatige observatie niet aan te merken als een inbreuk op de privacy.[11] Het

systeem is dus dat opsporingsambtenaren naast de strafvorderlijke bevoegdheden die hen ter beschikking staan in beginsel ook gebruik kunnen maken van de vrijwillige medewerking van anderen ten behoeve van de opsporing. Alleen indien een grondrecht in het geding komt ligt dit anders.[12]

De voornaamste beperkingen voor derden aan het vrijwillig medewerken vindt men onder meer in de privacywetgeving. Het betreft hier de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet voor bedrijven in het bijzonder. Beiden zullen kort in de volgende paragrafen worden besproken.

2.4.1. De Wet bescherming persoonsgegevens

De Wbp richt zich op de verwerking van verkeersgegevens voor zover het gaat om persoonsgegevens. Verwerking is alleen mogelijk indien een van de mogelijkheden van artikel 8 Wbp van toepassing is. Het begrip persoonsgegevens is een ruim begrip, "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon".[13] Rechtspersonen vallen dus niet onder deze definitie.

De essentie van de Wbp vindt men in de bepalingen 7, 8, 9 en 43. Hierbij gaat het om nadere regels omtrent het verzamelen en het verwerken van persoonsgegevens. Met name artikel 8 sub f Wbp is van belang en maakt de verwerking van gegevens mogelijk indien dit noodzakelijk is voor "de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt". De "noodzakelijkheid" wordt ingekleurd middels een proportionaliteit- en subsidiariteittoets. Het belang van de persoon van wie gegevens worden verwerkt legt een "zelfstandig gewicht in de schaal" en moet worden meegenomen in een concrete afweging.[14]

Voor wat betreft de afgifte van persoonsgegevens staat artikel 43 toe dat een aantal bepalingen van de Wbp buiten toepassing kunnen worden gelaten. Daarbij gaat het om het vereiste van verenigbaarheid (art. 9 lid 1 Wbp), de informatieplichten (artikelen 30 lid 3, 33 en 34 Wbp) en het recht van de betrokkene op kennisneming (artikel 35 Wbp). Artikel 43 Wbp kan worden gebruikt indien het buiten toepassing laten van deze bepalingen noodzakelijk is voor onder meer de opsporing en vervolging van strafbare feiten. Voor het verlenen van medewerking aan opsporing zal de grondslag dus moeten worden gevonden in artikel 8 sub f in samenhang met artikel 43 Wbp. Van belang is het hierbij om te beseffen dat de verantwoordelijke zelf de beslissing maakt om artikel 43 Wbp al dan niet toe te passen.

De grondslag in artikel 43 sub b Wbp, het voorkomen, vervolgen en opsporen van strafbare feiten, moet beperkt worden uitgelegd en is alleen van toepassing in "uitzonderlijke en spoedeisende gevallen".[15] Artikel 43 is dus een uitzonderingsbepaling die geen basis vormt voor een systematische gegevensverstrekking. Of dit in de praktijk ook zo blijkt uit te vallen is nog maar de vraag.[16]

Resumerend kan het volgende worden geconcludeerd. Niet alleen is de

verantwoordelijke voor de persoonsgegevens diegene die de uiteindelijke afweging maakt tussen de in het geding zijnde belangen, maar hij bepaalt tevens zelf - ook als de dringende noodzakelijkheid voor het opsporen en vervolgen van strafbare feiten evident is - of hij zal overgaan tot afgifte van persoonsgegevens. De betrokkene komt in zo´n situatie er karig vanaf. Gezien de mogelijkheid die de Wbp biedt tot het opzij zetten van de informatieplichten zal men in de loop van een strafprocedure zich pas bewust worden van het feit dat er persoonsgegevens zijn verstrekt.

2.4.2. De Telecommunicatiewet

De Telecommunicatiewet (Tw) stelt regels voor de openbare aanbieders van telecommunicatiewerken en diensten. Ook de Internet Service Provider (ISP) valt onder dit begrip. Artikel 11.2 Tw omvat een algemene zorgplicht, de aanbieder dient zorg te dragen voor een adequate bescherming van de "persoonsgegevens en de bescherming van de persoonlijke levenssfeer die uit de nationale en de internationale privacyregelgeving voortvloeien".[17] Ook vinden we enkele nadere regels in artikel 11.5 Tw omtrent de opslag van verkeersgegevens. Dit betreft dwingend recht waarvan niet kan worden afgeweken, zelfs niet door de abonnee.[18] De essentie van deze bepaling is dat de aanbieder zo spoedig mogelijk de gegevens dient te verwijderen of in ieder geval te anonimiseren. Op deze plicht tot anonimiseren zijn een aantal uitzonderingen opgenomen in lid 2 van art. 11.5 Tw, deze mogelijkheden (zoals het opsporen van fraude, of marktonderzoek) liggen echter allemaal in het verlengde van een normale bedrijfsvoering. Voor verder gebruik van deze gegevens moet voldaan zijn aan de eisen die de Wbp daar aan stelt.[19]

Het bovenstaande betekent dat ongeanonimiseerde gegevens alleen beschikbaar zijn wanneer zij onder een van de uitzonderingen van 11.5 lid 2 Tw te brengen zijn. Over andere gegevens dan deze kan de opsporingsambtenaar dan ook niet beschikken. Een aanbieder kan niet buiten dit vaste kader treden, ook als een opsporingsambtenaar daar om zou verzoeken.

2.5. Het vorderen van verkeersgegevens onder oud recht: 126n en 126u Sv

Voor wat betreft het vorderen van verkeersgegevens waren voorheen de artikelen 126n en 126u Sv de meest relevante bepalingen. Op grond van 126n Sv kon de officier van justitie in het belang van het onderzoek een vordering instellen voor het verkrijgen van inlichtingen omtrent al het verkeer dat had plaatsgevonden over een openbaar telecommunicatienetwerk. Vereiste hierbij was wel dat het vermoeden moest bestaan dat de verdachte had deelgenomen aan dat verkeer, tevens moest er sprake zijn van ontdekking op heterdaad dan wel een artikel 67-lid-1 Sv misdrijf of een misdrijf als bedoeld in artikel 138a Sr (hacking). De vordering kon worden gericht tot een ieder die werkzaam was bij een aanbieder.[20] De gegevens die middels artikel 126u Sv konden worden gevorderd waren dezelfde, maar deze bepaling richtte zich op het in georganiseerd verband beramen of plegen van misdrijven.[21]

2.6. De Commissie Mevis

De minister van justitie heeft in maart 2000 de Commissie Strafvorderlijke Gegevensvergaring ingesteld.[22] Deze Commissie Mevis (genoemd naar haar voorzitter) had als taak onderzoek te doen naar een aantal uitgangspunten als basis voor wetgeving ten aanzien van de strafvorderlijke gegevensvergaring in de informatiemaatschappij.[23] De commissie maakt in haar rapport onderscheid tussen het strafvorderlijke belang, het belang van diegene op wie de gegevens betrekking hebben en het belang van de verantwoordelijke van de gegevens.[24]

Een van de knelpunten die de Commissie constateert is het feit dat vrijwillige verstrekking op grond van de Wbp van de verantwoordelijke vraagt een zelfstandige afweging te maken, waarbij hij zich zal moeten afvragen of het opsporingsbelang dermate zwaar is dat verstrekking van gegevens is gerechtvaardigd. Niet verwonderlijk is dan ook de conclusie dat een dergelijke afweging voor de verantwoordelijke eigenlijk zo goed als niet te doen valt, dit vereist immers kennis van alle feiten en omstandigheden en die informatie kan nu eenmaal niet vaak worden verstrekt door de opsporingsinstanties. Dat de verantwoordelijke een onjuiste belangenafweging maakt op basis van incomplete gegevens ligt dus binnen de mogelijkheden. Dit kan volgens de Commissie gevolgen hebben voor de aansprakelijkheid van de verantwoordelijke, alsmede de bruikbaarheid van het bewijs.[25] Daarnaast is de Commissie van mening dat het uitgangspunt van vrijwilligheid op de spreekwoordelijke schop moet, strafvordering moet niet afhankelijk zijn van de vrijwillige medewerking van een derde; als er dus noodzaak is om bepaalde gegevens in het belang van het onderzoek ter beschikking te krijgen dan moeten deze gegevens gewoon kunnen worden bemachtigd.[26]

2.7. De Mevis bevoegdheden

Ten aanzien van de bevoegdheden die te vinden zijn in het Wetboek van Strafvordering constateert men dat alleen “ten dele” wordt voorzien in mogelijkheden om die gegevens te vorderen waaraan in de praktijk behoefte bestaat. Zo heeft de opsporingsambtenaar bijvoorbeeld geen bevoegdheid tot het vorderen van toekomstige gegevens. Daarnaast zijn de bevoegdheden voor wat betreft het vorderen van telecommunicatiegegevens beperkt tot de aanbieders van openbare telecommunicatienetwerken en diensten.[27]

Verder ontbreken specifieke bevoegdheden die gericht zijn op het bewerken van gegevens.[28] Het bewerken van gegevens zal dus gebaseerd moeten zijn op vrijwillige medewerking, wat kan leiden tot een hinderlijk conflict tussen de plichten en belangen van de betrokken partijen.[29] De Commissie acht in ieder geval het belang van “data-mining” groot voor strafvorderlijke doeleinden en voegt daarbij toe dat het niet ongewoon is dat voor een dergelijke bewerking grote hoeveelheden gegevens noodzakelijk zijn. Hierbij kan ook het verwerken van gegevens van niet-verdachten een belangrijke rol spelen daar hiermee significante verschillen tevoorschijn kunnen komen tussen verdachten en niet-verdachten. Daarbij wordt aangestipt dat het verwerken van gegevens van niet-verdachten dan ook wel noodzaakt tot een “goede

regeling … voor het bewaren en vernietigen van die gegevens".[30]

Over de beschikbaarheid van gegevens meldt de Commissie dat de in de praktijk gehanteerde bewaartermijnen over het algemeen niet als bezwaarlijk worden ervaren voor strafvordering, de telecommunicatiesector vormt hierop echter een uitzondering. Bij digitale gegevens speelt voornamelijk de vluchtigheid, gegevens kunnen worden verwijderd met een simpele druk op de knop. Er is dan ook behoefte aan een mogelijkheid om gegevens snel te bevriezen om zo het strafvorderlijk onderzoek te vergemakkelijken. Wettelijke verplichtingen tot het bewaren van gegevens zijn er, behouden enkele uitzonderingen (zoals artikel 13.4 Tw), vooralsnog niet.

Op grond van onder meer het bovenstaande komt de Commissie tot de conclusie dat de huidige regelgeving te beperkend is; uitgebreidere bevoegdheden evenals de onafhankelijkheid van de vrijwillige medewerking van derden zijn noodzakelijk.[31] Hierbij moet de kanttekening worden geplaatst dat het beeld wat de commissie schetst van de praktijk wellicht niet geheel overeenkomt met werkelijkheid.[32]

De commissie biedt in haar rapport een nieuw bevoegdhedenstelsel als oplossing. De voorgestelde bevoegdheden bestaan in principe uit vier, naar privacy gerangschikte, varianten. Zo kan er sprake zijn van "identificerende gegevens", van "andere gegevens", van "toekomstige gegevens" en van "gevoelige gegevens". Deze zullen kort worden besproken.

Identificerende gegevens

Identificerende gegevens kunnen door elke opsporingsambtenaar worden gevorderd in geval van verdenking van een strafbaar feit, de vordering kan worden gericht tot "een ieder die tot de gegevens toegang zou kunnen hebben", uitgezonderd de verdachte en verschoningsgerechtigden.[33] Niet alleen de rechtspersoon, maar dus ook elke burger wordt daarmee binnen het bereik van deze medewerkingverplichting gebracht. De opsporingsambtenaar kan een derde verplichten om antwoord te geven op de vraag of men al dan niet gegevens over de desbetreffende persoon van onderzoek in bezit heeft. Deze bevoegdheid mag niet doelloos worden toegepast, doch is ook weer niet zo strikt dat er een "aannemelijk vermoeden" moet bestaan dat gegevens aanwezig zouden zijn.[34]

Andere gegevens

De officier van justitie kan in het geval van verdenking van een ernstig misdrijf een vordering instellen tot het verkrijgen van "andere gegevens".[35] De vordering kan alleen worden gericht tot diegenen waarvan in redelijke mate kan worden vermoed dat men toegang heeft tot deze (opgeslagen dan wel vastgelegde) gegevens. De verdachte of verschoningsgerechtigden zijn uitgezonderd. Verder kan de vordering betrekking hebben op alle denkbare gegevens.[36] Hieronder vallen ook de identificerende gegevens zoals bedoeld in het door de Commissie voorgestelde artikel 126nc.[37]

Toekomstige gegevens
In het belang van het onderzoek kan de officier van justitie vorderen dat men "toekomstige gegevens" verstrekt. Is de informatie "dringend" nodig in het belang van het onderzoek, dan kan de officier – met een schriftelijke machtiging van de rechter-commissaris - vorderen dat gegevens na verwerking "direct" worden verstrekt. Ook bij deze bevoegdheid gaat het om alle denkbare gegevens waarover de verantwoordelijke "technisch de beschikkingsmacht heeft".[38]

Gevoelige gegevens
Het vorderen van gevoelige gegevens gebeurt door de officier van justitie in het belang van het onderzoek en met machtiging van de rechter commissaris. Er dient sprake te zijn van een verdenking van een ernstig misdrijf dat een ernstige inbreuk op de rechtsorde oplevert. Bij "gevoelige gegevens" gaat het om die gegevens waarbij "verstrekking reeds vanwege hun aard een heel specifieke of indringende inbreuk kan maken op fundamentele vrijheden of op de persoonlijke levenssfeer", zoals gegevens "over iemands godsdienst, ras, politieke gezindheid, gezondheid of diens seksuele leven". Ook de gegevens die vallen onder het brief of telefoongeheim van artikel 13 Gw plaatst de Commissie onder dit begrip, waaronder ook e-mail.[39]

Het bewerken van gegevens
De officier van justitie kan vorderen, indien het belang van het onderzoek dit dringend eist en na schriftelijke machtiging van de rechter commissaris, dat bepaalde gegevens opgeslagen in een computer bewerkt worden en de resultaten van deze bewerking worden verstrekt. Ook hier moet er sprake zijn van verdenking van een ernstig misdrijf dat een ernstige inbreuk op de rechtsorde oplevert. De bewerking kan bestaan uit de reeds eerder genoemde datamining of registervergelijking, waarbij ook gegevens van niet-verdachten kunnen worden bewerkt.[40]

Het bewaren van gegevens
Een beperkte bevoegdheid tot het bevriezen van gegevens kan worden ingezet door de hulpofficier van justitie indien er sprake is van een ernstig misdrijf en dit misdrijf een ernstige inbreuk op de rechtsorde oplevert. Gegevens blijven zo voor een termijn van 14 dagen toegankelijk, waarbij de bevroren gegevens kunnen worden gevorderd door gebruik te maken van de andere vorderingsbevoegdheden. Ook hier geldt dat de verantwoordelijke de technische mogelijkheden moet hebben om de gegevens toegankelijk te houden, indien dit niet zo is hoeft men aan de vordering geen gevolg te geven.[41]

2.8. Reacties op de Mevis bevindingen

In het kabinetsstandpunt naar aanleiding van het rapport van de Commissie neemt men de positie in dat de geschetste bevoegdheden in grote lijnen kunnen worden overgenomen. Het kabinet benadrukt hierbij de behoefte en noodzakelijkheid om in beginsel alle soorten gegevens te kunnen vorderen gezien het belang hiervan bij de opsporing van ernstige misdrijven. Wel worden door het kabinet enkele beperkingen gesteld.

