ERASMUS UNIVERSITEIT ROTTERDAM

Wie wat bewaart die heeft wat

Onderzoek naar nut en noodzaak van een bewaarverplichting voor historische verkeersgegevens van telecommunicatieverkeer

Faculteit der Rechtsgeleerdheid

Inhoudsopgave

1. Inleiding

1.1 De bewaarplicht voor historische verkeersgegevens

In de Wet van 27 mei 1999 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden) (Stb. 1999, 245) is uitvoering gegeven aan de voorstellen van de Parlementaire Enquête Commissie Opsporingsmethoden (PEC). Eén van de opsporingsmiddelen die met de Wet BOB hernieuwde regeling vond in het Wetboek van Strafvordering vormt de bevoegdheid tot het vorderen van inlichtingen omtrent het verkeer dat over een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van telecommunicatiediensten heeft plaatsgevonden (art. 126n/u Sv; het oude art. 125f). Met ingang van 1 september 2004 zijn de artikelen 126n/u vervangen door de artikelen 126n, 126na, 126u en 126ua, die een specifieke regeling geven voor het vorderen van verkeersgegevens en identificerende gegevens.[1]

De bovenomschreven strafvorderlijke bevoegdheden vormen aldus een kader waarin de belangen van de opsporing en de burger op voldoende uitgebalanceerde wijze tegen elkaar afgewogen kunnen worden. Om invulling te kunnen geven aan deze bevoegdheid dient de informatie in de systemen van de aanbieders beschikbaar te zijn. Het strafvorderlijk belang dat aldus wettelijk is verankerd, wordt echter geraakt door de Richtlijn betreffende privacy en elektronische communicatie[2] die het opslaan van persoonsgebonden informatie door aanbieders van telecommunicatienetwerken- en diensten in sterke mate beperkt en daarmee een barrière opwerpt voor de opsporing. Deze beperking weegt in nog sterkere mate daar waar het de Internet Service Providers betreft. De Telecommunicatiewet geeft immers strikte grenzen aan het bewaren van verkeergegevens, waardoor slechts die gegevens bewaard kunnen worden die, kort gezegd, noodzakelijk zijn voor de overbrenging van telecommunicatie en facturering van de geleverde diensten. Deze richtlijn is inmiddels door de nationale wetgevers van de lidstaten in de nationale telecommunicatiewetgevingen geïmplementeerd. Een belangrijk deel van de beschikbare informatie mag dus niet meer worden bewaard en daardoor verliest de opsporing de mogelijkheid om invulling te kunnen geven aan bovengenoemde strafvorderlijke bevoegdheden.

De richtlijn geeft de mogelijkheid om in nationale wetgeving te bepalen dat, ten behoeve van de opsporing en de staatsveiligheid, deze verkeersgegevens niet worden vernietigd.[3] Na de aanslagen in Madrid, in maart 2004, hebben de Europese Ministers van Justitie en Binnenlandse Zaken afgesproken dat het bewaren van deze verkeersgegevens binnen de Unie geharmoniseerd plaats dient te vinden. Een belangrijk argument daarvoor is het versterken van de effectiviteit de wederzijdse rechtshulp bij zware georganiseerde criminaliteit en terreurbestrijding.

---

[1] Staatsblad 2004, 105.
[2] Richtlijn 2002/58/EG.
[3] Richtlijn 2002/58/EG, artikel 1 onder 3.

1.2 Aanleiding voor het onderzoek

Gelet op het bovenstaande heeft de Europese Raad, op 25 maart 2004, de Verklaring betreffende de bestrijding van terrorisme aangenomen. Hierin wordt aangegeven dat maatregelen dienen te worden bestudeerd voor het opstellen van voorschriften voor het bewaren van verkeersgegevens, met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, daaronder begrepen terrorisme, door telecommunicatie-aanbieders.[4] Naar aanleiding hiervan is een ontwerp-kaderbesluit ingediend door Frankrijk, het Verenigd Koninkrijk, Ierland en Zweden over de bewaring van gegevens die zijn verwerkt en opgeslagen in verband met het aanbieden van openbare electronische-communicatiediensten of gegevens in openbare communicatienetwerken met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, daaronder begrepen terrorisme.[5] In het ontwerp wordt een bewaarplicht van ten minste 12 maanden en ten hoogste 36 maanden voorgesteld.[6] Er bestaat in Nederland geen algemene bewaarplicht van verkeers- en gebruiksgegevens. Ingevolge artikel 13.4, tweede lid, van de Telecommunicatiewet bestaat er wel een bewaarplicht voor bepaalde verkeersgegevens voor aanbieders van prepaid-card telefonie. De verplichting geldt voor een periode van drie maanden. Om invulling te kunnen geven aan de bevoegdheid van artikel 126n/u Sv is de opsporing derhalve afhankelijk van de informatie die in de systemen van de aanbieders beschikbaar is.