Een van de meest ingrijpende suggesties van het rapport is dat een vordering ook kan worden gericht tot de burger. Het kabinet is hierin terughoudender. Zo beperkt ze de voorgestelde bevoegdheden tot het vorderen van identificerende dan wel toekomstige gegevens tot "de houder van gegevens die anders dan ten behoeven van persoonlijk gebruik gegevens bewerkt".[42] Deze beperking is voor wat betreft het vorderen van identificerende gegevens blijkbaar niet absoluut, het kabinet stelt dat "identificerende gegevens die worden verwerkt ten behoeve van persoonlijk gebruik […] door de officier van justitie [kunnen worden] gevorderd".[43] Daarnaast is het kabinet net zoals de Commissie van mening dat de verantwoordelijkheid voor de gegevensvergaring bij de bevoegde instanties dient te liggen en niet bij de particuliere verantwoordelijken. De wetenschappelijke commissie van de Nederlandse Vereniging voor Rechtspraak komt het rapport en de voorgestelde dwangmiddelen juist te "ingrijpend" voor en zoekt een oplossing in het aanpassen van de Wbp.[44]

Inmiddels zijn de Mevis-bevoegdheden in grote lijnen overgenomen in het wetsvoorstel 'bevoegdheden vorderen gegevens' en de wet 'vorderen gegevens financiële sector'.[45]

Hoofdstuk 3. De wet bevoegdheden vorderen gegevens telecommunicatie[46]

3.1. Inleiding

Onder het oude recht kon justitie het vorderen van telecommunicatiegegevens primair baseren op twee grondslagen; de artikelen 126n Sv en 126u Sv. Artikel 126n Sv gaf de officier van justitie de mogelijkheid tot het verkrijgen van inlichtingen over verkeer dat plaats had gevonden over een openbaar telecommunicatienetwerk. Artikel 126u Sv betrof die gevallen waar in georganiseerd verband misdrijven worden beraamd of gepleegd. De wet vorderen gegevens telecommunicatie brengt een aantal belangrijke wijzigingen mee waarbij beiden artikelen op een aantal essentiële onderdelen zijn aangepast en een nadere bevoegdheidsverdeling tot stand komt.[47]

De motieven voor het invoeren van nieuwe bevoegdheden zijn niet nieuw, deze betreffen in hoofdlijnen de reeds in hoofdstuk twee besproken kritiek dat het verstrekken van gegevens veelal op vrijwillige basis plaatsvindt en de belangenafweging om tot verstrekking over te gaan niet ligt bij justitie maar bij de aanbieders zelf. Ook de mogelijke aansprakelijkheid van de houder die tot verstrekking overgaat baarde de minister zorgen.[48] Het ingenomen standpunt door het kabinet is dan ook dat de vrijwilligheid tot het verstrekken van gegevens komt te vervallen daar waar strafvorderlijke bevoegdheden kunnen worden toegepast.[49] Ook zou vrijwilligheid niet passen in een regeling die moest voldoen aan de eisen van artikel 10 GW en artikel 8 EVRM. De toegankelijkheid, voorzienbaarheid en waarborgen tegen willekeur zouden immers niet te garanderen zijn indien het verstrekken van gegevens in onderling overleg wordt bepaald.[50]

3.2. Het vorderen van verkeersgegevens: de artikelen 126n en 126u Sv

Het nieuwe artikel 126n Sv is beperkt tot die gevallen waarin sprake is van verdenking van een artikel-67-lid 1 misdrijf. De officier van justitie kan in zo'n geval, indien het belang van het onderzoek hiermee gediend is, verkeersgegevens vorderen van elke aanbieder van een "openbaar telecommunicatienetwerk" of "openbare telecommunicatiedienst". Indien het gaat om het beramen dan wel het plegen van misdrijven in georganiseerd verband in de zin van artikel 126o Sv, dan biedt artikel 126u Sv de officier van justitie vergelijkbare mogelijkheden.[51]

Met deze wijzigingen zoekt men naar een concretere afbakening van gegevens die door de opsporingsambtenaar kunnen worden gevorderd en een verfijnde verdeling van de bevoegdheden die kunnen worden toegepast. Volgens de minister lag het aanpassen van de bevoegdheden voor de hand omdat de oude bepalingen onduidelijkheden met zich meebrachten door de opkomst van allerlei nieuwe communicatietechnieken.[52]

Als uitgangspunt heeft men gekozen voor het begrip verkeersgegevens, dit begrip wordt omschreven als alle "gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker".[53] Middels een algemene maatregel van bestuur, thans het Besluit vorderen gegevens telecommunicatie, zijn de ontwikkelingen in de jurisprudentie tot op heden meegenomen.[54] Artikel 2 van het besluit biedt dan ook een nadere concretisering van het begrip wat aansluiting vindt bij de opmerkingen in de MvT .[55]

De memorie van toelichting maakt duidelijk dat het bij verkeersgegevens gaat om de "uiterlijke kenmerken van telecommunicatie en niet om de inhoud van hetgeen via het telecommunicatieverkeer wordt uitgewisseld".[56] Hierbij zijn een aantal voorbeelden gegeven. Ik noem onder meer de aansluitnummers, de gebruikte apparatuur, het tijdstip van aanvang, de duur van het verkeer, maar ook de vraag of er communicatie heeft plaatsgevonden. Met betrekking tot het internet gaat het om de betrokken e-mail adressen, de aanduiding (URL) van een website of een pagina binnen een website. De minister is hierbij nadrukkelijk van mening geweest dat het kennis nemen van de belangstellingssfeer van een gebruiker op zich niet gelijk kan worden gesteld met "het kennis nemen van [de inhoud van] de vertrouwelijke communicatie van de gebruiker".[57] De minister heeft echter nagelaten dit uitgangspunt hard te maken, op dit onbegrijpelijke standpunt wordt dan ook later nog ingegaan.

Verder zijn onder meer als voorbeeld genoemd de plaats waar de gebruiker van mobiele telecommunicatie zich bevindt (locatiegegevens), en het betalen van facturen. Met betrekking tot het vorderen van locatiegegevens wordt opgemerkt dat de bevoegdheid in principe hieraan niet in de weg staat, ook het vaststellen "met wie een persoon contacten onderhoudt of op welke plaats een persoon zich op een bepaald tijdstip bevond" kan een reden zijn voor het vorderen van verkeersgegevens. Locatiegegevens die betrekking hebben op het stand-by staan van een toestel zijn echter geen verkeersgegevens en kunnen niet worden gevorderd.[58] De nadere uitwerking in het Besluit vorderen gegevens telecommunicatie bevestigt dit.[59] Ook uit

een recent arrest van de Hoge Raad (weliswaar nog gewezen onder het oude 126n Sv) blijkt dat locatiegegevens van een GSM alleen te vorderen zijn onder de voorwaarde dat met de GSM "aan het telecommunicatieverkeer wordt deelgenomen".[60] Eveneens wordt opgemerkt dat de bevoegdheid eigenlijk niet is bedoeld voor een vorm van stelselmatige observatie, toch blijft het vorderen van verkeersgegevens de te gebruiken bevoegdheid ook al zou het voorzienbaar zijn dat dit tot een vorm van stelselmatige observatie zal leiden.[61] De reden hiervoor is dat de gegevens "immers uitsluitend verkregen [kunnen] worden door deze te vorderen van de telecommunicatieaanbieder, een handeling waartoe de bevoegdheid tot stelselmatige observatie (artikelen 126g en 126o) niet legitimeert". De officier van justitie dient volgens de minister dan maar te beoordelen of het in het belang van het onderzoek is om de gegevens op deze manier te vorderen, waarbij hij desnoods zijn vordering beperkt.[62] Als laatste is het nog relevant om te vermelden dat in de algemene maatregel van bestuur ook de naam-, adres- en woonplaatsgegevens (NAW-gegevens) zijn aangemerkt als verkeersgegevens.[63]

Voor het vorderen van inlichtingen telecommunicatie onder oud recht op grond van 126n Sv was het noodzakelijk dat de vordering betrekking had op telecommunicatie waar de verdachte aan had deelgenomen. Of, voor wat betreft het oude artikel 126u Sv, dat aan het verkeer een persoon had deelgenomen waarvan men redelijk kon vermoeden dat hij betrokken was bij het beramen of plegen van misdrijven in georganiseerd verband. Dit vermoeden, dat een verdachte aan telecommunicatie moet hebben deelgenomen, is vervallen. Deze wijziging vindt plaats in het kader dat een ruimere bevoegdheid volgens de minister bij zou dragen aan een effectievere opsporing. Daarnaast kent de meer ingrijpende telecommunicatie tapbevoegdheid een dergelijke beperking ook niet, het zou dan ook volgens de minister niet in verhouding staan om hier wel een dergelijke beperking te handhaven.[64]

Het oude artikel 126n Sv gaf drie situaties waarbinnen verkeersgegevens kunnen worden gevorderd. Het betrof hier de ontdekking op heterdaad, de verdenking van een artikel-67-lid-1 misdrijf, of het misdrijf computervredebreuk van artikel 138a Sr. De ontdekking op heterdaad evenals de verdenking van het misdrijf van 138a Sr zijn aldus als grondslag voor een vordering komen te vervallen, met als reden dat deze twee gronden in de praktijk zelfstandig niets bleken toe te voegen.[65] Voor wat betreft de opsporing van eenvoudige hacking van 138a Sr valt deze keuze niet te begrijpen, gezien de hogere drempel zullen immers verkeersgegevens hier niet meer te vorderen zijn en juist die gegevens zijn bij hacking onmisbaar bij de opsporing! Hoe dan ook, de gronden die worden genoemd in de nieuwe bevoegdheden zijn terug te brengen tot de tweenavolgende mogelijkheden, te weten: de verdenking van een artikel-67-lid-1 misdrijf, of een artikel-67-lid-1 misdrijf dat in georganiseerd verband wordt beraamd of gepleegd en - eventueel in samenhang met andere misdrijven - een ernstige inbreuk op de rechtsorde oplevert.[66]

Tevens is een duidelijk onderscheid geïntroduceerd tussen reeds bestaande gegevens en toekomstige gegevens.[67] Het vorderen van toekomstige gegevens is beperkt in duur, namelijk voor ten hoogste drie maanden. Bij het beëindigen, verlengen, wijzigen of aanvullen van de vordering dient de officier van justitie daarnaast ook proces-

verbaal op te maken.[68] Het vorderen van toekomstige gegevens was al mogelijk onder de oude regeling, maar deze bevoegdheid werd niet uitdrukkelijk in de wet genoemd. Met het expliciet opnemen hiervan in de wet wordt deze bevoegdheid nu dan ook nadrukkelijk vastgelegd.[69] Wat moet nu worden verstaan onder toekomstige gegevens? De minister kent dit begrip een grotere omvang toe dan de reeds vastgelegde gegevens; het gaat om gegevens die een aanbieder op "enig moment voorhanden heeft", ook gegevens die normaliter niet in het kader van de bedrijfsvoering worden opgeslagen maar wel voorhanden zijn kunnen dus onderwerp zijn van de vordering.[70] Dit betekent dat een registratieplicht niet bestaat voor gegevens die een aanbieder wel kan registreren maar dit niet doet, de gegevens zijn dan immers ook niet voorhanden. In dit kader merkt de minister dan ook op dat "in beginsel aan aanbieders van telecommunicatie geen verplichtingen worden opgelegd gegevens op te slaan uitsluitend en alleen ter wille van de strafvordering".[71]

Voor wat betreft de manier waarop gegevens worden gevorderd moet een onderscheid worden gemaakt tussen verkeersgegevens die tevens NAW-gegevens zijn, en andere verkeersgegevens. Op de eerste categorie van gegevens, verkeersgegevens die zowel NAW-gegevens zijn, is het Besluit verstrekking gegevens telecommunicatie (CIOT-besluit) van toepassing, hierover zo meer.[72] Voor het vorderen van alle overige verkeersgegevens zijn volgens de minister reeds toereikende procedures en modellen voorhanden die naar zijn inzicht vooralsnog niet hoeven worden aangepast.[73]

Van het doen van een vordering verkeersgegevens dient proces-verbaal te worden opgemaakt door de officier van justitie. Middels een nota van wijziging zal in deze formulering van art. 126n/u een wijziging worden aangebracht, de regel wordt dat de OvJ het "proces-verbaal doet opmaken".[74] Volgens de toelichting wordt daarmee aansluiting gezocht bij de praktijk daar het gebruikelijk is dat processen-verbaal van de toepassing van opsporingsbevoegdheden worden opgemaakt door de opsporingsambtenaar. In het proces-verbaal moet worden vastgelegd het misdrijf, de naam van de verdachte indien bekend (of een zo nauwkeurig mogelijke aanduiding van de persoon), de feiten of omstandigheden waaruit blijkt dat aan de voorwaarden voor de vordering is voldaan, welke gegevens gevorderd worden, en in het geval van een vordering toekomstige gegevens de periode waarover de vordering zich uitstrekt.[75] Bij het vorderen van toekomstige gegevens dient ook bij wijziging, aanvulling, verlenging of beëindiging van de vordering proces-verbaal te worden opgemaakt.[76]

Op de vraag of de persoon waartegen een strafvorderlijke bevoegdheid is toegepast ook hiervan in kennis dient te worden gesteld levert artikel 126bb Sv een antwoord. Dit artikel betreft een algemene notificatieplicht en verlangt dat een betrokkene in kennis wordt gesteld dat een bepaalde bevoegdheid jegens hem is uitgeoefend zodra het belang van het onderzoek dit toelaat. Op deze notificatieplicht wordt voor wat betreft het vorderen van verkeersgegevens geen uitzondering gemaakt.

3.3. Het vorderen van gebruikersgegevens: 126na, 126ua Sv

Strafvordering biedt thans twee nieuwe mogelijkheden, beiden laagdrempelig, waarmee het de opsporingsambtenaar mogelijk wordt gemaakt om gebruikersgegevens te vorderen. De bevoegdheid van 126na Sv komt toe aan iedere opsporingsambtenaar in geval van verdenking van een misdrijf en indien noodzakelijk voor het belang van het strafvorderlijk onderzoek.[77] De gegevens die kunnen worden gevorderd zijn limitatief bepaald in artikel 126na lid 1 Sv, het gaat hier om de naam, het adres, postcode, woonplaats, maar ook het (geheime) nummer en de vorm van dienstverlening van "een gebruiker van telecommunicatie".[78] De vordering kan zich richten tot elke aanbieder van een openbaar telecommunicatienetwerk of openbare telecommunicatiedienst. Artikel 126ua Sv biedt overeenkomstige mogelijkheden, maar ziet specifiek op een artikel 126o Sv situatie; het in georganiseerd verband beramen of plegen van misdrijven.

Het is de bedoeling dat beide nieuwe bevoegdheden een gedeeltelijke vervanging vormen voor artikel 13.4 lid 1 Telecommunicatiewet, voor zover het gaat om het opvragen van gebruikersgegevens. In dit artikel uit de Telecommunicatiewet is bepaald dat een aanbieder alleen gebruikersgegevens dient te verstrekken indien deze gegevens nodig zijn voor de opsporingsambtenaar om de aftapbevoegdheid of de bevoegdheid tot het vorderen van verkeersgegevens aan te wenden. Gezien het feit dat dit oogmerk geen vereiste meer vormt voor de toepassing van beide nieuwe bevoegdheden, bieden 126na en 126ua Sv veel ruimere mogelijkheden om gebruikersgegevens op te vragen als voorheen het geval was. Dit zou dan ook volgens de minister de opsporingsmogelijkheden ten goede komen.[79]

Een verdere verplichting voor de telecommunicatie aanbieder die tot op heden alleen te vinden was in artikel 13.4 lid 2 van de Telecommunicatiewet heeft ook zijn weg gevonden naar de artikelen 126na en 126ua Sv. Het gaat daarbij om de verplichting om gebruikersgegevens te achterhalen indien hem deze gegevens in eerste instantie niet bekend zijn. Deze vorderingsbevoegdheid is echter voorbehouden aan de officier van justitie en kan alleen worden toegepast indien de gebruikersgegevens noodzakelijk zijn voor het toepassen van de bevoegdheden tot het vorderen van verkeersgegevens, of het opnemen van telecommunicatie.[80] Hierbij zou het dan alleen moeten gaan om "de meest dringende gevallen waarin de gebruikersgegevens onmisbaar zijn" omdat anders deze bevoegdheden niet kunnen worden toegepast. Ook ten aanzien van bijvoorbeeld het prepaid telefoon abonnement bestaat de verplichting voor de aanbieder om achter gebruikersgegevens aan te gaan.[81]

Artikel 13.4 lid 2 Tw behoudt ook naast de bovenstaande nieuwe bevoegdheden een aanvullende werking, zo blijft de daaruit voortvloeiende verplichting voor aanbieders om gegevens na verwerking voor een periode voor drie maanden te bewaren bestaan zodat men aan hun informatieverplichtingen kan voldoen.[82]

De wijze waarop gebruikersgegevens zoals bedoeld in de artikelen 126na en 126ua worden gevorderd vindt plaats volgens de procedure zoals deze is omschreven in het Besluit verstrekking gegevens telecommunicatie. Deze procedure is zoals al reeds is

opgemerkt tevens van toepassing wanneer verkeersgegevens worden gevorderd die kunnen worden aangemerkt als gebruikersgegevens.