1.3 Uitvoering van het onderzoek

Bij brief van 23 december 2004 (kenmerk 057/PIDS/2004)) is de Erasmus Universiteit Rotterdam, Faculteit der Rechtsgeleerdheid – in de persoon van mr dr V. Mul – uitgenodigd offerte uit te brengen voor de uitvoering van een onderzoek naar de bewaarplicht voor historische verkeersgegevens bij aanbieders van telecommunicatienetwerken en –diensten en de internet service providers. Het doel van het onderzoek is een bijdrage te leveren ter ondersteuning van het Nederlandse standpunt met betrekking tot het Ontwerp-kaderbesluit van de Europese Unie over de bewaarplicht van gegevens die zijn verwerkt en opgeslagen in verband met het aanbieden van openbare elektronische communicatiediensten of gegevens in openbare communicatienetwerken met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, daaronder begrepen terrorisme. Het dossieronderzoek is uitgevoerd door mr dr V. Mul, mr P.C. Verloop, mr J.H.J. Verbaan en mevr. mr M.C. Bannier met assistentie van mevr. J. Holleman en dhr. H.J. Weisfelt en onder supervisie van prof. mr P.A.M. Mevis. Het onderzoek is verricht onder begeleiding van een daartoe ingestelde begeleidingscommissie.

Het onderzoek is verricht in de periode maart 2005 tot en met mei 2005 en is in verschillende fasen uitgevoerd. Ten behoeve van het onderzoek is door de opdrachtgever een lijst met afgeronde strafzaken aangeleverd. Uit deze lijst is door de onderzoekers een selectie van zaken gemaakt, zowel naar geografische spreiding als naar zaaksgrootte. Daarbij

[4] Verklaring betreffende de bestrijding van terrorisme, Brussel 25 maart 2004, p. 4.
[5] Council of the European Union, Brussel 28 april 2004, 8958/04.
[6] Council of the European Union, Brussel 28 april 2004, 8958/04, art. 4.

zijn zowel Nationale Recherche-, Regionale Recherche- en TGO-zaken aan de orde gekomen als zaken die op districtsniveau zijn gedraaid. Aldus is getracht een goed beeld te krijgen van de rol die historische verkeersgegevens spelen in strafrechtelijke onderzoeken. Tevens is bij deze selectie gekeken naar een onderverdeling tussen zaken waarin gegevens betreffende telecommunicatieverkeer een rol spelen en zaken waarin gegevens betreffende internetverkeer een rol hebben gespeeld. In hoofdstuk 2 zal nader worden ingegaan op de wijze waarop uitvoering is gegeven aan het onderzoek.

2. Onderzoeksverantwoording

2.1 Inleiding

Het onderzoek heeft zich gericht op het nut en de noodzaak van een bewaarplicht van historische verkeersgegevens bij aanbieders van telecommunicatienetwerken en –diensten en de internet service providers. Om nut en noodzaak te kunnen kwantificeren dient enerzijds inzicht te worden geschapen in de samenstelling van de op grond van artikel 126n/u Sv gevorderde verkeersgegevens (welke soort gegevens, leeftijd gegevens) en anderzijds in de invloed die het vorderen van deze verkeersgegevens heeft gehad op de bewijsvergaring in strafrechtelijke onderzoeken.

Dat heeft geleid tot de volgende kernvragen:

- 'Op welke wijze wordt uitvoering gegeven aan de bevoegdheid tot het vorderen van gegevensverkeer en welke knelpunten openbaren zich in dit verband?

- 'Wat zijn de gevolgen van een verruiming van de bewaringstermijn in de praktijk?'

In de onderzoeksopdracht wordt ook aangegeven dat het zwaartepunt van onderhavig onderzoek dient te liggen op verkeersgegevens betreffende internetverkeer en –diensten.

2.2 Onderzoeksvragen

De hierboven geformuleerde kernvragen zijn door de opdrachtgever uitgewerkt in een aantal concrete onderzoeksvragen:

- In welk percentage van de onderzochte zaken heeft het onderzoek aan telecommunicatie (ex art. 126n/u Sv) geresulteerd tot direct bewijs[7]?
- In welk percentage van de onderzochte zaken heeft het onderzoek aan telecommunicatie (ex art. 126n/u Sv) geresulteerd tot indirect bewijs[8]?
- In welk percentage van de onderzochte zaken heeft het ontbreken van verkeersgegevens een negatieve invloed gehad op het verloop van het onderzoek, in termen van directe of indirecte bewijsgaring?
- Wat is het effect van de verruiming van de bewaartermijn op de doorlooptijden van de onderzoeken?
- Wat is de leeftijd van verkeersgegevens op het moment van vordering?

[7] Zie Bijlage 4.
[8] Zie Bijlage 4.

- In welk percentage van de onderzochte zaken zou een verruiming van de bewaarplicht een positieve invloed hebben gehad op het verloop van het onderzoek, in termen van directe of indirecte bewijsgaring?
- Uit welke componenten bestaat "de set" van gevorderde verkeersgegevens in de onderzochte dossiers?
- Wat is de bijdrage per "soort verkeersgegeven" in de onderzochte zaken, in termen van directe of indirecte bewijsgaring?
- Welke gegevens, die in de "de set" van de gevorderde verkeersgegevens ontbraken, zouden een positieve invloed op het verloop van de onderzochte zaken hebben gehad, in termen van directe of indirecte bewijsgaring?

Deze door de opdrachtgever geformuleerde onderzoeksvragen zijn onder te verdelen in drie te onderscheiden categorieën. Enerzijds vragen die op basis van interviews en dossieronderzoek 'harde' onderzoeksresultaten opleveren (leeftijd van de gegevens, componenten van gevorderde gegevens), anderzijds een categorie van vragen waarbij de mening van de geïnterviewden van grote invloed kan zijn op de uitkomsten (negatieve invloed van ontbreken verkeersgegevens, effect van verruiming, positieve invloed van verruiming) en tot slot een categorie van vragen waarbij zowel de mening van de geïnterviewden als dossieronderzoek een rol spelen. Een lijst van de vragen waarlangs het interview werd vormgegeven is als bijlage bijgevoegd.[9]

2.3 Onderzoeksopzet

De onderzoeksmethoden die gedurende het voorgestelde onderzoek zijn gebruikt, variëren per onderzoeksfase.

Fase 1 Literatuuronderzoek
Gedurende fase 1 (de voorbereidingsfase) is de beschikbare literatuur en jurisprudentie verzameld en geanalyseerd. Hiervoor wordt verwezen naar de bijlage waarin een literatuurlijst is opgenomen.[10]

Fase 2 Dossieronderzoek en interviews
Fase twee (het afnemen interviews en dataverzameling) heeft overwegend in het teken van empirisch onderzoek gestaan. Door de opdrachtgever is een eerste selectie van zaken aangeboden aan de onderzoekers. Binnen al deze zaken was door de desbetreffende opsporingsinstantie aangegeven dat het gebruik van historische verkeersgegevens op grond van een vordering ex art. 126n/u (oud), zie bladzijde 9, binnen deze zaken van belang was en in sommige zaken zelfs van essentieel belang is geweest.

Binnen deze zaken is er door de onderzoekers een zo representatief mogelijke selectie gemaakt, waarin zowel zaken op het niveau van de Nationale Recherche en regionale recherche als de districtsrecherche zijn betrokken. Naast de spreiding voor wat betreft het niveau in de politie-organisatie waarop onderzoeken zijn verricht is eveneens voor een

[9] Zie Bijlage 1.
[10] Zie Bijlage 2.

territoriale spreiding van de onderzochte opsporingsonderzoeken gekozen. Hierdoor kon een zo evenwichtig mogelijk beeld ontstaan. De selectie bestaat uit vijfenzestig zaaksdossiers, die tezamen een goede afspiegeling vormen van het gebruik van de bijzondere opsporingsbevoegdheid ex art. 126n/u Sv (oud) .

Het gaat daarbij telkens om strafzaken die reeds onherroepelijk zijn. Slechts ten aanzien van afgedane strafzaken kunnen immers conclusies worden getrokken met betrekking tot de invloed die historische verkeersgegevens hebben gehad op het bewijs.

De onderzoekers hebben deze dossiers bestudeerd en in aansluiting hierop zijn de onderzoeksvragen in interviews voorgelegd aan relevante betrokkenen. Het betreft dan leden van de opsporingsdiensten, in het bijzonder de recherche (teamleiders), die betrokken zijn geweest bij de onderzochte zaaksdossiers, teneinde een inzicht te verkrijgen in het rendement van de toepassing van de bevoegdheid van artikel 126n/u Sv (oud).

Deze wijze van onderzoek geeft een goed beeld van het gebruik van historische verkeersgegevens binnen de opsporing gedurende de laatste jaren. Een nadeel van de gekozen onderzoeksmethode aan de hand van zaaksdossiers ligt in het feit dat er geen onderzoek is verricht naar het aandeel van de historische verkeersgegevens in het totale aantal onderzoeken dat is verricht door de opsporingsinstanties.
Het feit dat er uit de aangeboden selectie 65 zaaksdossiers zijn gevonden waarbinnen het gebruik van historische verkeersgegevens een (belangrijke) rol heeft gespeeld, kan niet leiden tot de wetenschappelijk onderbouwde conclusie dat die gegevens dus van (essentieel) belang zijn voor alle opsporingsonderzoeken. Uit de gehouden interviews kwam wel duidelijk naar voren dat men binnen de opsporing met grote regelmaat gebruik maakt van onderhavige bevoegdheid en dat veel voor de opsporing relevante informatie door middel van deze bevoegdheid verzameld wordt.

Een ander aspect van het dossieronderzoek is inherent aan de wijze waarop een dossier betreffende een strafzaak wordt opgebouwd. In een dergelijk dossier worden immers slechts die zaken opgeschreven c.q. bijgevoegd die van belang zijn geweest voor de desbetreffende zaak. Het is daardoor onmogelijk voor de onderzoekers om uit de bestudering van slechts de dossiers een beeld te krijgen van die gegevens die men niet heeft gekregen, of die vorderingen die geen resultaat hebben opgeleverd voor het onderzoek. Het bovengenoemde aspect heeft ertoe geleid dat de rol die de interviews hebben gespeeld binnen dit onderzoek aanzienlijk is toegenomen.

Wil men wetenschappelijk onderbouwde conclusies trekken over nut en noodzaak binnen de opsporingspraktijk van een bewaartermijn ruimer dan de nu gebruikelijke drie maanden, zou er zicht moeten zijn op het aantal strafrechtelijke onderzoeken die voordeel gehad zouden hebben bij een ruimere bewaartermijn en dus niet opgelost zijn of een langere doorlooptijd hebben gehad vanwege het niet meer aanwezig zijn van historische verkeersgegevens bij de aanbieders. In de aangeleverde opsporingsonderzoeken zijn dergelijke dossiers niet aangetroffen. De geïnterviewden hebben ook geen melding gemaakt van het veelvuldig voorkomen van een hiaat in hun opsporingsactiviteiten door overschrijding van de termijn.