Gebruikersgegevens worden verkregen middels het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT).[83] De aanbieders van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst dienen continu geactualiseerde bestanden met gebruikersgegevens ter beschikking van het CIOT te stellen zodat het CIOT rechtstreeks de beschikking heeft over deze informatie.[84] Inhoudelijk gezien blijven deze bestanden beperkt tot die gegevens waarover de aanbieder in het kader van zijn normale bedrijfsvoering de beschikking heeft en die hij verplicht dient op te slaan.[85] De opsporingsambtenaar die van zijn vorderingsbevoegdheid gegeven in 126na of 126ua Sv gebruik maakt, zal voor het opvragen van gebruikersgegevens met zijn verzoek dan ook niet bij de aanbieder maar bij het CIOT moeten aankloppen waarna men de gevraagde gegevens zal trachten op te sporen in de door haar toegankelijke gegevensbestanden.

De Internet Service Provider (ISP) geniet in dit geheel vooralsnog een tijdelijke uitzonderingspositie, de ISP hoeft dan ook (nog) niet te voldoen aan de verplichting om gebruikersgegevens aan het CIOT beschikbaar te stellen.[86] Deze uitzonderingspositie die om praktische dan wel technische redenen in het leven is geroepen is echter beperkt tot twee jaar na inwerkingtreding van het besluit. Het is ook niet op voorhand uitgesloten dat internet aanbieders zich middels een convenant alsnog via het CIOT tot gegevensverstrekking verplichten.[87]

Een vordering op grond van artikel 126ua of artikel 126na Sv is gebonden aan bepaalde formele eisen, zo dient ook hier een proces-verbaal door de desbetreffende opsporingsambtenaar te worden opgemaakt. De inhoudelijke vereisten aan het proces-verbaal zijn nagenoeg gelijk aan de vereisten voor het proces-verbaal van artikel 126n en respectievelijk artikel 126u Sv. [88]

Waar het de notificatieplicht betreft ligt de situatie voor gebruikersgegevens anders dan bij verkeersgegevens. Toepassing van de algemene notificatieplicht van artikel 126bb Sv wanneer gebruikersgegevens zijn gevorderd is door de minister afgewezen, wat dan ook blijkt uit de in de wet opgenomen uitzonderingen.[89] Gezien de geringe betekenis van de gegevens, de afwezigheid van een vergelijkbare notificatieplicht onder het regime van de Wbp, en het enorm aantal verzoeken op jaarbasis zou notificatie van de betrokkenen volgens de minister niet opportuun zijn.[90] Evenwel moet hierbij niet uit het oog worden verloren dat indien gebruikersgegevens worden gevorderd middels de artikelen 126n dan wel 126u Sv, waarbij de gevorderde verkeersgegevens zijn aan te merken als gebruikersgegevens, er wel degelijk sprake is van een notificatieplicht.

De artikelen 126na en 126ua Sv bieden tevens de mogelijkheid tot het stellen van voorvragen, de opsporingsambtenaar kan aan een aanbieder dus de vraag voorleggen of men over gegevens van een bepaalde persoon beschikt. Deze mogelijkheid bestond niet onder het oude recht, een vordering kon immers alleen betrekking hebben op het "verkeer" over een communicatienetwerk. Voorvragen zullen nu juist specifiek

betrekking hebben op NAW-gegevens zoals de tenaamstelling of een telefoonnummer.[91] Een aanbieder zal dus antwoord moeten geven op de vraag welke naam bij een nummer hoort, of bij een adres. Ook de vraag of een persoon gebruik maakt van zijn diensten kan aan de aanbieder worden gesteld.[92]

3.4. De wet vorderen gegevens financiële sector

Het is van belang om voor een moment stil te staan bij de wet vorderen gegevens financiële sector. Deze wet omvat maatregelen in het kader van het bestrijden van terrorisme en het vergroten van de veiligheid middels een aantal nieuwe strafvorderlijke vorderingsbevoegdheden die specifiek de financiële sector treffen; zoals kredietinstellingen, wisselkantoren of verzekeringsbedrijven. De bevoegdheden zijn direct gebaseerd op de aanbevelingen van de Commissie Mevis. Daar het rapport Mevis al eerder in detail aan bod is gekomen in hoofdstuk twee zal hier worden volstaan met een korte bespreking. Geconstateerd kan in ieder geval worden dat de uitwerking van deze wet qua keuzes en uitgangspunten enigszins afwijkt van de bevoegdheidsverdeling die we terugzien in de wet vorderen gegevens telecommunicatie.

Men maakt net zoals de Commissie Mevis een onderverdeling in "identificerende gegevens", "andere gegevens" en "gevoelige gegevens". Gegevens kunnen worden gevorderd van iedereen die in beroeps- of bedrijfsmatige zin financiële dienstverlening aanbiedt. Geen categorie gegevens is hierbij uitgesloten van de bevoegdheden.[93] Ook zijn de bevoegdheden niet beperkt tot alleen de verdachte en kunnen dus gegevens van niet-verdachte personen worden gevorderd.[94]

De drie basisbevoegdheden zijn als volgt te omschrijven. De opsporingsambtenaar kan in geval van een misdrijf, of situatie zoals omschreven in 126o Sv, identificerende gegevens vorderen.[95] "Andere gegevens" kunnen worden gevorderd door alleen de officier van justitie, hierbij dient er wel sprake te zijn van een artikel-67-lid-1 misdrijf of van een situatie zoals bedoeld in 126o Sv. Tevens is vereist het vermoeden dat men toegang heeft tot de gevorderde gegevens.[96] Gevoelige gegevens kunnen door de officier van justitie alleen worden gevorderd na machtiging daartoe door de rechter-commissaris, waarbij er sprake moet zijn van ofwel een artikel-67-lid-1 misdrijf dat in samenhang met andere door de verdachte gepleegde misdrijven een ernstige inbreuk op de rechtsorde oplevert of van een situatie zoals bedoeld in artikel 126o Sv. Ook hier geldt dat de officier van justitie een redelijk vermoeden moet hebben dat de gegevens door de persoon toegankelijk zijn.[97]

Het vorderen van toekomstige gegevens is eveneens mogelijk, de officier van justitie kan een vordering tot het verstrekken van gegevens daartoe uitbreiden. Noodzakelijk is echter wel een schriftelijke machtiging van de rechter-commissaris indien de gegevens direct dienen te worden verstrekt als het belang van het onderzoek dit "dringend vordert".[98] Een machtiging is dus niet nodig als de gegevens enige tijd later na verwerking aan de officier van justitie worden aangeleverd. Daarnaast geldt de notificatieplicht van artikel 126bb Sv onverkort, uitgezonderd het vorderen van identificerende gegevens.

Vrijwillige medewerking aan het verstrekken van gegevens is zowel door de Commissie Mevis als de minister in de MvT bij de wet vorderen gegevens telecommunicatie uitgesloten indien strafvorderlijke bevoegdheden kunnen worden toegepast. Mac Gillavry merkt daarover op dat het enigszins onduidelijk is of dit in vergelijkbare mate geldt voor deze wet.[99] Gezien dat men direct heeft voortgebouwd op het rapport Mevis en het feit dat de minister nadrukkelijk de verantwoordelijkheid legt bij de justitiële autoriteiten lijkt mij dit echter wel de achterliggende intentie. Dit is immers ook in overeenstemming met het standpunt dat de minister heeft ingenomen in de MvT bij de wet vorderen gegevens telecommunicatie.[100]

De minister heeft het rapport van de commissie-Mevis niet gevolgd in de suggestie om een aparte bevoegdheid te creëren voor het stellen van voorvragen. Deze mogelijkheid wordt dan ook als het ware ingebakken in de bestaande bevoegdheid tot het vorderen van identificerende gegevens. Een belangrijk verschil met de wet vorderen gegevens telecommunicatie is dat er blijkbaar geen sprake hoeft te zijn van een vermoeden dat de financiële instelling over de gevraagde gegevens beschikt.[101]

Gegevens worden schriftelijk gevorderd, dat wil zeggen dat de opsporingsambtenaar of officier van justitie de vordering op schrift dient te stellen en overhandigt aan de adressaat van de vordering. Een mondelinge vordering is ook mogelijk, maar kan alleen worden gedaan bij dringende noodzaak. Een vordering dient dan achteraf alsnog op schrift te worden gesteld en te worden verstrekt binnen drie dagen. Worden gegevens verstrekt dan wordt hiervan proces-verbaal opgemaakt.[102]

Hoofdstuk 4. Rechtsvergelijking Verenigd Koninkrijk

4.1. Inleiding

Een blik buiten de grenzen van Nederland levert ons een beeld op van andere soortgelijke strafvorderlijke voorzieningen voor het vorderen van telecommunicatiegegevens. Het Engelse recht is in die zin interessant dat de Engelse situatie tot op enkele jaren geleden vergelijkbare kenmerken vertoonde met de Nederlandse systematiek; namelijk de vrijwillige medewerking als uitgangspunt met daarnaast een aantal wettelijke beperkingen die doen denken aan de situatie zoals onder de Wbp. Voornamelijk onder de invloed van jurisprudentie van het EHRM heeft zich ook hier een transformatie voltrokken, maar men slaat een andere weg in dan de Nederlandse wetgever.

4.2. Gegevensvergaring in het Verenigd Koninkrijk: Privacyrecht

Het basisprincipe in het Engelse recht is dat in het algemeen de opsporingsambtenaar zijn opsporingsbevoegdheden zal baseren op 'Common-law' (wat in principe erop neerkomt dat alles mag, tenzij…), waarmee beperkte inbreuken op de privacy gelegitimeerd kunnen worden. Voor ernstige inbreuken, zoals die bedoeld in artikel 8 EVRM, dient echter een duidelijke wettelijke basis voorhanden te zijn. Uitgangspunt in

het Engelse recht is de vrijwillige medewerking aan strafvordering, maar ook hier bindt de privacywetgeving de vrijwilligheid van burgers en bedrijven aan enkele beperkingen.[103]

4.2.1. De Data Protection Act 1998

De Data Protection Act 1998 (DPA 1998) geeft algemene regels voor het verwerken van persoonsgegevens in het Verenigd Koninkrijk.[104] Zo moet verstrekking rechtmatig zijn en heeft men recht op informatie omtrent de verwerking van gegevens.[105] Van belang voor strafvordering zijn met name de uitzonderingen, de DPA 1998 biedt namelijk een artikel dat enigermate gelijkenis vertoont met artikel 43 van de Nederlandse Wbp.[106] Zo hoeft niet te worden voldaan aan het eerste data 'protection principle' indien gegevens worden verstrekt ten behoeve van "prevention or detection of crime" of "the apprehension or prosecution of offenders". Beide uitzonderingen hebben gevolgen voor zowel het recht op informatie van de betrokkene alsmede de eisen die aan de verwerking van persoonsgegevens worden gesteld. De bepaling is qua opzet ruimer dan artikel 43 Wbp en biedt redelijk wat speelruimte om elke verstrekking ten behoeve van strafvordering te kunnen toestaan. Vergelijkbaar met de situatie onder de Wbp is het meewerken aan strafvordering onder de DPA 1998 geheel de vrijwillige keuze van de verwerker, ook al is de strafvorderlijke noodzaak van de verstrekking van persoonsgegevens duidelijk.[107]

4.2.2. Telecommunications Data Protection and Privacy Regulations 1999

De Telecommunications Data Protection and Privacy Regulations 1999 (TDPPR 1999) betreft specifieke privacywetgeving voor aanbieders van telecommunicatienetwerken en/of diensten en heeft een aanvullende werking ten aanzien van de DPA 1998.[108] Bij verkeersgegevens gaat het in de TDPPR 1999 om al het verkeer dat wordt verwerkt door de aanbieder van een telecommunicatienetwerk of dienst om zo een verbinding tot stand te brengen en te houden. Ook de persoonlijke gegevens van de abonnee met betrekking tot de afgenomen dienst worden daarnaast als verkeersgegevens aangemerkt. Het anonimiseren dan wel wissen van deze gegevens dient plaats te vinden nadat de verbinding is beëindigd.[109]

Voor opsporing en de vervolging van strafbare feiten bevat de TDPPR 1999 een aparte bepaling, deze maakt het mogelijk dat het wel of niet toepassen van de TDPPR 1999 achterwege kan blijven indien hierdoor strafvordering wordt gehinderd of het een en ander in conflict is met een wettelijke regeling of gerechtelijk bevel. Deze bepaling creëert dus een brede opening voor strafvorderlijke doeleinden zonder echt veel grenzen. Het is dan ook mogelijk dat een aanbieder op verzoek van justitie kan overgaan tot het verzamelen van gegevens die bijvoorbeeld normaliter buiten de normale bedrijfsvoering liggen. Beperkingen op deze vrijwillige medewerking bestaan alleen voor zover daarbij bij wet in is voorzien.[110]

4.3. Telecommunicatie en de RIPA 2000

Mac Gillavry constateert dat voor de inwerkingtreding van de Regulation of Investigatory Powers Act 2000 menig ISP in de overtuiging verkeerde dat verkeersgegevens en NAW-gegevens geheel probleemloos op vrijwillige basis konden worden verstrekt.[111] Zoals reeds is opgemerkt stond sectie 29 DPA 1998 niet aan vrijwillige medewerking in de weg, het telecommunicatiegeheim van de Telecommunications Act 1984 biedt de burger dan ook geen echte (privacy) waarborgen voor zowel inhoudelijke communicatie alsmede verkeersgegevens wanneer het opsporen of voorkomen van strafbare feiten als verwerkingsgrond wordt aangevoerd.[112]

De RIPA 2000 brengt in de bovenstaande situatie enige verandering en biedt een nieuwe wettelijke benadering voor het vorderen en aftappen van telecommunicatiegegevens.[113] Hiermee eindigt ook, althans in theoretische zin, de mogelijkheid tot vrijwillige verstrekking van deze gegevens.[114] De RIPA 2000 biedt een basis om aanbieders te verplichten tot het verstrekken en vastleggen van (toekomstige) gegevens en ontlast tevens de telecommunicatieaanbieders van de verantwoordelijkheid om het opsporingsbelang af te wegen tegen het verstrekken van deze gegevens.

Het begrip telecommunicatiegegevens ("communications data") in de RIPA 2000 moet in een zeer brede context worden gelezen. Het gaat hierbij om "any traffic data" als onderdeel van communicatie voor het gebruik door een postale dienst of telecommunicatiesysteem om zo (toekomstige) verzending mogelijk te maken, maar ook alle informatie die niet betrekking heeft op de inhoud van communicatie en het gebruik betreft van een postale- of telecommunicatiedienst door een persoon. Ook subscriber information wordt aangemerkt als 'traffic data', namelijk "any information … that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service".[115] De aanbieder is hierbij gehouden om "lawful" met deze gegevens om te gaan, bij het verstrekken of verzamelen van gegevens moet men dus handelen binnen het wettelijk kader dat door de RIPA 2000 is geschapen.[116] Dit houdt voor wat betreft het verkrijgen van telecommunicatiegegevens in dat men bevoegd dient te zijn om op te treden, en dat de bevoegdheid in overeenstemming met de daarvoor geldende regels wordt uitgeoefend.[117] Bevoegdheden staan verdeeld over verschillende afdelingen van de RIPA 2000.