2.4 Onderzoek terzake van internet

Het gebruik van internet is in de afgelopen tijd aanzienlijk toegenomen maar was daarvoor nog een betrekkelijk onbekend medium. De opsporing op het gebied van internet is op dit moment volop in ontwikkeling, maar was tot voorkort ook een betrekkelijk onontgonnen gebied voor de opsporing. Gezien het feit dat er op het moment van het onderzoek nog te weinig afgeronde strafzaken bestonden voor wat betreft de verkeersgegevens betreffende internetverkeer en –diensten is het voor de onderzoekers niet mogelijk geweest om op grond van dossieronderzoek een gefundeerde mening over nut en noodzaak van een bewaarplicht ten aanzien van internetgegevens te formuleren.
Daarom is er voor gekozen om, naast het onderzoek van een aantal dossiers, met een aantal deskundigen op dit gebied binnen de recherche in een aantal interviews en een rondetafelgesprek de behoefte aan internetgegevens binnen de opsporing zowel op dit ogenblik als in de toekomst te peilen. Daarbij is uitgebreid gesproken over de huidige situatie en de mogelijkheden en onmogelijkheden in de toekomst. Voorts is een interview met betrekking tot dezelfde onderwerpen ook afgenomen van een officier van justitie. Dit deel van het onderzoek geeft dus een aantal knelpunten voor en wensen van de opsporing weer ten aanzien van de vastlegging van historische verkeersgegevens met betrekking tot internetverkeer. Deze conclusies volgen met name uit de interviews en gesprekken, maar kunnen niet worden onderbouwd op basis van onderzoek naar reeds afgeronde zaaksdossiers.

2.5 Onderzoek van dossiers: aantallen

Er zijn in het kader van het onderzoek 65 zaaksdossiers bestudeerd. In tabel 2.1 wordt aangegeven hoe de verdeling van de zaken op de verschillende niveaus van opsporing was.

Tabel 2.1 Verdeling zaaksdossiers op niveau van opsporing.

	Aantal zaken	percentage
Nationaal niveau	10	15%
Regionaal niveau	37	57%
District niveau	18	28%
Totaal aantal onderzochte zaken	65	100%

Een verklaring voor het kleinere aantal zaken op nationaal niveau ligt in het feit dat op dat niveau langduriger opsporingsonderzoeken worden verricht dan op regionaal niveau of op het niveau van de districten.

In tabel 2.2 wordt een verdeling getoond ten aanzien van de soort gegevens die in een belangrijke mate een rol hebben gespeeld bij de bewijsvergaring in strafzaken. Uit de tabel

kan worden opgemaakt dat niet in alle onderzochte opsporingsonderzoeken exact was aan te geven welke gegevens een cruciale rol hebben gehad. In sommige zaken waren meerdere soorten gegevens van belang in de bewijsgaring in andere zaken speelde de gegevens die in eerdere onderzoeken waren gevorderd een rol als aanvangsinformatie om een bepaald opsporingsonderzoek in gang te zetten.

Tabel 2.2 Verdeling zaaksdossiers per soort gegeven.

	Aantal zaken	percentage
A- en B-analyse gegevens	34	52%
Locatiegegevens	12	18%
Mastgegevens	8	12%
Meerdere gegevens van belang	11	18%
Totaal aantal onderzochte zaken	65	100%

Opmerking verdient het dat bij de verdeling naar soort van gegevens per zaak door de onderzoekers geen onderscheid is gemaakt voor zover het gaat om direct of indirect verkregen belastend of ontlastend materiaal voortgekomen uit de opgevraagde gegevens. Uit de gehouden interviews is het de onderzoekers gebleken dat dergelijk onderscheid nauwelijks te maken is. De waardering van het bewijs is immers aan de rechter voorbehouden en kan door de onderzoekers niet ingevuld worden op basis van dossieronderzoek en interviews met rechercheurs.

2.6 Vormen van criminaliteit binnen de onderzochte opsporingsonderzoeken.

De onderzochte opsporingsonderzoeken omvatten vele vormen van criminaliteit. Hierbij kan men denken aan levensdelicten, vermogensdelicten, kinderporno, rechtshulpverzoeken, ontvoeringen, verboden wapenbezit, grootschalige fraude en de handel in verdovende middelen. Binnen één enkel opsporingsonderzoek zijn vaak verscheidene vormen van criminaliteit te onderscheiden. Het is dan ook niet mogelijk om percentages van bepaalde vormen van criminaliteit binnen de verrichte onderzoeken weer te geven.

3. Achtergrond van de regeling met betrekking tot historische verkeersgegevens

3.1 Ontwerp Kaderbesluit van 28 april 2004[11]

In navolging van de Verklaring betreffende de bestrijding van het terrorisme, die door de Europese Raad werd aangenomen op 25 maart 2004, is een ontwerp kaderbesluit voorgesteld waarin voorschriften worden opgesteld voor het bewaren van verkeersgegevens door telecommunicatieaanbieders ten behoeve van de opsporing en vervolging van strafbare feiten, waaronder terrorisme. De aldus bewaarde gegevens kunnen aan de andere lidstaten worden verstrekt in overeenstemming met de relevante EU-instrumenten inzake justitiële samenwerking.

In het ontwerp wordt een bewaarplicht voorgesteld voor gegevens van minimaal 12 maanden en maximaal 36 maanden. Uit de definitie, die in de bepaling van artikel 2 van het ontwerp is opgenomen volgt dat onder gegevens zowel verkeersgegevens als locatiegegevens worden verstaan. Dat wil zeggen gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of de facturering daarvan of waarmee de geografische positie van de eindapparatuur van een gebruiker van een algemeen beschikbaar elektronische communicatiedienst wordt aangegeven met inbegrip van de daaraan gerelateerde abonnee- en daaraan gerelateerde gebruikersgegevens. De bewaarplicht strekt zich ook uit tot SMS-, EMS-, MMS- en Internet-verkeersgegevens.

De strekking van het ontwerp is de harmonisatie van de wetgeving, die binnen de lidstaten met betrekking tot het bewaren van gegevens door telecommunicatie-aanbieders geldt, met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten. De doelstelling is effectievere politiële en justitiële samenwerking in strafzaken mogelijk te maken.

3.2 Juridisch kader

In 1971 werd de telefoontap ingevoerd in Nederland. Daarbij werd de inlichtingenplicht voor verkeersgegevens bij telefonie overgeheveld naar artikel 125f Wetboek van Strafvordering (hierna: Sv). Deze bepaling werd destijds in de Memorie van Toelichting nauwelijks gemotiveerd of toegelicht. De Tweede Kamer deed nog een verzoek om een uitvoeriger toelichting en motivering van dit wetsvoorstel, maar de regering beperkte zich tot de opmerking dat het hoofdzakelijk een "verplaatsing" van een reeds lang bestaande bepaling (art. 100 lid 3 Sv oud) betrof welke verplaatsing geen nadere toelichting behoefde.

[11] Zie noot 4.

In 1993 (Wet Computercriminaliteit) en de jaren daarop werd de bevoegdheid herhaaldelijk aangepast aan de veranderende telecomwetgeving maar inhoudelijk veranderde artikel 125f nauwelijks.

De conclusies van het rapport van de Parlementaire Enquête Commissie Opsporingsmethoden (Inzake opsporing) leidden tot de wettelijke regeling van een aantal gebruikte opsporingsmethoden en de daarvoor noodzakelijke bevoegdheden. In 2000 is de bevoegdheid van art. 125f bij de Wet bijzondere opsporingsbevoegdheden (Wet BOB)[12] gewijzigd in het nieuwe art. 126n Sv, terwijl een nieuwe bevoegdheid tot het opvragen van verkeersgegevens in gevallen van een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd, als omschreven in artikel 67, eerste lid, die gezien hun aard of samenhang met andere misdrijven, die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, is ingevoerd in art. 126u Sv.

De Wet BOB dient als grondslag voor opsporingsmiddelen die gepaard gaan met inbreuken op de persoonlijke levenssfeer en de regulering van de inzet van die middelen. Deze middelen worden over het algemeen heimelijk ingezet om informatie te verzamelen die voor het strafrechtelijk onderzoek van belang kan zijn. Met de Wet BOB is getracht de doorzichtigheid van de toepassing van opsporingsbevoegdheden die een inbreuk maken op de persoonlijke levenssfeer te vergroten en geheime, buiten de officier van justitie om toegepaste bevoegdheden uit te bannen. Daarnaast is de controleerbaarheid van de toepassing achteraf vergroot.

De bevoegdheid tot het vorderen van inlichtingen terzake van het telefoonverkeer kwam met invoering van de Wet BOB op 1 februari 2000 als volgt te luiden:

Artikel 126n (oud)

1. In geval van ontdekking op heterdaad, verdenking van een misdrijf als omschreven in artikel 67, eerste lid, of het misdrijf, bedoeld in artikel 138a van het Wetboek van Strafrecht kan de officier van justitie in het belang van het onderzoek een vordering doen inlichtingen te verstrekken terzake van alle verkeer dat over een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten, heeft plaatsgevonden en ten aanzien waarvan het vermoeden bestaat, dat de verdachte eraan heeft deelgenomen.
2. De vordering, bedoeld in het eerste lid, kan worden gericht tot ieder die werkzaam is bij een aanbieder van een openbaar telecommunicatienetwerk, onderscheidenlijk een aanbieder van openbare telecommunicatiediensten.
3. De artikelen 217, 218 en 219 zijn van overeenkomstige toepassing.

Per 1 september 2004 is de Wet Vorderen gegevens telecommunicatie[13] in werking getreden. De bepalingen van artikel 126n en 126u werden aangepast en zulks heeft geresulteerd in het

12 Stb. 1999, 245

13 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, Stb. 2004, 105

onderstaand huidige artikel 126n dat ten aanzien van het onderzoek naar misdrijven in georganiseerd verband nog steeds zijn pendant kent in artikel 126u 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.