Het vorderen van communicatiegegevens kan in eerste instantie samenvallen met het onderscheppen van communicatieverkeer in het algemeen. Hiervoor biedt de RIPA 2000 een speciale interceptiebevoegdheid middels een 'interception warrant'. Een dergelijk bevel verplicht de telecommunicatieaanbieder tot het onderscheppen en verstrekken van de communicatie die verloopt via zijn systeem, inclusief alle "related communications data".[118] Afgifte van een dergelijk bevel loopt niet via een rechter maar via de Secretary of State op verzoek. Een dergelijk verzoek kan onder meer worden gedaan door de 'Chief Constable' (hoofdcommissaris) van een politiekorps.[119] Het bevel zelf dient verder een naam of omschrijving te bevatten van de persoon die

dient te worden afgetapt.[120] De tapbevoegdheid is qua duur beperkt tot 3 maanden, met mogelijkheid tot het verlengen hiervan.[121] De verplichtingen voor een telecommunicatieaanbieder die voortvloeien uit een 'interception warrant' zijn niet onbeperkt, men hoeft niet zover te gaan dat men maatregelen dient te nemen welke "not reasonably practicable" zijn.[122]

Het materiaal dat via een 'interception warrant' is verkregen is uitgesloten als bewijs in het strafproces.[123] Dit is natuurlijk een bijzondere uitzondering in vergelijking met andere Europese landen, doch verklaarbaar. Het komt erop neer dat men veel waarde hecht aan de beslotenheid waarmee het opsporingsonderzoek plaatsvindt. De achterliggende theorie is dan ook dat indien dergelijk bewijs voor de rechter zou worden gebracht dit de opsporingsmethoden bloot zou leggen en op termijn de effectiviteit daarvan zou aantasten.[124] Als laatste dient nog te worden opgemerkt dat de 'interception warrant' procedure onderworpen is aan een strenge geheimhoudingsplicht die geldt voor iedere betrokkene.[125]

Het verzamelen van zuiver communicatiegegevens door de opsporingsambtenaar kan op twee manieren gebeuren. Zo kan hij allereerst een 'authorisation' bemachtigen van een bevoegd persoon. Hierbij gaat het om een ambtenaar die werkzaam is bij een 'relevant public authority' (zoals de politiedienst, maar ook de douane of belastingdienst) en door de Secretary of State is aangewezen. Op zijn beurt kan hij anderen bevoegd verklaren om zelfstandig de noodzakelijke gegevens te verzamelen.[126] Bij de politie gaat het dan om personen met de rang van minimaal 'Superintendent'. Voor communicatiegegevens die vallen onder sectie 22 lid 4 sub c, zoals "account and subscriber information", voldoet de rang van "Inspector".[127] De 'authorisation' bevoegdheid kan bijvoorbeeld worden ingezet wanneer de aanbieder zelf niet in staat is om de desbetreffende gegevens te vergaren. Van de bevoegdheid kan gebruik worden gemaakt indien sprake is van een van de in de RIPA 2000 genoemde doelen, waarbij toepassing van de bevoegdheid zowel proportioneel als ook noodzakelijk dient te zijn.[128]

Een tweede mogelijkheid is dat de opsporingsambtenaar een 'notice' (kennisgeving) doet uitgaan aan een post- of telecommunicatieaanbieder. Indien noodzakelijk kan deze 'notice' worden afgedwongen middels het Engelse civiele recht.[129] Vereiste bij een dergelijke kennisgeving is dat de ambtenaar moet vermoeden dat de aanbieder ook daadwerkelijk beschikt of kan beschikken over de desbetreffende telecommunicatiegegevens.[130] Is dit het geval, dan zal de aanbieder op last van de kennisgeving zijn gegevens beschikbaar moeten stellen dan wel de gevraagde gegevens traceren en alsnog aan de bevoegde ambtenaar moeten aanreiken. Hierbij dient het een en ander voor de aanbieder wel binnen het redelijk haalbare te liggen.[131] Tevens geldt ook hier dat toepassing van deze kennisgeving is beperkt tot een aantal specifieke doelen en proportioneel moet zijn met het voorgenomen doel.[132]

Zowel de 'authorisation' als ook de 'notice' dienen in principe op schrift te worden gesteld en behoren een beschrijving te bevatten van de gegevens die de telecommunicatieaanbieder moet verstrekken of verzamelen.[133] Voor beiden geldt tevens dat de duur van de periode waarover een aanbieder gegevens dient te

verstrekken of te vergaren in beginsel beperkt is tot een maand. Deze periode kan herhaaldelijk met een maand worden verlengd.[134] Aan de verstrekking dan wel het verzamelen op basis van een 'notice' komt een einde zodra deze wordt ingetrokken.[135]

Controle op de toepassing van de RIPA 2000 bevoegdheden in de praktijk komt toe aan de 'Interception of Communications Commissioner'. Niet alleen de opsporingsambtenaren maar ook de telecommunicatieaanbieders dienen volledige meewerking te verlenen bij het uitvoeren van deze taak. Het resultaat blijft echter beperkt tot het uitbrengen van een jaarlijks rapport, machtsmiddelen zoals het opleggen van sancties zijn er niet. Deze beperkingen zouden dan ook de transparantheid van de bevoegdheidstoepassing niet ten goede komen.[136] Controle kan tevens plaatsvinden middels een aangewezen tribunaal onder de RIPA 2000. Dit tribunaal handelt naar aanleiding van een klacht en kan onder meer vergoedingen toekennen maar bijvoorbeeld ook toegepaste of nog lopende bevoegdheden zoals de 'authorisation' en de 'interception warrant' toetsen en desgewenst vernietigen of beëindigen.[137] Hierbij moet voor ogen worden gehouden dat de RIPA 2000 evenwel in het algemeen geen notificatieprocedure kent en dat er tevens sprake is van een zeer vergaande geheimhoudingsplicht voor de betrokken partijen waar het de 'interception warrant' betreft. Mac Gillavry constateert dat in de Engelse juridische literatuur dit geleid heeft tot kritiek met betrekking tot de waarde van een dergelijk klachtensysteem, gezien het indienen van een klacht zo wel erg moeilijk, wellicht zelfs nagenoeg onmogelijk, wordt gemaakt.[138]

4.4. Rechtsvergelijkende constateringen

De normering van de Engelse bevoegdheden wijkt in belangrijke mate af van de tapbevoegdheid en de bevoegdheid tot het vorderen van verkeersgegevens die we kennen in het huidige Nederlandse recht, zowel qua reikwijdte als bevoegdheidstoedeling. Voor wat betreft de 'interception warrant' kan het volgende worden geconstateerd. In tegenstelling tot de Nederlandse variant is aan de Engelse tapbevoegdheid eveneens de mogelijkheid gekoppeld om verkeersgegevens te bemachtigen. Ligt in Nederland de autoriteit bij de officier van justitie, gekoppeld aan het vereiste van een machtiging van de rechter-commissaris, in Engeland wordt een dergelijk verzoek gedaan door de hoofdcommissaris van politie aan de Secretary of State. Van een onafhankelijke rechterlijke toetsing vooraf is bij een dergelijke ingrijpende bevoegdheid dus geen sprake. Eveneens karakteristiek is de ruime opzet van de bevoegdheid, er vindt in het geheel geen differentiatie plaats naargelang het soort strafbare feit of personen. In beginsel kan de tapbevoegdheid dus worden toegepast onder alle denkbare omstandigheden, iets wat onmogelijk zou zijn met de Nederlandse tapbevoegdheid van art. 126m Sv. Het meest opmerkelijke verschil is wel dat de verkregen gegevens niet als bewijs kunnen dienen in het strafproces, waarbij tevens sprake is van een strenge geheimhoudingsplicht. Een notificatieplicht zoals wij die kennen in 126bb Sv vinden we hier dan ook niet. Aan het proces-verbaal worden weinig inhoudelijke eisen gesteld, het is reeds voldoende als alleen de betrokkene of de plaats waar de tap dient te worden geplaatst wordt omschreven. Verdere eisen, zoals het vermelden van feiten en omstandigheden dat aan de voorwaarden voor het toepassen van de bevoegdheid is voldaan, worden aan het proces-verbaal niet

opgelegd.

Zowel de 'authorisation' als de 'notice' zijn specifiek gericht op het verkrijgen van verkeersgegevens en zijn dan ook in dat opzicht vergelijkbaar met 126n/u Sv. Rust deze bevoegdheid in Nederland bij de officier van justitie, net als bij de Engelse tapbevoegdheid is het ook hier wederom de politie die kan overgaan tot toepassing van de bevoegdheden. Hierbij dient een onderscheid te worden gemaakt tussen betrekkelijk eenvoudige 'account information', welke door de adjudant van politie kan worden opgevraagd, en alle andere communicatiegegevens die alleen binnen het handbereik van een inspecteur van politie vallen. Deze opzet verschilt toch wel enigszins met de Nederlandse situatie. Zo wordt hier immers binnen een bevoegdheid gedifferentieerd naargelang het soort gegevens en de autoriteit. Een aparte bevoegdheid zoals 126na/ua Sv om gebruikersgegevens te vorderen kent de RIPA 2000 niet. Dit toont dan ook meer overeenkomsten met de Nederlandse mogelijkheid om middels 126n/u Sv zowel verkeers- als gebruikersgegevens te vorderen, zij het dat daar van een andere bevoegdheidstoedeling sprake is; immers komt die bevoegdheid alleen toe aan de officier van justitie. De 'authorisation' heeft qua mogelijkheden geen equivalent in het Nederlandse recht, het vorderen van verkeersgegevens via 126n/u Sv ligt dan ook eerder in de lijn van de Engelse 'notice' waarbij het dwangmatige karakter van het bevel en de verstrekking door de telecommunicatieaanbieder zelf voorop staat. Het is immers niet zo dat de Nederlandse opsporingsambtenaar, indien de aanbieder niet zelf over de gegevens beschikt, zelf dan maar kan optreden om de gewenste gegevens te vergaren. Ook voor deze bevoegdheden geldt eveneens dat geen nadere differentiatie plaatsvindt naar het soort strafbaar feit of noodzakelijkheid voor het onderzoek, alleen de vereiste proportionaliteit stelt hier grenzen aan de toepassing. Een notificatieplicht vergelijkbaar met 126bb Sv is ook hier niet aanwezig.

Karakteristiek voor de hierboven beschreven bevoegdheden is dan ook wel dat ze vrij ruim van opzet zijn, zo kunnen communicatiegegevens niet alleen worden gevorderd voor strafvorderlijke doeleinden maar voor een veel breder scala aan toepassingen. Ook de afwezigheid van enige rechterlijke toetsing en het gebrek aan nuance bij de afbakening van de bevoegdheden - in contrast met de Nederlandse bevoegdheden - zijn opmerkelijk te noemen. Voor wat betreft de rechtswaarborgen heeft de Nederlandse regeling dan ook mijns inziens duidelijk de voorkeur, meerdere concrete grenzen zorgen dat niet al te losjes met de opsporingsbevoegdheden wordt omgesprongen. Evenzo maakt een uitgebreidere notificatieplicht ook een betere controle mogelijk. Het Engelse telecommunicatierecht slaat juist de tegengestelde weg in, zeer ruime bevoegdheden met weinig wettelijke beperkingen. En als die beperkingen er al zijn, dan zijn ze minimaal omschreven.[139] De rechtszekerheid is dan ook in het Nederlandse recht nadrukkelijker aanwezig en lijkt de aangewezen weg om ook in de toekomst verdere invulling te geven aan deze bevoegdheden.

Hoofdstuk 5. Algehele Reflectie

5.1. Inleiding

De concrete uitwerking van de vernieuwde bevoegdheden voor het vorderen van communicatie- en gebruikersgegevens roept de nodige vragen op ten aanzien van een aantal uitgangspunten en argumenten die aan de wijzigingen ten grondslag liggen. Niet alleen op nationaal constitutioneel niveau, maar onvermijdelijk ook in een Europees kader dient de regeling tegen het licht te worden gehouden. In de navolgende paragrafen zal ik eerst in het specifiek ingaan op de vraag in welke verhouding verkeersgegevens dienen te staan ten opzichte van de bescherming die de inhoud van communicatie geniet. Hierna zal ik enkele van de meest belangrijke voorwaarden van de nieuwe bevoegdheden nader onder de loep nemen.

5.2. Convergentie inhoud en verkeersgegevens

Onder het nieuwe recht gaan de bevoegdheden uit van een gelijkvormige groep van verkeersgegevens waarbinnen geen onderscheid te maken valt; alle verkeersgegevens zijn a priori gelijkgesteld. Dit uitgangspunt lijkt mij in toenemende mate onrealistisch. Zoals de minister reeds aangaf in de memorie van toelichting was de wet onder meer een reactie op de technische ontwikkelingen in telecommunicatiemogelijkheden; de nieuwe bevoegdheden zouden hier beter op toegesneden zijn. Dit heeft echter ook een keerzijde; nieuwe technologische ontwikkelingen vervagen de ooit zo duidelijke grens tussen de inhoud van communicatie en de verkeersgegevens zelf, hetgeen het per saldo juist moeilijker maakt om wetgeving goed af te stemmen op de realiteit.

Het meest duidelijk komt dit wel tot uitdrukking op het Internet, waar bijvoorbeeld verkeersgegevens in de vorm van URL of IP-adressen inzicht kunnen geven in iemands interesseprofiel. URL adressen kunnen evenzeer inhoudelijke elementen bevatten of zelfs ook naar de volledige inhoud van de communicatie wijzen. En wat te denken van het onderwerpveld bij een email bericht? Ook bij de reguliere (mobiele) telefonie zien we een vervagende grens door de introductie van allerlei nieuwe services (bijvoorbeeld het internetten via de telefoon). Maar niet alleen de vervagende scheidslijn tussen inhoud en verkeersgegevens werkt problematisch, zo merkt Koops terecht op dat een toenemende vergaringdrang naar gegevens een even grote druk legt op de privacy gevoeligheid.[140] Zo is het niet ondenkbaar dat gegevens die in isolatie geen (grote) privacy inbreuk opleveren, dit in een bepaalde omvang en/of samenhang juist wel doen, veelvuldig telefonisch contact of het frequent bezoeken van bepaalde internet sites kan zonder meer gevoelige informatie opleveren; denk bijvoorbeeld aan de persoon die geregeld de website van ‘zijn’ politieke partij bezoekt.

Bovenstaande heeft tot gevolg dat men gegevens onder het begrip verkeersgegevens brengt die in werkelijkheid een hybride karakter dragen en waarvoor wellicht een ander wettelijk regime zou moeten gelden. De regering is zich hier blijkbaar van bewust, althans haar standpunt naar aanleiding van vragen van de Eerste Kamer maakt duidelijk dat bijvoorbeeld ingegeven zoekwoorden die onderdeel vormen van

een zoekopdracht en als zodanig in de URL verschijnen "als inhoud [moeten] worden gezien".[141] Betekent dit nu dat deze specifieke reeds opgeslagen verkeersgegevens niet kunnen worden verkregen op basis van art. 126n/u Sv, maar de officier van justitie gebruik zal moeten maken van 125i Sv - het onderzoek in een geautomatiseerd werk, welke thans ook wordt gebruikt om opgeslagen e-mail te vorderen - of de nieuwe bevoegdheden 126ng en 126ug Sv van het wetsvoorstel bevoegdheden vorderen gegevens? Het kabinet houdt vooralsnog vast aan de exclusiviteit van de artikelen 126n/u Sv voor wat betreft het vorderen van verkeersgegevens, desalniettemin lijkt het onontkoombaar om andere bevoegdheden in overweging te nemen als de artikelen 126n/u Sv geen oplossing bieden. De vraag rijst immers hoe men een absolute scheiding tussen verkeersgegevens en inhoud kan rechtvaardigen als men reeds moet erkennen dat bepaalde soorten van verkeersgegevens dualistisch van karakter zijn en mede als inhoud van communicatie moeten worden gezien. Dit punt staat dan ook eigenlijk niet in de literatuur ter discussie, en het lijkt mij een gegeven dat onder omstandigheden het verzamelen van verkeersgegevens een zeer ingrijpend beeld op kan leveren van iemands persoonlijke levenssfeer, analoog aan inhoudelijke communicatie.

5.3. De grondwettelijke status van verkeersgegevens en het communicatiegeheim

Het huidige artikel 10 Gw beperkt zich tot het beschermen van verkeersgegevens die tevens persoonsgegevens zijn. Verkeersgegevens genieten niet de bescherming van artikel 13 Gw, althans is dit het heersende standspunt van het kabinet.[142] Als onderbouwing geeft ze onder meer als reden dat het verzamelen van verkeersgegevens per definitie minder ingrijpend zal zijn dan het kennisnemen van de inhoud van een gesprek.[143] Ook de Commissie Franken heeft in haar rapport de bescherming van verkeersgegevens onder (een nieuw) artikel 13 Grondwet afgewezen, onder meer omdat hier dan een rechterlijke machtiging tegenover zou komen te staan.[144] Deze afwijzende houding heeft de nodig kritiek losgemaakt, en zeker niet onterecht. Zo merkt het College Bescherming Persoonsgegevens op dat het onwenselijk is dat de overheid alleen onder strenge voorwaarden kennis kan nemen van de inhoud van communicatie, maar met veel minder beperkingen dat communicatieverkeer zou kunnen controleren.[145] Terecht werpt men ook de vraag op of onder zulke omstandigheden er eigenlijk nog wel sprake kan zijn van vertrouwelijke communicatie. Men pleit in de literatuur dan ook voor een andere benadering waarbij niet de inhoud van communicatie het primair te beschermen rechtsgoed is, maar artikel 13 Gw juist voornamelijk waarborgt dat men kan beschikken over een vertrouwelijk communicatiekanaal.[146] Met dit als uitgangspunt genieten zowel inhoud als verkeersgegevens gelijke bescherming.

5.4. Verkeersgegevens in Europees kader: artikel 8 EVRM

In een aantal arresten heeft het EHRM zich gebogen over de vraag waar verkeersgegevens nu staan ten opzichte van het in artikel 8 EVRM genoemde 'respect for correspondence' en het 'respect for private life'. Ten aanzien van deze jurisprudentie van het Europese Hof is het kabinet van mening dat deze niet zou

dwingen tot een ander gezichtspunt, zo zou het Europese Hof zelf een duidelijk onderscheid maken tussen verkeersgegevens en het onderscheppen van communicatie.[147] Dit standpunt overtuigt naar mijn mening niet, en wel om twee redenen. Het door het EHRM besproken verschil tussen verkeersgegevens ('metering') en het onderscheppen van communicatie betreft de constatering dat het laatste nooit legitiem kan zijn zonder de noodzaak ervoor in combinatie met een wettelijke basis, terwijl het registreren van verkeersgegevens ook zonder wettelijke grondslag legitieme doeleinden kent (facturering e.d.).[148] Het EHRM zegt hiermee *niet* dat verkeersgegevens per definitie zouden vallen onder geen of een beperkter beschermingsregime, in tegendeel. De cruciale vraag die het kabinet zich had moeten stellen is de vraag of het gebruik van verkeersgegevens kan botsen met het communicatiegeheim van artikel 8 EVRM.[149] Het Hof beantwoord deze belangrijke vraag in het arrest Malone immers met een glashelder 'ja'. Zo stelt het EHRM in 'Mallone' dat "the Court does not accept … that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Art. 8. The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone."[150] Het telefoongedrag van een persoon wordt dus beschermd door het communicatiegeheim omdat het een integraal element van de communicatie zelf betreft.

Ook de privacy en elektronische communicatie richtlijn, welke eisen stelt aan de lidstaten met betrekking tot het nemen van maatregelen om zo "het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens" te garanderen maakt per definitie geen onderscheid tussen communicatiegegevens en inhoud.[151]

In het 'P.G. & J.H. vs. VK' arrest bouwt het Hof verder op het standpunt ingenomen in 'Malone', zo merkt ze op met betrekking tot de wettelijke waarborgen die dienen te bestaan dat: "what is required by way of safeguards will depend, to some extent at least, on the nature and the extent of the interference in question. In this case, the information obtained concerned the telephone numbers called from B's flat between two dates. It did not include any information about the contents of those calls, or who made or received them. The data obtained and the use that could be made of it, were therefore strictly limited."[152] Ook deze overweging geeft blijk van het feit dat niet alleen de inhoud van communicatie centraal staat, ook de verkeersgegevens (naar wie is gebeld en door wie) zijn medebepalend bij de vraag of het communicatiegeheim is geschonden. Bepalend is dan ook, zoals onder meer Dommering constateert, "hoeveel er over een persoon in of door de privé-communicatie bekend wordt."[153] Een dergelijke nuancering dient mijns inziens dan ook in wetgeving verdisconteert te zijn.

5.5. Van uniformiteit naar diversiteit; differentiëren naar privacygevoeligheid?

Convergentie tussen verkeersgegevens enerzijds en inhoud anderzijds zou aanleiding zijn om een nadere differentiatie tussen verkeersgegevens op basis van privacygevoeligheid te overwegen (Koops, 2003). Een dergelijke differentiatie lijkt me zeker niet onwenselijk, het is immers van gewicht om ervoor te zorgen dat het opsporingsbelang en de bescherming die de burger - ook vanuit Europees opzicht –

verdient tegen inbreuken op zijn persoon zo goed mogelijk in balans met elkaar zijn.

Een nuancering van de bevoegdheid, zoals bijvoorbeeld is te vinden in de wet 'vorderen gegevens financiële sector' dat in grote lijnen gebaseerd is op de Commissie Mevis bevoegdheden, levert desondanks een aantal voorzienbare praktische problemen op. In de eerste plaats lijkt mij het uitgangspunt dat we efficiënt en gemakkelijk kunnen differentiëren naar privacygevoelige verkeersgegevens niet reëel, althans is dit op zijn minst niet eenvoudig te bewerkstelligen. Het is immers geen redelijke verwachting dat bepaalde categorieën van verkeersgegevens altijd in dezelfde mate een inbreuk zullen vormen op het communicatiegeheim; zo kan bijvoorbeeld het belgedrag of internet surfgedrag van een persoon meer zeggen dan dat van een ander. Of het opvragen en gebruiken van verkeersgegevens het communicatiegeheim raakt en in welke mate het dat doet lijkt mij dus zeer contextgevoelig waarbij men het een en ander zal moeten beoordelen aan de hand van concrete omstandigheden.

Hes stelt daartegen een aanpak voor waarbij vooraf onderscheid wordt gemaakt op een abstract technisch niveau.[154] Hij constateert daarbij dat de huidige definitie van het begrip verkeersgegeven niet voldoende mogelijkheden biedt om de "diffuse scheidslijn tussen inhoud en verkeersgegevens" op te heffen. Als oplossing stelt hij dan ook voor om per individueel communicatie protocol te definiëren en vast te leggen wat als inhoud heeft te gelden en wat niet.[155] Het gevolg hiervan is echter zeer technologieafhankelijke wetgeving waar alles tot in detail op zeer abstract technisch niveau zal moeten worden uitgewerkt. Juist het streven naar een hanteerbare techniekonafhankelijke regeling en het sluimerende gevaar dat techniekafhankelijke regelgeving op termijn snel zal verouderden lijken mij sterk te pleiten tegen een dergelijke aanpak. Ook biedt het geen oplossing voor verkeersgegevens die in combinatie met elkaar wellicht een zeer gedetailleerd beeld kunnen schetsen van iemands interessesfeer; zoiets valt immers moeilijk vooraf in een definitie te vangen. Daarnaast zal het categorisch beschermen van bepaalde communicatiegegevens, ongeacht of er nu wel of niet sprake is van privacygevoelige informatie, gevolgen hebben voor het strafvorderlijk onderzoek.

Koops is van mening dat verkeersgegevens "die deels (hoe weinig ook) inhoud van telecommunicatie betreffen" moeten vallen onder de veel strengere telecommunicatietap bevoegdheid.[156] Ik wil meegaan in het standpunt dat inhoudelijke elementen, dan wel informatie vergelijkbaar met inhoud die indirect kan worden afgeleid uit het samenspel van verkeersgegevens, in een ander beschermingsregime zouden moeten vallen. Daarbij lijkt het mij wel belangrijk om een onderscheid tussen maken tussen die verkeersgegevens waaraan werkelijke, als het ware tastbare, elementen van inhoud kleven – bijvoorbeeld de zoekgegevens in een internet URL - en die verkeersgegevens die op zich zelfstaand geen inhoudelijk element bevatten maar wellicht in combinatie met andere verkeersgegevens een bepaald beeld kunnen schetsen van de communicatie zelf. Een verdergaande bescherming voor de eerste categorie gegevens lijk mij hierbij in beginsel meer vanzelfsprekend dan voor gegevens van de tweede categorie. Doch moet niet worden onderkend dat dit onderscheid tevens kunstmatig is, wanneer gegevens uit de tweede categorie

informatie opleveren vergelijkbaar met de eerste categorie dan dient ook hetzelfde beschermingsregime van toepassing te zijn. Resteert nog de vraag hoe en op welke manier onderscheid te maken.

Bij een eventuele differentiatie speelt een toetsingsmoment. Is er nu wel of niet sprake van 'inhoud' en middels welke toepasselijke bevoegdheid moet deze 'inhoud' worden gevorderd? Zouden duidelijke richtlijnen bestaan aangaande wat te gelden heeft als inhoudelijke communicatie dan hoeft bij de telecommunicatieaanbieder in ieder geval geen vergissing te bestaan over de gegevens die zij dient te verstrekken aan justitie. Maar als heldere criteria juist moeilijk te geven zijn, zeker wanneer interpretatie eraan te pas dient te komen om verkeersgegevens te kunnen categoriseren, ontstaat een aanzienlijk probleem. Om de gegevens onder te verdelen naar privacygevoeligheid dient men ze in te zien, zouden we het toetsingsmoment dus leggen bij justitie dan gaan we er vanuit dat de officier van justitie - wellicht met behulp van een kristallen bol – weet dan wel zou moeten weten in welke categorie de desbetreffende gegevens zullen vallen zodat hij de juiste bevoegdheid kan toepassen. Dat is natuurlijk onwerkelijk, het vorderen van gegevens middels een met beperkte waarborgen omgeven bevoegdheid zonder dat men eigenlijk weet hoe gevoelig bepaalde gegevens zullen zijn lijkt mij geenszins een bevredigende systematiek. Zeker bij verkeersgegevens waar de privacygevoeligheid toch al voorshands niet altijd even eenvoudig is in te schatten is dit uitgangspunt niet houdbaar. Een vergelijkbaar probleem speelt ook bij het nieuwe wetsvoorstel 'bevoegdheden vorderen gegevens', gemodelleerd naar de Mevis bevoegdheden. Zo kan bijvoorbeeld de inhoud van email worden gevorderd indien er sprake is van een relatie met de verdachte of het strafbare feit.[157] Maar hoe en door wie dient te worden vastgesteld of hier inderdaad sprake van is en onder welke voorwaarden? Hoe en door wie wordt bepaald of er sprake is van gevoelige gegevens of niet, en onder welke voorwaarden? Het gebrek aan waarborgen maakt het uiteindelijk redelijk eenvoudig om enorme hoeveelheden (mogelijk zeer gevoelige) gegevens (ten onrechte) in bezit te krijgen, een dergelijke opzet dient dan ook te worden vermeden.

Een voor de hand liggende oplossing is dat de toetsing met betrekking tot het rubriceren, voordat gegevens aan justitie worden verstrekt, in ieder geval wordt gelegd bij een onafhankelijke derde partij. Dit zou niet de houder van de gegevens zelf moeten zijn, we zouden zo immers opnieuw een situatie in het leven roepen die doet denken aan de verstrekking van gegevens onder de Wbp waarbij ook de houder de afweging tot afgifte maakte. Houders van verkeersgegevens zullen niet zitten te wachten op extra verantwoordelijkheden, afgezien van legio andere denkbare problemen rondom de toetsing zelf. Tevens lijkt me dit moeilijk te rijmen met jurisprudentie van het EHRM in het kader van artikel 8 EVRM.[158] In het arrest Kopp, waar het ging om het ongeoorloofd afluisteren van een advocaat, maakt het Hof duidelijk dat juist het maken van onderscheid met betrekking tot de inhoud problematisch van aard is en een wettelijke regeling dan ook om voorzienbaarheid en grondige waarborgen vraagt. In casu werd deze beoordeling overgelaten aan een ambtenaar van de juridisch afdeling van de telefoondienst, iets wat volgens het Hof volstrekt ontoelaatbaar was.[159] Vooralsnog lijkt de Nederlandse wetgever zich er niet om te bekommeren wie de taak op zich neemt, op welke manier dit gebeurt en met

welke waarborgen dit deel van de procedure is omkleed.

Een andere oplossing voor dit alles zou natuurlijk kunnen zijn om het geheel dan maar onder één zwaar regime te brengen waarbij de normering van de bevoegdheden hoog wordt gelegd, zoals bijvoorbeeld het geval is bij de randvoorwaarden voor toepassing van de tapbevoegdheid. Dit biedt een sluitende oplossing voor de hierboven aangedragen problemen. Evenwel moet voor ogen worden gehouden dat ook voldoende verkeersgegevens zullen worden opgevraagd die niet onder een dergelijk beschermingsregime zouden hoeven te vallen, de vraag is dan ook of een dergelijke oplossing niet te drastisch voorkomt en een wat genuanceerder systeem vooralsnog de voorkeur heeft boven een 'brute force' categorisatie.

5.6. Identificerende gegevens

Een notificatieplicht (126bb Sv) maakt geen onderdeel uit van het vorderen van gebruikersgegevens; een schriftelijk proces verbaal en het registreren van het aantal vorderingen door het CIOT moet onder meer zorgen voor de nodige transparantheid en controle. Dat een notificatieplicht 'onwerkzaam' zou zijn gezien een groot aantal te verwachten verzoeken lijkt mij een zwak argument van het kabinet, het is immers ook blijkbaar de verwachting dat het prima mogelijk is om elke vordering op schrift te stellen. Daarnaast is het nog maar de vraag of algemene informatie over het aantal vorderingen voldoende is om zo "het gebruik in algemene zin te controleren".[160] Dergelijke gegevens zeggen immers niet bijster veel over de inhoudelijke procedure die aan het opvragen vooraf is voorgegaan. Juist het belang van een notificatieplicht, wat tot doel heeft om het gebruik van bevoegdheden transparant en controleerbaar te maken, lijkt hierbij dan ook relevant. Het CBP is in dit kader eveneens sceptisch en stelt dat in haar ervaring "de informatiehuishouding van de politie nu vaak niet in overeenstemming is met de geldende voorschriften".[161] Extra maatregelen om ongeregeldheden in het toepassen van de bevoegdheid te voorkomen lijken mij dus wenselijk, des te meer daar de verwachting is dat het gebruik van de bevoegdheid enorm zal toenemen. Zonder enig concreet toezicht wat uit meer bestaat dan het louter bijhouden van het aantal verzoeken lijkt de kans op fouten juist toe te nemen. De suggestie dat de voorwaarden gebonden aan het toepassen van de bevoegdheid, zoals het op schrift stellen van de vordering, dan ook zouden nopen tot weloverwogen gebruik lijkt in het licht hiervan twijfelachtig; dit zijn niet meer dan papieren barrières. Zo ziet het CBP meer in een schrikeffect door een financiële vergoeding te koppelen aan elke bevraging om enige terughoudendheid te bewerkstelligen.[162] Niet onterecht dunkt me, als één zaak gevoelig ligt dan is dit wel het justitiële budget.

Dat het opvragen van gebruikersgegevens volgens het kabinet op zich niet erg ingrijpend zou zijn voor de betrokkenen geeft eveneens reden tot twijfel, het is immers niet ondenkbaar dat door de vordering de relatie tussen de verstrekker en de persoon waarop de vordering betrekking heeft onder spanning komt te staan.[163] Zeker nu ook gebruikersgegevens van niet-verdachten kunnen worden gevorderd dient men ook hier beter bedacht te zijn op de mogelijke gevolgen van het achterwege blijven van een notificatieplicht bij het opvragen van gebruikersgegevens. Daarnaast zou, wetsystematisch gezien, het onderbrengen van het vorderen van gebruikersgegevens

bij de officier van justitie eveneens niet misstaan gezien de officier van justitie de bevoegde autoriteit is bij tal van de wet BOB bevoegdheden.

5.7. Gebruikersgegevens als verkeersgegevens?

Ook de bevoegdheden voor wat betreft het vorderen van gebruikersgegevens zijn er niet echt duidelijker op geworden. De wetgever biedt de opsporingsambtenaar immers twee, van elkaar volledig losstaande, mogelijkheden; middels de artikelen 126na en 126ua Sv kunnen identificerende gebruikersgegevens worden gevorderd. Dit doet men nog eens dunnetjes over door een tweede ingang te bieden via artikel 126n/u Sv waarmee dezelfde gegevens kunnen worden verkregen; gebruikersgegevens (NAW-gegevens) worden hier immers aangemerkt als verkeersgegevens.[164] Deze tweeslachtigheid is onnodig verwarrend, het leidt er in ieder geval niet toe dat de definitie wat nu onder verkeersgegevens dient te worden verstaan er enigszins helderder op wordt. Daarnaast loopt het verkrijgen van verkeersgegevens voor zover deze gebruikersgegevens betreffen eveneens via het CIOT, dubbelop dus.[165] De wetgever draagt nog verder bij aan deze chaos door ook gebruikersgegevens zoals het betalen van rekeningen of het gebruik van bepaalde technische voorzieningen onder de definitie te brengen.[166] Het was wellicht duidelijker en consistenter geweest om gebruikersgegevens in zijn algemeenheid samen te brengen in één specifieke regeling.

5.8. Verdachte versus niet verdachte

De artikelen 126n en 126u Sv geven de officier van justitie de mogelijkheid om gegevens op te vragen over een ieder indien dit in het belang is van het onderzoek. Dat nu ook gegevens van niet-verdachten in aanmerking komen ligt besloten in het opsporingsbelang en het argument dat de telecommunicatietap bevoegdheid de beperking ook niet meer kent. Hierbij wordt echter ten onrechte uit het oog verloren dat, alhoewel de telecommunicatietap een zwaardere bevoegdheid is waarbij de 'verdachte eis' niet geldt, zij daarentegen juist met zwaardere waarborgen is omkleed; zo is immers een machtiging van de rechter-commissaris vereist en kan de bevoegdheid alleen worden toegepast indien het onderzoek dit dringend vordert. Het laten varen van de 'verdachte eis' bij de telecommunicatietap bevoegdheid was juist de reden om de randvoorwaarden ervan aan te scherpen.[167] Deze lat ligt wel een heel stuk lager bij de bevoegdheden van 126n/u Sv waardoor zij in een bredere context toepasbaar zal zijn. Gegevens van niet-verdachten worden op deze manier dan ook een stuk sneller toegankelijk.