Deze wet bevat een aantal belangrijke wijzigingen. Als eerste bevatten de artikelen 126n en 126u Sv sinds de wijziging een nauwkeuriger afgebakende reikwijdte van de bevoegdheid. De vordering behoeft sinds de wetswijziging niet meer alleen betrekking te hebben op de gegevens betreffende het verkeer waarvan kon worden vermoed dat de verdachte er aan deelnam. Ook is er in de wetswijziging een onderscheid gecreëerd tussen historische en

toekomstige gegevens. De wijze waarop een vordering kan worden gedaan wordt geregeld bij Algemene maatregel van Bestuur.[14]

De bevoegdheid tot het vorderen van gegevens betreffende de naam, adres, woonplaats, postcode, nummer en soort dienst van personen die gebruik maken van telecommunicatiewerken of –diensten, de zogenaamde gebruikersgegevens, is geregeld in artikel 126na/ua. Voor de toepassing van deze bevoegdheid is de tussenkomst van de officier van justitie niet vereist. Opsporingsambtenaren kunnen in het belang van het onderzoek naar een gepleegd misdrijf of naar aanleiding van het redelijk vermoeden dat in georganiseerd verband misdrijven als omschreven in artikel 67, eerste lid, worden beraamd of gepleegd, die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren gebruik maken van deze nieuwe bevoegdheid die voor de wetswijziging geacht werd onderdeel uit te maken van de bevoegdheid van art. 126n/u.

3.3 Soorten gegevens

Bij strafvorderlijk onderzoek naar telecommunicatie, gebaseerd op de wetgeving als hierboven beschreven, zijn de volgende categorieën van gegevens van belang.

3.3.1 Gebruikersgegevens

Met verkeersgegevens (artikel 126n/u Sv.) worden bedoeld de gegevens betreffende de gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker. Het begrip verkeersgegevens dat in het Wetboek van Strafvordering wordt gebruikt is ruimer dan het begrip zoals in het verband van de Telecommunicatiewet wordt gehanteerd, omdat het (onder meer) de gebruikersgegevens omvat. Daarnaast gaat het om gegevens die worden verwerkt in verband met het overbrengen van communicatie over een elektronisch communicatienetwerk. De bevoegdheid maakt in zoverre een minder grote inbreuk op de persoonlijke levenssfeer nu het vorderen van gebruikersgegevens er als zodanig niet in resulteert dat een min of meer volledig beeld wordt verkregen van bepaalde aspecten van iemands privé-leven. Daarnaast zijn de gebruikersgegevens ook nodig alvorens andere bevoegdheden kunnen worden toegepast, bijvoorbeeld de bevoegdheid tot het vorderen van verkeersgegevens en de bevoegdheid tot het opnemen van telecommunicatie (art. 126m/t Sv).

3.3.2 Verkeersgegevens

Met verkeersgegevens (art. 126n/u Sv) worden bedoeld gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk.[15] Het gaat

[14] 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, 2004, 394.

om de uiterlijke kenmerken van de telecommunicatie en niet om de inhoud. De artikelen 126n en 126u richten zich derhalve op "wie" er met "wie" contact heeft gehad en niet "wat" er wordt gezegd. Toepassing van de bevoegdheid deze gegevens te vorderen kan erin resulteren dat een min of meer volledig beeld van bepaalde aspecten van iemands privé-leven wordt verkregen.

3.3.3 Locatiegegevens

Onder locatiegegevens worden verstaan gegevens die worden verwerkt in een elektronisch communicatienetwerk waarmee de geografische positie van de randapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven.[16] Bij vaste telefonie moet worden gedacht aan het adres van het desbetreffende netwerkaansluitpunt. Bij mobiele telefonie zal daarbij naar de huidige stand van de techniek moeten worden uit gegaan van de gegevens betreffende de netwerkcel waarbinnen het randapparaat zich bevindt. Van belang is in dit kader dat de gebruiker daadwerkelijk gebruik dient te maken van zijn mobiele telefoon. Er dient met andere woorden communicatie plaats te vinden. Onder locatiegegevens zijn niet begrepen de gegevens betreffende de locatie van een persoon op een moment waarop geen telecommunicatieverkeer plaatsvindt.

3.3.4 Toekomstige gegevens

In aansluiting op bestaande jurisprudentie[17] is in de wijziging van het huidige artikel 126n expliciet opgenomen dat ook toekomstige gegevens binnen de bevoegdheid van dit artikel gevorderd kunnen worden. Indien gegevens worden gevorderd die betrekking hebben op de toekomst, betekent dit dat aan de aanbieder van telecommunicatie wordt gevraagd de gegevens te verstrekken, betreffende telecommunicatieverkeer dat in een komende periode plaats zal gaan vinden. Het kan daarbij gaan om gegevens die de aanbieder op enig moment voor handen heeft, maar die hij wellicht in het kader van de bedrijfsvoering niet zou bewaren. Deze bevoegdheid voorziet niet in een plicht tot medewerking betreffende het vergaren van gegevens die de aanbieder bij de normale bedrijfsuitoefening niet ter beschikking krijgt. Indien gesproken wordt over het bevriezen van verkeersgegevens betreft het slechts toekomstige gegevens. Het bevriezen van deze gegevens is dus geen alternatief voor het generiek opslaan van historische verkeersgegevens.