Vermeldenswaard is tevens het feit dat de telecommunicatietap bevoegdheden die betrekking hebben op een situatie waarbij misdrijven worden gepleegd in georganiseerd verband (de artikelen 126t/s Sv) wel een eis van vermoedelijke betrokkenheid kennen, de bevoegdheid voor het vorderen van verkeersgegevens in een 126o lid 1 Sv situatie (126u Sv) kent deze beperking in het geheel niet. Bovendien, zo merkt Corstens op, is de zwaarste vorm van het subsidiariteitsbeginsel die we vinden bij de telecommunicatietap ('indien het onderzoek dit dringend vordert') juist aangelegd omdat het onderzoek "kan en meestal plaats zal vinden zonder

medeweten van de betrokkenen die bovendien niet alle verdachten behoeven te zijn".[168] Dit is een extra zorgvuldigheid die 126n/u Sv aan niet-verdachten niet kan bieden. Het is geen ondenkbaar scenario dat het voor justitie verleidelijk zal zijn om te vissen in het netwerk van contacten hopende op bruikbare informatie waar men – dus bij puur toeval - tegenaan loopt. Dat daarvoor eerst het communicatienetwerk tot in redelijk detail bloot moet worden gelegd, voordat men enigszins een inschatting kan maken van de bruikbaarheid en betrokkenheid van de contacten bij een misdrijf, mag duidelijk zijn. De drempel van subsidiariteit ('in het belang van het onderzoek') is immers zo laag mogelijk aangebracht, en op volledige bewijsuitsluiting hoeft justitie ook niet bedacht te zijn gezien dat een formele onrechtmatigheid door het onrechtmatig toepassen van een bevoegdheid zeker niet altijd leidt tot bewijsuitsluiting.[169] Het een en ander kan dan ook leiden tot welwillende misbruik van de zeer ruime reikwijdte van de bevoegdheid, afgezien van de pertinente vraag of het gebruik ervan ooit aan een rechter zal worden voorgelegd.

Hoe het laten vervallen van de 'verdachte eis' zich verhoudt tot de minimumeisen van artikel 8 EVRM is onduidelijk. Het uitgangspunt is dat normen toegankelijk en voorzienbaar dienen te zijn. Het laatste brengt met zich mee dat voldoende duidelijk moet zijn voor de burger wanneer en onder welke omstandigheden een beperking mogelijk is. Ook het ontbreken van een notificatieplicht voor wat betreft niet-verdachten doet een veel grotere groep van personen ontstaan die niet de mogelijkheid zullen hebben om te controleren of ten aanzien van hen rechten zijn geschonden. De adviescommissie van de Nederlandse Orde van Advocaten stelde het laten vervallen van de 'verdachte eis' en de mogelijke onverenigbaarheid ervan met artikel 8 EVRM reeds eerder ter discussie waar het de telecommunicatietap bevoegdheid zelf betreft.[170] Met name de gewijzigde reikwijdte van de bevoegdheden 126n/u Sv zijn niet helder afgebakend, het is immers in beginsel mogelijk om het volledig communicatienetwerk van personen bloot te leggen; niet alleen van de verdachte, maar van een ieder in "het belang van het onderzoek". Het kabinet moet dit als zodanig ook erkennen en merkt op dat een "beperking van de persoonlijke levenssfeer van de verdachte eerder [is] gerechtvaardigd dan een beperking van de persoonlijke levenssfeer van een niet verdachte persoon … de voorgestelde bevoegdheden [kunnen] weliswaar in beginsel kunnen worden toegepast ter verkrijging van gegevens betreffende niet verdachte personen, maar … hierbij [is] grotere terughoudendheid geboden. In het proces-verbaal dient hierover verantwoording te worden afgelegd."[171] Het is maar afwachten of deze "grote terughoudendheid" ook daadwerkelijk in de praktijk gebezigd zal worden. Het hanteren van strengere voorwaarden ten aanzien van niet-verdachten om zo terughoudendheid te bewerkstellingen voor wat betreft de confrontatie van niet-verdachte personen met ingrijpende opsporingsbevoegdheden, bijvoorbeeld dat een dergelijke vordering alleen gedaan kan worden indien het belang van het onderzoek het dringend vordert, lijkt mij daarbij wenselijk.

5.9. Noodzaak vorderen verkeersgegevens nieuwe stijl

Voor wat betreft de vraag of de wijzigingen van de bevoegdheden ook "noodzakelijk zijn in een democratische samenleving" zoals artikel 8 EVRM vereist kan worden

gesteld dat de onderbouwing op dit punt enigszins magertjes in de memorie van antwoord uit de verf komt. Het blijft beperkt tot de opmerking dat "de bevoegdheid verkeersgegevens te vorderen, zoals deze thans reeds is neergelegd in de artikelen 126n en 126u Sv, gezien [wordt] als onmisbaar bij de opsporing van strafbare feiten".[172] Echt onderbouwd wordt dit standpunt, dat dergelijke gegevens zeer noodzakelijk zouden zijn voor het opsporingsonderzoek, niet. De praktijk lijkt een genuanceerder beeld te schetsen. Zo valt uit het rapport "het gebruik van (historische) verkeersgegevens in de opsporingspraktijk" van de politie Rotterdam Rijnmond onder meer te concluderen dat voor wat betreft de zware en de middencriminaliteit de noodzaak aan verkeersgegevens beperkt blijft. In 70% van de gevallen zou ook door het inzetten van andere bevoegdheden voldoende informatie kunnen worden verzameld om een zaak op te lossen. Bij onderzoek naar zaken die in het verleden hebben plaatsgevonden of bij fraudepraktijken blijkt de behoefte aan verkeersgegevens groter.[173] Daarnaast is het opmerkelijk te noemen dat juist de eenvoudige hacking van 138 a lid 1 Sr, waarbij verkeersgegevens echt noodzakelijk zijn, uit de wet is geschrapt als grond om verkeersgegevens te vorderen.

Uit het Stratix Consulting rapport valt te concluderen dat werkelijke belemmeringen bij de opsporing juist vooral liggen in onder meer praktische problemen bij de telecommunicatieaanbieder. Zo zijn vaak bepaalde gegevens gewoonweg niet beschikbaar of moeilijk te lokaliseren.[174] Het is dan ook nog maar de vraag of er vanuit de opsporingspraktijk ook daadwerkelijk veel behoefte is aan het uitbreiden van bijvoorbeeld de kring van personen waarvan gegevens kunnen worden gevorderd ten opzichte van de bevoegdheid inlichtingen telecommunicatie zoals die voorheen bestond. Zo concludeert het Stratix rapport dat voor wat betreft telefonie de aanbieders "goed in staat [zijn] om aan de vorderingen te voldoen" waarbij historische verkeersgegevens de voornaamste rol innemen.[175] Hoe het een en ander in verhouding staat met betrekking tot de bevoegdheidsuitbreiding lijkt me in ieder geval voldoende stof doen opwaaien en zou het kabinet moeten dwingen tot het beter motiveren van de overwegingen die aan de wijzigingen van 126n en 126u Sv ten grondslag liggen.

5.10. Conclusies

Met het vorderen van verkeersgegevens heeft de wetgever in beginsel een legitiem doel voor ogen, niemand zal immers ontkennen dat dergelijke gegevens een nuttige en soms zelfs belangrijke rol kunnen spelen in het strafvorderlijk onderzoek. Desondanks dient de wetgever een balans te zoeken tussen de privacy van de burger en de inbreukmakende strafvorderlijke bevoegdheden. De overwegingen zouden ervan blijk moeten geven dat men bereid is een evenwicht tussen beiden te garanderen. De mentaliteitsverandering in de politiek waarbij de privacy maar plaats moet maken voor het opsporingsbelang van justitie in het kader van veiligheid en terrorismebestrijding lijkt echter een niet te stoppen tendens en is dan ook niet onopgemerkt gebleven.[176] Aan een kant valt het gezichtspunt van de politiek best te begrijpen, andersom moeten we ons ook realiseren dat de privacy die wij nu inleveren niet zomaar weer aan ons zal worden teruggegeven.

Bij het introduceren van deze nieuwe bevoegdheden heeft het kabinet zich gebaseerd op bepaalde aannames en argumenten die op bepaalde punten verbetering dan wel nuancering behoeven om zo de rechtsbescherming van de burger maximaal te effectueren. Voor wat betreft verkeersgegevens in zijn algemeenheid concludeerden we in paragraaf 5.3 dat deze onlosmakelijk gekoppeld zijn aan het communicatiegeheim, waarbij de interpretatie van de regering evenmin in overeenstemming is met artikel 8 EVRM en de daarbij relevante jurisprudentie. Het beschermingsregime wat men op Europees niveau garandeert vinden we op nationaal constitutioneel niveau helemaal niet terug, daarvoor treffen we aan een wetgever die weigert op de juiste manier daar gestalte aan te geven. Het is vooralsnog vreemd dat voor 'gewone' gevoelige gegevens, zoals informatie met betrekking tot iemands levensovertuiging of gezondheid, de wetgever extra bescherming nodig acht[177] terwijl vergelijkbare informatie even gemakkelijk uit bepaalde soorten van verkeersgegevens kan worden afgeleid maar waar dergelijke extra waarborgen ontbreken. In paragraaf 5.4 constateerden we dat een differentiatie naar privacygevoeligheid voor wat betreft verkeersgegevens een mogelijkheid zou zijn om aan de te beschermen privacybelangen tegemoet te komen. Men zou daarbij onderscheid moeten maken tussen zuivere verkeersgegevens waaraan geen inhoudelijke elementen kleven, verkeersgegevens waaraan (vooraf aan te wijzen) duidelijke inhoudelijke elementen kleven, en verkeersgegevens die samengenomen in een bepaalde context iets over de inhoud van communicatie (en dus over een of meerdere personen wat) kunnen vertellen. Kan veel (gevoelige) informatie over personen uit verkeersgegevens kan worden afgeleid dan dienen de waarborgen daarop te worden afgestemd; te denken valt daarbij aan een verplichte machtiging van de rechter-commissaris en verstrekking alleen wanneer het belang van het onderzoek dit dringend vordert. Tevens dient te worden vermeden dat de opsporingsambtenaar c.q. officier van justitie onbedoeld toegang krijgt tot gegevens die middels een zwaardere bevoegdheid hadden moeten worden verkregen, het is daarbij noodzakelijk om de praktijk zo in te richten dat voorshands duidelijk is met wat voor informatie hij te maken heeft zodat hij de toe te passen bevoegdheden daarop kan afstemmen. Het inschakelen van een onafhankelijke derde die deze afweging maakt lijkt hierbij noodzakelijk, ook dit traject dient te worden voorzien met de nodige waarborgen.

In paragraaf 5.7 is voor wat betreft de voorwaarden waaronder de bevoegdheden kunnen worden uitgeoefend vastgesteld dat het meest discutabele punt ligt bij de uitbreiding van de kring van personen waarover gegevens kunnen worden gevorderd en de lichte voorwaarden waaronder dit kan gebeuren. Als de wetgever meent dat gegevens van niet-verdachten met grote terughoudendheid dienen te worden gevorderd ten opzichte van gegevens van de verdachte(n), dan dient hij deze terughoudendheid ook te garanderen, liefst bij wet. Vooral de hoeveelheid gegevens die gevorderd kan worden biedt ruime mogelijkheden tot het blootleggen van communicatienetwerken van niet-verdachte personen. Justitie zal wellicht in de verleiding komen om gegevens te vorderen over personen, niet omdat er sprake is van enige relatie (op wat voor manier dan ook) tot een misdrijf, maar juist om te constateren of er wellicht van een vorm van betrokkenheid sprake is. Personen ten aanzien van wie geen enkele rol bij het strafbare feit bekend is kunnen zo met zeer ingrijpende opsporingsmethoden worden geconfronteerd. Het zoeken van

rechtvaardiging in het feit dat andere bevoegdheden, zoals de stelselmatige observatiebevoegdheid van 126g Sv, ook geen 'verdachte eis' kennen gaat mijns inziens mank; deze bevoegdheden zijn immers ook niet lichtvaardig in te zetten tegen niet-verdachten zonder dat er sprake is van een kenbare relatie tot het strafbare feit. Een mogelijke samenhang van het (al dan niet bewuste) gedrag van een derde met een strafbaar feit zal (vooraf aan het inzetten van de observatie bevoegdheid) in het algemeen veel ondubbelzinniger aanwezig zijn zodat de geobserveerde veelal zelf als verdachte kan worden aangemerkt. Een lijst van bijvoorbeeld enkel gevoerde telefoongesprekken is in dat opzicht veel minder concreet. Tevens speelt het communicatiegeheim bij deze bevoegdheden geen enkele rol. Ik pleit dan ook voor een duidelijke beperking van de bevoegdheid voor wat betreft niet-verdachte personen, waarbij aansluiting kan worden gezocht bij de beperkingen van de telecommunicatietap bevoegdheid. Men kan hierbij denken aan een nuancering waarbij verkeersgegevens van niet-verdachten alleen mogen worden gevorderd indien het onderzoek dit dringend vordert, om zo uitdrukking te geven aan de terughoudendheid die de officier van justitie dient te betrachten.

Aan de meeste van de hierboven genoemde bezwaren zou eventueel middels wijziging dan wel aanvulling van het Besluit verstrekking gegevens telecommunicatie en het Besluit vorderen gegevens telecommunicatie op een eenvoudige manier tegemoet kunnen worden gekomen zonder dat een directe wetswijziging noodzakelijk is.

Niet de historische ontwikkeling, maar het problematische karakter van verkeersgegevens ten opzichte van, ik zou bijna zeggen, 'ouderwetse' vormen van communicatie rechtvaardigt de noodzaak voor een nadere wettelijke regeling voor dit type gegevens. De wetgever doet er echter goed aan om voor ogen te houden dat de toegenomen opslag en beschikbaarheid van digitale informatie nooit geen vrijbrief zou mogen zijn om zich zo gemakkelijk mogelijk deze informatie eigen te maken. Zeker in combinatie met een bewaarplicht levert dit een vergaarbak aan informatie op die de overheid naar believen zou kunnen gebruiken. 'Big Brother is watching you' zegt men wel eens, het lijkt er op dat de eerste stapjes daadwerkelijk zijn gezet.

LITERATUUR

De gebruikte literatuur is onderverdeeld in de volgende categorieën:

a. Boeken, tijdschriften, en internet
b. Kamerstukken Tweede Kamer der Staten-Generaal (TK)
c. Kamerstukken Eerste Kamer der Staten-Generaal (EK)
d. Staatsbladen van het Koninkrijk der Nederlanden (Stb.)
e. Internationale verdragen en richtlijnen
f. Engels recht
g. Jurisprudentie

a. Boeken, tijdschriften, en internet

Adviescommissie strafrecht Nederlandse Orde van Advocaten, *Preadvies inzake concept wetsvoorstel en concept besluit vorderen gegevens telecommunicatie*, 2000.

Artz, M.J.T., en van Eijk, M.M.M., *Klant in het web: privacywaarborgen voor internettoegang*, Achtergrondstudies en Verkenningen 17, College Bescherming Persoonsgegevens. <www.cbpweb.nl>

Asher, L.F., Ekker, A.H. (Red.), *Verkeersgegevens. Een juridische en technische inventarisatie*, Instituut voor informatierecht, 2003

College Bescherming Persoonsgegevens, *Advies Grondrechten in het digitale tijdperk*. <www.cbpweb.nl>

College Bscherming Persoonsgegevens, *Bedrijven geen verlengde arm Justitie*, 2001. <www.cbpweb.nl>

College Bescherming Persoonsgegevens, *Meer waarborgen en controle nodig bij informatievergaring door politie*, 2001. <www.cbpweb.nl>

Commissie Grondrechten in het Digitale Tijdperk, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2000.

Corstens, G.J.M., *Het Nederlandse strafprocesrecht*, Gouda Quint, 1999.

H. Franken e.a., *Zeven essays over informatie-technologie & recht*, ITeR nr. 63, SDU, 2004.

Koekkoek, A.K., *De Grondwet*, Tjeenk Willink, 2000.

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

Mac Gillavry, E.C., *De voorstellen van de Commissie Mevis: dwangmiddelen*

voor de informatiemaatschappij, NJB 2001, p. 1411-1418

Mevis, P.A.M., *Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*, 2001. <www.justitie.nl>

Nederlandse Vereniging voor Rechtspraak, *Advies inzake het rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij*, Den Haag, 2001. <http://www.nvvr.org>

Politie Rotterdam Rijnmond, *Het gebruik van (historische) verkeersgegevens in de opsporingspraktijk*, 2003

Stratix Consulting, *Bewaren verkeersgegevens door telecommunicatieaanbieders*, 2003. <www.justitie.nl>

Wiemans, P., Stevens, L., Koops, B., *Strafvorderlijke gegevensvergaring nieuwe stijl*, Nederlands Juristenblad 2004, p. 1680-1686.

b. Kamerstukken Tweede Kamer der Staten-Generaal (TK)

TK 2004-2005, 29 441, nr. 8
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), 2e nota van wijziging, vergaderjaar 2004-2005.

TK 2003-2004, 29 441, nr. 2
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), oorspronkelijk voorstel van wet, vergaderjaar 2003-2004.

TK 2001-2002, 28 366, nr. 1.
Kabinetsstandpunt over het rapport Gegevensvergaring in strafvordering van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, vergaderjaar 2001–2002.

TK 2001-2002, 28 353, nr. 3.
Wijziging van het Wetboek van Strafvordering in verband met de regeling van bevoegdheden tot het vorderen van gegevens van instellingen in de financiële sector, mede ter uitvoering van het op 16 oktober 2001 te Luxemburg tot stand gekomen Protocol bij de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de Lid-Staten van de Europese Unie, door de Raad vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie (vorderen gegevens financiële sector), memorie van toelichting, vergaderjaar 2001-2002.

TK 2001-2002, 28 059, nr. 3.
Wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), memorie van toelichting, vergaderjaar 2001-2002.

TK 2001-2002, 28 366, nr. 1
Kabinetsstandpunt over het rapport Gegevensvergaring in strafvordering van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, brief van de minister van justitie aan de Voorzitter van de Tweede Kamer der Staten-Generaal, vergaderjaar 2001-2002.

TK 1998-1999, 25 892, nr. 6.
Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), nota naar aanleiding van het verslag, vergaderjaar 1998-1999.

TK 1997-1998, 25 892, nr. 3.
Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), memorie van toelichting, vergaderjaar 1998-1999.

TK 1996-1997, 25 403, nr. 3.
Wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), memorie van toelichting, vergaderjaar 1996-1997.

TK 1996–1997, 23 251, nr. 15.
Partiele wijziging van het Wetboek van Strafvordering (herziening van het gerechtelijk vooronderzoek), brief van de minister van justitie, vergaderjaar 1996-1997.

TK 1996-1997, 25 533, nr. 3
Regels inzake de telecommunicatie (Telecommunicatiewet), memorie van toelichting, vergaderjaar 1996-1997.

c. Kamerstukken Eerste Kamer der Staten-Generaal (EK)

EK 2003–2004, 28 059, nr. A.
Wijziging van het wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), memorie van antwoord, vergaderjaar 2003-2004.

d. Staatsbladen van het Koninkrijk der Nederlanden (Stb.)

Stb. 2004, 394.
Besluit van 3 augustus 2004, houdende aanwijzing van de gegevens over een gebruiker en het telecommunicatie-verkeer met betrekking tot die gebruiker die van een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst kunnen worden gevorderd (Besluit vorderen gegevens telecommunicatie), Staatsblad van het Koninkrijk der Nederlanden.

Stb. 2004, 395.
Besluit van 3 augustus 2004 tot vaststelling van het tijdstip van inwerkingtreding van de wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), Stb. 2004, 105 en het Besluit vorderen gegevens telecommunicatie, Staatsblad van het Koninkrijk der Nederlanden.

Stb. 2004, 226.
Besluit van 14 mei 2004 tot vaststelling van het tijdstip van inwerkingtreding van de wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van bevoegdheden tot het vorderen van gegevens van instellingen in de financiële sector, mede ter uitvoering van het op 16 oktober 2001 te Luxemburg tot stand gekomen Protocol bij de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de Lid-Staten van de Europese Unie, door de Raad vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie (vorderen gegevens financiële sector), Staatsblad van het Koninkrijk der Nederlanden.

Stb. 2004, 105.
Wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), Staatsblad van het Koninkrijk der Nederlanden.

Stb. 2004, 395.
Besluit van 3 augustus 2004 tot vaststelling van het tijdstip van inwerkingtreding van de wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), Stb. 2004, 105 en het Besluit vorderen gegevens telecommunicatie, Staatsblad van het Koninkrijk der Nederlanden.

Stb. 2000, 71.
Besluit van 26 januari 2000, houdende regels voor de verstrekking van gegevens door aanbieders van openbare telecommunicatienetwerken en -diensten met het oog op het onderzoek van telecommunicatie (Besluit verstrekking gegevens telecommunicatie), Staatsblad van het Koninkrijk der

Nederlanden.

e. Internationale verdragen en richtlijnen

Verdrag inzake bestrijding van strafbare feiten verbonden met elektronische netwerken, 23 november 2001, Traktatenblad 2002, nr. 18

Richtlijn betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), 12 juli 2002, 2002/58/EG.

Richtlijn betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, 15 december 1997, 97/66/EG.

f. Engels recht

Accessing Communications Data Draft Code Of Practice, sectie 3.2, <http://www.homeoffice.gov.uk>

Regulation of Investigatory Powers Act 2000. <http://www.hmso.gov.uk/acts/acts2000/20000023.htm>

Telecommunications Data Protection and Privacy Regulations 1999. <www.legislation.hmso.gov.uk>

g. Jurisprudentie

Europees Hof voor de Rechten van de Mens

25 maart 1998, (Kopp), NJ 2001/459.
25 september 2001 (P.G. & J.H. vs. VK), NJ 2003/670.
2 augustus 1984 (Malone), NJ 1988/534.

Hoge Raad der Nederlanden

7 september 2004, LJN AO9090. <http://www.rechtspraak.nl>

Rechtbank Haarlem

Haarlem, 17 juni 2003, LJN AH9116, <http://www.rechtspraak.nl>

Noten

[1] Mevis, P.A.M., Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek, mei 2001, p. 7.
[2] Richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, artikel 6 lid 1.
[3] Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie, artikel 2 sub b.
[4] Idem, overweging 15.
[5] Verdrag inzake bestrijding van strafbare feiten verbonden met elektronische netwerken, Tr. 2002 nr. 18, art 1 sub d.
[6] Ekker, Anton, Publiekrechtelijke bescherming van verkeersgegevens, in: Asher, L.F., Ekker, A.H. (Red.), Verkeersgegevens. Een juridische en technische inventarisatie, Instituut voor informatierecht, 2003, p. 44.
[7] E.e.a. volgt uit art. 10 GW.
[8] Koekkoek, A.K., De Grondwet, Tjeenk Willink, Deventer, 2000, p. 162.
[9] Idem, p. 162.
[10] Corstens, G.J.M., Het Nederlandse strafprocesrecht, Gouda Quint, 1999, p. 340.
[11] Kamerstukken II 1996-1997, 25 403, nr. 3, p. 10.
[12] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 18.
[13] Wet bescherming persoonsgegevens, art. 1 onder a.
[14] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 87. Zie ook de zinsnede "tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder op het recht op bescherming van de persoonlijke levensfeer prevaleert".
[15] Kamerstukken II 1998-1999, 25 892, nr. 6, p. 31 e.v.
[16] Rechtbank Haarlem, 17 juni, 2003, LJN AH9116, <www.rechtspraak.nl> In dit vonnis werd de afgifte van persoonsgegevens naar aanleiding van een algemeen verzoek door de officier van justitie zonder meer rechtmatig geacht.
[17] Kamerstukken II 1996-1997, 25 533, nr. 3, p. 119.
[18] Artz, M.J.T., en van Eijk, M.M.M., Klant in het web: privacywaarborgen voor internettoegang, Achtergrondstudies en Verkenningen 17, College Bescherming Persoonsgegevens, p. 30. <www.cbpweb.nl>
[19] Idem, p. 57.
[20] Artikel 126n Sv, lid 1.
[21] Artikel 126u Sv, lid 1.
[22] Staatscourant 17 maart 2000, nr 55.
[23] Mevis, P.A.M., Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek, mei 2001, p. 2. <www.justitie.nl>
[24] Idem, p. 6.
[25] Idem, p. 25. Men maakt tevens de constatering dat de verantwoordelijke voor de gegevensverstrekking, niet verwonderlijk, gevrijwaard wil blijven van enige aansprakelijkheid. Er zou dan ook behoefte bestaan bij de verantwoordelijke aan een toets om te beoordelen of het verzoek om gegevens terecht is en afgifte proportioneel zal zijn.
[26] Idem, p. 39.
[27] Idem, p. 38.
[28] Idem, p. 29. De commissie maakt onderscheid tussen "data-mining", waarbij het gaat het om "het ontdekken van zinvolle, eerder onbekende of zelfs onverwachte informatie" middels speciale programmatuur in de gegevens van een database, en registervergelijking waar het gaat om het koppelen van registers om deze te vergelijken dan wel aan te vullen.

[29] Idem, p. 42.

[30] Idem, p. 30.

[31] Idem, p. 44.

[32] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p 203. Mac Gillavry constateert dat in de praktijk het tegenovergestelde gebeurt, juridische knelpunten blijken geen wezenlijk probleem te vormen daar opsporingsambtenaren en verantwoordelijken hun belangen goed op elkaar af weten te stemmen. Het privacybelang van de cliënt delft daarbij veelal het onderspit.

[33] Mevis, P.A.M., Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek, mei 2001, p. 59. Onder identificerende gegevens verstaat de commissie "a. naam, adres, woonplaats en postadres, b. geboortedatum en geslacht, c. administratieve kenmerken, d. in geval van een rechtspersoon, in plaats van de gegevens onder a en b: rechtsvorm en vestigingsplaats."

[34] Idem, p. 56.

[35] Idem, p. 63. Als voorbeeld van "andere gegevens" noemt de Commissie onder meer de zogenaamde locatiegegevens, zoals het gebruik van mobiele diensten maar ook bijvoorbeeld het gebruik van een betaalpas of bibliotheekpas. Hiermee, merkt men op, ontstaat de mogelijkheid om een persoon te gaan volgen op een manier die vergelijkbaar is met de stelselmatige observatie van art. 126g Sv.

[36] Idem, p.57.

[37] Idem, p. 61.

[38] Idem, p. 65. Zie artikel 126ne, lid 1 en 3.

[39] Idem, p. 67.

[40] Idem, p. 68.

[41] Idem, p. 70 e.v.

[42] Kamerstukken II 2001-2002, 28 366, nr. 1, p. 4 e.v.

[43] Idem, p. 13.

[44] NVR, Advies inzake het rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, Den Haag, 22 november, 2001. <http://www.nvvr.org>

[45] Staatsblad 2004, 226.

[46] Staatsblad 2004, 105. Het wetsvoorstel is op 1 september 2004 in werking getreden, Stb. 2004, 395.

[47] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 1-2.

[48] Idem, p. 2-3.

[49] Idem, p. 20.

[50] Kamerstukken II, 2001–2002, 28 366, nr. 1, p. 5.

[51] Zie artikelen 126n lid 1, 126u lid 1 Sv.

[52] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 2. Zie tevens de formulering van het oude artikel 126n, waarbij het gaat om het vorderen van "inlichtingen [...] terzake van alle verkeer dat over een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten, heeft plaatsgevonden".

[53] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 7. Zie tevens artikelen 126n lid 1 en 126u lid 1 Sv.

[54] Idem, p. 7.

[55] Besluit vorderen gegevens telecommunicatie, Staatsblad 2004, 394, p. 1 e.v.

[56] Idem, p. 7.

[57] Idem, p. 7.

[58] Idem, p. 8.

[59] Besluit vorderen gegevens telecommunicatie, Staatsblad 2004, 394, p. 9.

[60] Hoge Raad, 7 september 2004, LJN AO9090. <www.rechtspraak.nl>

[61] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 8.

[62] Kamerstukken I, 2003-2004, 28 059, nr. A, p. 4.
[63] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 7.
[64] Idem, p. 9.
[65] Idem, p. 26.
[66] Idem, p. 10.
[67] Zie artikelen 126n lid 1 sub a/b en 126u lid 1 sub a/b Sv.
[68] Zie artikelen 126n lid 4 en 6, en 126u lid 4 en 6 Sv.
[69] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 10.
[70] Idem, p. 10.
[71] Idem, p. 22.
[72] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 22.
[73] Idem, p. 10.
[74] Kamerstukken II 2004-2005, 29 441, nr. 8, p. 2.
[75] Artikelen 126n lid 5, 126u lid 5 Sv.
[76] Idem.
[77] Zie artikel 126na lid 1 Sv.
[78] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 5.
[79] Idem, p. 11. In dit kader wijzigt het wetsvoorstel ook enkele bepalingen van de Telecommunicatiewet.
[80] Zie de artikelen 126ua lid 2, 126 na lid 2 Sv.
[81] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 12-13.
[82] Idem, p. 13.
[83] Het Besluit verstrekking gegevens telecommunicatie, Staatsblad 2000, 71. Het Besluit is een nadere uitwerking van artikel 13.4 Tw.
[84] Artikel 3 lid 3, artikel 4, Besluit verstrekking gegevens telecommunicatie.
[85] Nota van toelichting, onder art. 4, Staatsblad 2000, 71.
[86] Artikel 11, Besluit verstrekking gegevens telecommunicatie.
[87] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 18.
[88] Zie artikelen 126ua lid 3, 126na lid 3 Sv.
[89] Idem.
[90] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 13, 17.
[91] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 241.
[92] Kamerstukken II 2001-2002, 28 059, nr. 3, p. 13, 27.
[93] Kamerstukken II 2001-2002, 28 353, nr. 3, p. 4.
[94] Idem, p. 5.
[95] Zie de artikelen 126nc en 126uc Sv.
[96] Zie de artikelen 126nd en 126ud Sv.
[97] Zie de artikelen 126nf en 126uf Sv.
[98] Zie artikel 126ne Sv.
[99] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 230.
[100] Kamerstukken II 2001-2002, 28 353, nr. 3., p. 7.
[101] Idem, p. 10.
[102] Idem, p. 8.
[103] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan

strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 334.

[104] DPA1998, <http://www.hmso.gov.uk/>

[105] De DPA 1998 bevat een aantal "data protection principles", waarin ondermeer is te lezen dat "personal data shall be processed fairly and lawfully". Dit wordt in Schedule 1 van de DPA verder uitgewerkt.

[106] DPA 1998, chapter 29, part IV, exemptions, sectie 29. <http://www.hmso.gov.uk/>

[107] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 340.

[108] Telecommunications Data Protection and Privacy Regulations 1999. <www.legislation.hmso.gov.uk>

[109] TDPPR 1999, Section 6, lid 1 sub a t/m c en lid 2.

[110] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 344.

[111] Idem, p. 348.

[112] Idem, p. 353.

[113] RIPA 2000, <http://www.hmso.gov.uk/acts/acts2000/20000023.htm>

[114] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 434.

[115] RIPA 2000, sectie 21, lid 4.

[116] RIPA 2000, sectie 21, lid 4.

[117] RIPA 2000, sectie 21, lid 2 sub a en b, maar ook sectie 1, lid 5 voor de interception warrant.

[118] RIPA 2000, sectie 5 lid 1 sub d

[119] RIPA 2000, sectie 6, lid 1 en 2.

[120] RIPA 2000, sectie 8 lid 1.

[121] RIPA 2000, sectie 9 lid 1 en lid 6.

[122] RIPA 2000, sectie 11 lid 5.

[123] RIPA 2000, sectie 17 lid 1.

[124] Met dank aan Gavin Sutter, LL.M. van het Institute for Computer & Communications Law Centre for Commercial Law Studies, University of London, voor de nadere toelichting hieromtrent.

[125] RIPA 2000, sectie 19.

[126] RIPA 2000, sectie 22, lid 3.

[127] Accessing Communications Data Draft Code Of Practice, sectie 3.2, <http://www.homeoffice.gov.uk>

[128] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 423. Zie tevens RIPA 2000, sectie 22 lid 2 en lid 5. Genoemde doelen betreffen onder meer de nationale veiligheid, of het opsporen van strafbare feiten.

[129] RIPA 2000, sectie 22 lid 8.

[130] RIPA 2000, sectie 22 lid 4.

[131] RIPA 2000, sectie 22 lid 7.

[132] RIPA 2000, sectie 22 lid 2, 4 en 7.

[133] RIPA 2000, sectie 23, lid 1 sub a en b en lid 2 sub a en b.

[134] RIPA 2000, sectie 23, lid 4 en 5.

[135] RIPA 2000, sectie 23, lid 8.

[136] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 428.

[137] RIPA 2000, sectie 67 lid 7, sub a en b.