3.4 Jurisprudentie over de bepalingen van 126n en 126u

De Hoge Raad heeft zich in zijn uitspraak van 7 september 2004[18] al nader uitgelaten wat er onder verkeersgegevens als bedoeld in de artikelen 126n respectievelijk 126u Sv moet worden verstaan. De Hoge Raad stelt in zijn arrest dat inlichtingen omtrent de wijze van totstandkoming en afwikkeling van het telecommunicatieverkeer, zoals de bij het verkeer

15 Artikel 11.1 onder b Telecommunicatiewet.
16 Artikel 11.1 onder d Telecommunicatiewet.
17 Gerechtshof Amsterdam 9 juni 1994, NJ 1994, 710 en HR 7 april 1998, NJ 1998, 559.
18 HR 7 september 2004, NJ 2004, 609.

betrokken aansluitnummers, de gebruikte apparatuur, het tijdstip van de aanvang en de duur van het verkeer en de vraag of daadwerkelijke communicatie heeft plaatsgevonden als verkeersgegevens kunnen worden aangemerkt. Hieronder vallen de gegevens betreffende de locatie van een gebruiker van een telecommunicatiemiddel, indien en voor zover deze het middel daadwerkelijk gebruikt en aan het telecommunicatieverkeer deelneemt. Niet als verkeersgegevens kunnen worden aangemerkt gegevens die betrekking hebben op de inhoud van het telecommunicatieverkeer. Daarmee wordt door de Hoge Raad invulling gegeven aan de definitie die de Telecommunicatiewet geeft.

3.5 Wet bescherming persoonsgegevens

Thans bestaat er nog geen wettelijke verplichting tot het opslaan van historische verkeersgegevens, behoudens de in de bepaling van artikel 13.4 lid 2 Telecommuncatiewet geregelde verplichting om gegevens voor een periode van 3 maanden op te slaan ten aanzien van prepaid abonnementen. Dit betreft echter een beperkte set van gegevens, te weten de tijdstippen waarop telecommunicatie heeft plaatsgevonden, de met die tijdstippen en de desbetreffende telecommunicatie corresponderende nummers en het basisstation waar die gegevens zijn binnen gekomen. De vordering als bedoeld in de artikelen 126n/u beslaat derhalve slechts die gegevens die door de aanbieder van een telecommunicatiedienst of –netwerk ten behoeve van een ander doel, meestal facturering, zijn opgeslagen. De gegevensbeheerder van bedrijven die dergelijke gegevens opslaan, bepaalt derhalve welke gegevens worden opgeslagen en voor welke periode zulks gebeurd. De gegevensverwerking wordt beperkt door de eisen die de Telecommunicatiewet en de Wet bescherming persoonsgegevens daaraan stellen. De gegevenverwerking wordt beperkt door de eisen die in dit hoofdstuk worden gesteld. De aanbieder van een openbaar elektronisch telecommunicatienetwerk of –dienst is verplicht om verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen, te wissen of anoniem te maken wanneer ze niet langer nodig zijn voor het doel van de transmissie van communicatie. Deze verplichting geldt echter niet voor verkeersgegevens die noodzakelijk zijn voor de facturering. Met instemming van de abonnee of gebruiker kunnen de gegevens daarnaast verder worden verwerkt ten behoeve van de marketing van elektronische communicatiediensten (marktonderzoek) of de levering van diensten met een toegevoegde waarde (art. 11.5 Telecommunicatiewet). Verder geldt dat de aanbieders in afwijking van deze verplichtingen gegevens kunnen verwerken indien dat noodzakelijk is in het belang van de opsporing en vervolging van strafbare feiten (art. 11.13, tweede lid van de Telecommunicatiewet)". In een dergelijk geval is dus de verwerking van verkeersgegevens toegestaan ten behoeve van het voldoen aan een vordering van de officier van justitie op grond van de artikelen 126n/u Strafvordering. Zoals hiervoor is opgemerkt kan deze vordering slechts betrekking hebben op de gegevens die ten tijde van de vordering zijn verwerkt dan wel na het tijdstip van de vordering worden verwerkt (art. 126n, eerste lid, Sv). Daarnaast gelden de eisen van de Wet bescherming persoonsgegevens. Gegevens mogen slechts worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (art. 7 Wbp). Op basis van de bepaling van artikel 9 Wbp kunnen de gegevens niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. De gegevensverwerking wordt daarmee beperkt tot de doelen die de aanbieder van de telecommunicatiedienst of het telecommunicatienetwerk zelf zal hebben. De

voorkoming, opsporing en vervolging van strafbare feiten zal geen doel van de aanbieder zijn. Artikel 43 Wpb geeft echter de mogelijkheid voor de aanbieder om, in afwijking van het in artikel 9 Wbp gestelde, gegevens verder te verwerken indien dit noodzakelijk is in het belang van, onder andere, de voorkoming, opsporing en vervolging van strafbare feiten en de veiligheid van de staat.

4. Nut en noodzaak historische verkeersgegevens betreffende telecommunicatie

4.1 Inleiding

In het kader van dit onderzoek is de nadruk gelegd op een inventarisatie van het gebruik van de bevoegdheid van art. 126n/u aan de hand van een aantal zaaksdossiers en beantwoording van de vraag of een verplichte bewaartermijn van verkeersgegevens van invloed zou zijn geweest op de uitkomsten van het desbetreffende opsporingsonderzoek. Bovendien is een inventarisatie gemaakt van de soorten gegevens die worden verstrekt in het kader van het gebruik van de bevoegdheid zoals neergelegd in de bepaling van art. 126n/u. Hierbij dient opgemerkt te worden dat het merendeel van de door de onderzoekers onderzochte zaken zich heeft afgespeeld onder de bevoegdheid van de bepalingen van de artikelen 126n en 126u Sv (oud).