[138] Mac Gillavry, E.C., Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, Wolf Legal Publishers, 2004, p. 429.

[139] Het is dan ook nog maar de vraag in hoeverre de Engelse opsporingsbevoegdheden in overeenstemming zijn met de eisen die voortvloeien uit het EVRM. Zo is het gebrek aan rechterlijke toetsing, of althans een vergelijkbare zware vorm van bestuurlijk of politiek toezicht, bij het tappen of opvragen van zeer privacygevoelige communicatiegegevens onbegrijpelijk.
[140] Koops, B., Verkeersgegevens en strafrecht, in: Asher, L.F., Ekker, A.H. (Red.), Verkeersgegevens. Een juridische en technische inventarisatie, Instituut voor informatierecht, 2003, p. 68.
[141] Kamerstukken I, 2003–2004, 28-059, nr. A, p. 9.
[142] Kamerstukken I, 2003–2004, 28-059, nr. A, p. 9.
[143] Idem, p. 9.
[144] Commissie Grondrechten in het Digitale Tijdperk, 2000, p. 159 e.v.
[145] College Bescherming Persoonsgegevens, Advies Grondrechten in het digitale tijdperk. <www.cbpweb.nl>
[146] Ekker, A., Publiekrechtelijke bescherming van verkeersgegevens, in: Asher, L.F., Ekker, A.H. (Red.), Verkeersgegevens. Een juridische en technische inventarisatie, Instituut voor informatierecht, 2003, p. 52. Voor wat betreft de wenselijkheid van een nieuw artikel 13 Gw zal in het kader van deze scriptie hieraan verder geen aandacht worden besteed.
[147] Kamerstukken I, 2003–2004, 28-059, nr. A, p. 9.
[148] EHRM, 2 augustus 1984 (Malone), NJ 1988/534.
[149] EHRM, 25 september 2001 (P.G. & J.H. vs. VK), NJ 2003/670. "It is not in dispute that the obtaining by the police of information relating to the numbers called on the telephone in B.'s flat interfered with the private lives or correspondence (in the sense of telephone communications) of the applicants who made use of the telephone in the flat or were telephoned from the flat."
[150] EHRM, 2 augustus 1984 (Malone), NJ 1988/534, nr. 84
[151] Artikel 5, richtlijn privacy en elektronische communicatie, 2002/58/EG.
[152] EHRM, 25 september 2001 (P.G. & J.H. vs. VK), NJ 2003/670, nr. 46.
[153] Dommering, E.J., Telecommunicatie in de jaren negentig: van de Big bang naar een geordend heelal of een nieuw zwart gat?, in: H. Franken e.a., Zeven essays over informatie-technologie & recht, ITeR nr. 63, Den Haag: SDU, p. 212. <http://www.ivir.nl>
[154] Hes, Ronald, Verkeersgegevens in nieuwe generaties telecommunicatiesystemen, in: Asher, L.F., Ekker, A.H. (Red.), Verkeersgegevens. Een juridische en technische inventarisatie, Instituut voor informatierecht, 2003, p. 18.
[155] Een protocol zorgt ervoor dat systemen met elkaar kunnen communiceren. In het Internet model van Hes wordt een onderscheid gemaakt tussen inhoud op applicatieniveau, waarbij het gaat om technische communicatie protocollen waaraan snel inhoudelijke elementen kunnen kleven, en zeer abstracte protocollen die louter betrekking hebben op het aangaan en beëindigen van een verbinding.
[156] Koops, B., Verkeersgegevens en strafrecht, in: Asher, L.F., Ekker, A.H. (Red.), Verkeersgegevens. Een juridische en technische inventarisatie, Instituut voor informatierecht, 2003, p. 69.
[157] Tweede Kamer, 2003–2004, 29 441, nr. 2. Zie de voorgestelde artikelen 126ng/ug lid 2 Sv.
[158] EHRM, 25 maart 1998, (Kopp), NJ 2001/459.
[159] Idem. Zie overweging 72 e.v.; "the law does not clearly state how, under what conditions and by whom the distinction is to be drawn between matters specifically connected with a lawyer's work … and those relating to activity other than that of counsel. Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge …".
[160] Kamerstukken I, 2003–2004, 28-059, nr. A, p. 10
[161] CBP, Meer waarborgen en controle nodig bij informatievergaring door politie, 2001. <www.cbpweb.nl>
[162] CBP, Bedrijven geen verlengde arm Justitie, 2001. <www.cbpweb.nl>
[163] Mac Gillavry, E.C., De voorstellen van de Commissie Mevis: dwangmiddelen voor de informatiemaatschappij, NJB 2001, p. 1413.
[164] Kamerstukken II, 2001–2002, 28 059, nr. 3, p. 7.

[165] Idem, p. 17.
[166] Idem, p. 7.
[167] Kamerstukken II, 1996–1997, 23 251, nr. 15, p. 2.
[168] Corstens, G.J.M., Het Nederlandse strafprocesrecht, Gouda Quint, 1999, p. 420.
[169] Idem, p. 423.
[170] Adviescommissie strafrecht NOVA, Preadvies inzake concept wetsvoorstel en concept besluit vorderen gegevens telecommunicatie, 2000.
[171] Kamerstukken II, Kabinetsstandpunt over het rapport Gegevensvergaring in strafvordering van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, 2001–2002, 28 366, nr. 1, p. 10.
[172] Kamerstukken I, 2003–2004, 28-059, nr. A, p. 7.
[173] Politie Rotterdam Rijnmond, Het gebruik van (historische) verkeersgegevens in de opsporingspraktijk, 2003, p. 5.
[174] Stratix Consulting, Bewaren verkeersgegevens door telecommunicatieaanbieders, 2003, p. 31 e.v. <www.justitie.nl>
[175] Idem, p. 54.
[176] Wiemans, P., Stevens, L., Koops, B., Strafvorderlijke gegevensvergaring nieuwe stijl, Nederlands Juristenblad 2004, p. 1680-1686.
[177] Kamerstukken II, Wetsvoorstel bevoegdheden vorderen gegevens, 2003–2004, 29 441, nr. 2. zie het voorgestelde artikel 126nf Sv.

BIJLAGE 1 – Bevoegdheden vorderen gegevens telecommunicatie, Sv

Artikel 126n

1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, kan de officier van justitie in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker. De vordering kan slechts betrekking hebben op gegevens die bij algemene maatregel van bestuur zijn aangewezen en kan gegevens betreffen die:

a. ten tijde van de vordering zijn verwerkt, dan wel
b. na het tijdstip van de vordering worden verwerkt.

2. Onder een gebruiker van telecommunicatie wordt in dit artikel verstaan de natuurlijke persoon of rechtspersoon die met de aanbieder een overeenkomst is aangegaan met betrekking tot het gebruik van een openbaar telecommunicatienetwerk of de levering van een openbare telecommunicatiedienst, alsmede de natuurlijke persoon of rechtspersoon die daadwerkelijk gebruik maakt van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst.

3. De vordering, bedoeld in het eerste lid, kan worden gericht tot iedere aanbieder van een openbaar telecommunicatienetwerk, onderscheidenlijk iedere aanbieder van een openbare telecommunicatiedienst. Artikel 96a, derde lid, is van overeenkomstige toepassing.

4. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, wordt de vordering gedaan voor een periode van ten hoogste drie maanden.

5. De officier van justitie maakt van de vordering proces-verbaal op, waarin hij vermeldt:

a. het misdrijf en, indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;
b. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, eerste volzin, zijn vervuld;
c. indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon omtrent wie gegevens worden gevorderd;
d. de gegevens die worden gevorderd;
e. indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, de periode waarover de vordering zich uitstrekt.

6. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, wordt de vordering beëindigd zodra niet meer wordt voldaan aan de voorwaarden, bedoeld in het eerste lid, eerste volzin. Van een wijziging, aanvulling, verlenging of beëindiging van de vordering maakt de officier van justitie proces-verbaal op.

7. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld

met betrekking tot de wijze waarop de gegevens door de officier van justitie worden gevorderd.

Artikel 126u

1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker. De vordering kan slechts betrekking hebben op gegevens die bij algemene maatregel van bestuur zijn aangewezen en kan gegevens betreffen die:

a. ten tijde van de vordering zijn verwerkt, dan wel
b. na het tijdstip van de vordering worden verwerkt.

2. Onder een gebruiker van telecommunicatie wordt in dit artikel verstaan de natuurlijke persoon of rechtspersoon die met de aanbieder een overeenkomst is aangegaan met betrekking tot het gebruik van een openbaar telecommunicatienetwerk of de levering van een openbare telecommunicatiedienst, alsmede de natuurlijke persoon of rechtspersoon die daadwerkelijk gebruik maakt van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst.

3. De vordering, bedoeld in het eerste lid, kan worden gericht tot iedere aanbieder van een openbaar telecommunicatienetwerk, onderscheidenlijk iedere aanbieder van een openbare telecommunicatiedienst. Artikel 96a, derde lid, is van overeenkomstige toepassing.

4. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, wordt vordering gedaan voor een periode van ten hoogste drie maanden.

5. De officier van justitie maakt van de vordering proces-verbaal op, waarin hij vermeldt:

a. een omschrijving van het georganiseerd verband;
b. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, eerste volzin, zijn vervuld;
c. indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon omtrent wie gegevens worden gevorderd;
d. de gegevens die worden gevorderd;
e. indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, de periode waarover de vordering zich uitstrekt.

6. Indien de vordering gegevens betreft als bedoeld in het eerste lid, tweede volzin, onder b, wordt de vordering beëindigd zodra niet meer wordt voldaan aan de voorwaarden, bedoeld in het eerste lid, eerste volzin. Van een wijziging, aanvulling, verlenging of beëindiging van de vordering maakt de officier van justitie proces-verbaal op.

7. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de gegevens door de officier van justitie worden gevorderd.

Artikel 126na

1. In geval van verdenking van een misdrijf kan de opsporingsambtenaar in het belang van het onderzoek een vordering doen gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie. Artikel 126n, tweede en derde lid, is van toepassing.

2. Indien de gegevens, bedoeld in het eerste lid, bij de aanbieder niet bekend zijn en zij nodig zijn voor de toepassing van artikel 126m of artikel 126n kan de officier van justitie in het belang van het onderzoek vorderen dat de aanbieder de gevorderde gegevens op bij algemene maatregel van bestuur te bepalen wijze achterhaalt en verstrekt.

3. In geval van een vordering als bedoeld in het eerste of tweede lid is artikel 126n, vijfde lid, onder a, b, c en d, van overeenkomstige toepassing en blijft artikel 126bb buiten toepassing.

4. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de gegevens door de opsporingsambtenaar of de officier van justitie worden gevorderd.

Artikel 126ua

1. In een geval als bedoeld in artikel 126o, eerste lid, kan de opsporingsambtenaar in het belang van het onderzoek een vordering doen gegevens te verstrekken terzake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van telecommunicatie. Artikel 126u, tweede en derde lid, is van toepassing.

2. Indien de gegevens, bedoeld in het eerste lid, bij de aanbieder niet bekend zijn en zij nodig zijn voor de toepassing van artikel 126t of artikel 126u, kan de officier van justitie in het belang van het onderzoek vorderen dat de aanbieder de gevorderde gegevens op bij algemene maatregel van bestuur te bepalen wijze achterhaalt en verstrekt.

3. In geval van een vordering als bedoeld in het eerste of tweede lid is artikel 126u, vijfde lid, onder a, b, c en d, van overeenkomstige toepassing en blijft artikel 126bb buiten toepassing.

4. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot de wijze waarop de gegevens door de opsporingsambtenaar of de officier van justitie worden gevorderd.

BIJLAGE 2

Data Protection Act 1998, chapter 29, part IV Exemptions

29. - (1) Personal data processed for any of the following purposes-

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of any tax or duty or of any imposition of a similar nature,

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

Selecties uit de Regulation of Investigatory Powers Act 2000

Section 5, chapter I, Interception

5. - (1) Subject to the following provisions of this Chapter, the Secretary of State may issue a warrant authorising or requiring the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following-

(a) the interception in the course of their transmission by means of a postal service or telecommunication system of the communications described in the warrant;

(d) the disclosure, in such manner as may be so described, of intercepted material obtained by any interception authorised or required by the warrant, and of related communications data.

(2) The Secretary of State shall not issue an interception warrant unless he believes-

(a) that the warrant is necessary on grounds falling within subsection (3); and
(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary-

(a) in the interests of national security;
(b) for the purpose of preventing or detecting serious crime;
(c) for the purpose of safeguarding the economic well-being of the United

Kingdom;

6. - (1) An interception warrant shall not be issued except on an application made by or on behalf of a person specified in subsection

Section 21, chapter II, Acquisition and disclosure of communications data

(2) Conduct to which this Chapter applies shall be lawful for all purposes if-

(a) it is conduct in which any person is authorised or required to engage by an authorisation or notice granted or given under this Chapter; and
(b) the conduct is in accordance with, or in pursuance of, the authorisation or requirement.

(4) In this Chapter "communications data" means any of the following-

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;
(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person-
(i) of any postal service or telecommunications service; or
(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;
(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

8. - (1) An interception warrant must name or describe either-

(a) one person as the interception subject; or
(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.

9. - (1) An interception warrant-

(a) shall cease to have effect at the end of the relevant period; but
(b) may be renewed, at any time before the end of that period, by an instrument under the hand of the Secretary of State or, in a case falling within section 7(2)(b), under the hand of a senior official.

(2) An interception warrant shall not be renewed under subsection (1) unless the Secretary of State believes that the warrant continues to be necessary on grounds falling within section 5(3).

11. - (1) Effect may be given to an interception warrant either-

(a) by the person to whom it is addressed; or
(b) by that person acting through, or together with, such other persons as he may require (whether under subsection (2) or otherwise) to provide him with assistance with giving effect to the warrant.

(4) Where a copy of an interception warrant has been served by or on behalf of the person to whom it is addressed on-

(a) a person who provides a postal service,
(b) a person who provides a public telecommunications service, or

(5) A person who is under a duty by virtue of subsection (4) to take steps for giving effect to a warrant shall not be required to take any steps which it is not reasonably practicable for him to take.

19. - (1) Where an interception warrant has been issued or renewed, it shall be the duty of every person falling within subsection (2) to keep secret all the matters mentioned in subsection (3).

22. - (1) This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data.

(2) It is necessary on grounds falling within this subsection to obtain communications data if it is necessary-

(a) in the interests of national security;
(b) for the purpose of preventing or detecting crime or of preventing disorder;
(c) in the interests of the economic well-being of the United Kingdom;
(d) in the interests of public safety;
(e) for the purpose of protecting public health;
(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
(h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

(3) Subject to subsection (5), the designated person may grant an authorisation for persons holding offices, ranks or positions with the same relevant public authority as the designated person to engage in any conduct to which this Chapter applies.

(4) Subject to subsection (5), where it appears to the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator-

(a) if the operator is not already in possession of the data, to obtain the data; and
(b) in any case, to disclose all of the data in his possession or subsequently obtained by him.

(7) A person who is under a duty by virtue of subsection (6) shall not be required to do anything in pursuance of that duty which it is not reasonably practicable for him to do.

(8) The duty imposed by subsection (6) shall be enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

23. - (1) An authorisation under section 22(3)-

(a) must be granted in writing or (if not in writing) in a manner that produces a record of its having been granted;
(b) must describe the conduct to which this Chapter applies that is authorised and the communications data in relation to which it is authorised;
(c) must specify the matters falling within section 22(2) by reference to which it is granted; and
(d) must specify the office, rank or position held by the person granting the authorisation.

(2) A notice under section 22(4) requiring communications data to be disclosed or to be obtained and disclosed-

(a) must be given in writing or (if not in writing) must be given in a manner that produces a record of its having been given;
(b) must describe the communications data to be obtained or disclosed under the notice;
(c) must specify the matters falling within section 22(2) by reference to which the notice is given;
(d) must specify the office, rank or position held by the person giving it; and
(e) must specify the manner in which any disclosure required by the notice is to be made.

(4) An authorisation under section 22(3) or notice under section 22(4)-

(a) shall not authorise or require any data to be obtained after the end of the period of one month beginning with the date on which the authorisation is granted or the notice given; and
(b) in the case of a notice, shall not authorise or require any disclosure after the end of that period of any data not in the possession of, or obtained by, the postal or telecommunications operator at a time during that period.

(5) An authorisation under section 22(3) or notice under section 22(4) may be

renewed at any time before the end of the period of one month applying (in accordance with subsection (4) or subsection (7)) to that authorisation or notice.

(6) A renewal of an authorisation under section 22(3) or of a notice under section 22 (4) shall be by the grant or giving, in accordance with this section, of a further authorisation or notice