Het verkregen inzicht in de toegevoegde waarde die historische verkeersgegevens bij de bewijsvergaring in strafzaken kunnen hebben, zal in dit hoofdstuk aan de hand van de geformuleerde onderzoeksvragen worden beschreven, waarbij conclusies getrokken worden ten aanzien van het belang van de te onderscheiden verkeersgegevens.

Uitgaande van de invloed die historische verkeersgegevens hebben gehad op het bewijs in strafzaken zal een conclusie worden getrokken ten aanzien van de invloed die een verruiming van de bewaartermijn van historische verkeersgegevens zal hebben op toekomstige strafrechtelijke onderzoeken. In deze conclusie zal getracht worden de kernvragen 'Op welke wijze wordt uitvoering gegeven aan de bevoegdheid tot het vorderen van gegevensverkeer en welke knelpunten openbaren zich in dit verband?' en 'Wat zijn de gevolgen van verruiming van de bewaringstermijn in de praktijk?' te beantwoorden, geplaatst in het terzake geldende juridische kader. Die laatste vraag zal in het kader van dit onderzoek met name worden bezien in het licht van de belangen van de richtige opsporing: welke bewaartermijn voldoet aan de wensen van de opsporende instanties?

Bij de keuze van relevante zaken is een zo representatief mogelijke selectie gemaakt, waarin zowel Nationale en Regionale Rechercheonderzoeken als Team Grootschalige Opsporing-onderzoeken (TGO) en districtszaken zijn betrokken. Zoals in hoofdstuk 2 uiteengezet bestaat deze selectie uit een zestigtal zaaksdossiers die tezamen een goede afspiegeling vormen van het gebruik van de bijzondere opsporingsbevoegdheid ex artikel 126n/u. Daarenboven zijn de onderzoeksvragen in interviews voorgelegd aan relevante betrokkenen. Het betreft hierbij leden van de opsporingsdiensten, in het bijzonder de opsporingsambtenaren werkzaam bij de verschillende recherchediensten die betrokken zijn geweest bij de onderzochte zaaksdossiers teneinde een zo nauwkeurig mogelijk inzicht te verkrijgen in het rendement dat in de praktijk wordt verkregen door de toepassing van de bevoegdheid van artikel 126n/u.

4.2 In welk percentage van de onderzochte zaken heeft het onderzoek aan telecommunicatie (ex art. 126n/u Sv) geresulteerd tot direct dan wel indirect bewijs?

Uit het onderzoek blijkt dat het onderscheid tussen direct en indirect bewijs dat voortgekomen is uit de inzet op grond van de bevoegdheden neergelegd in de bepalingen van de artikelen 126n/u Sv in de meeste zaken die zijn onderzocht niet altijd eenduidig te maken is. Een antwoord op de vraag om in percentages aan te duiden in welke mate de verkeersgegevens direct dan wel indirect bewijs opleverden bleek niet mogelijk. Eén van de oorzaken hiervan is dat slechts in een deel van de vonnissen de bewijsmiddelen waren uitgewerkt. Een andere oorzaak is gelegen in het feit dat verkeersgegevens gebruikt worden in verhoren. Een voorbeeld hiervan is de situatie waarin een verdachte wordt geconfronteerd met de gegevens die zijn verkregen uit de vordering historische verkeersgegevens. Er kunnen dan twee scenario's geschetst worden voor het geval deze gegevens niet in overeenstemming zijn met zijn oorspronkelijke verklaring. Ten eerste kan de verdachte naar aanleiding van deze confrontatie een bekennende verklaring afleggen. Ten tweede kan hij blijven bij zijn oorspronkelijke verklaring en zou deze later door de rechtbank als kennelijk leugenachtig kunnen worden betiteld en op die wijze meewerken aan het bewijs. Daarnaast kan een verklaring van de verdachte die niet overeenkomt met het beeld dat door middel van de verkeersgegevens is verkregen, meewerken in de rechterlijke overtuiging. In het eerste geval zouden de gegevens kunnen worden aangemerkt als indirect bewijs, in het tweede geval, de kennelijke leugenachtigheid van de verklaring van de verdachte, betreft het direct bewijs dat uit de gegevens naar voren is gekomen.

Van de onderzochte zaken heeft de A- en/of B-analyse[19] van telefoongegevens in tweeëndertig opsporingsonderzoeken een rol gespeeld bij het leveren van bewijs. De locatiegegevens hebben in negen zaken geresulteerd in bewijs. Met name in ontvoeringszaken spelen deze gegevens een prominente rol. Met behulp van locatiegegevens kan de locatie waar ontvoerders en hun slachtoffer zich bevinden, worden achterhaald.

ONTVOERING. Een werknemer van een begrafenisondernemer wordt ontvoerd. De begrafenisondernemer belt de politie om aan te geven dat hij gebeld was door de desbetreffende werknemer met een verzoek om het losgeld voor te schieten. De politie kon aan de hand van de gegevens van het mobiele nummer, waarvan door de begrafenisondernemer werd aangegeven dat dit het nummer van zijn werknemer betrof, met behulp van locatiegegevens vaststellen dat hij, de ontvoerde, zich vermoedelijk in Etten-Leur bevond. De locatie kon zelfs tot op de straat exact worden vastgesteld. Onderzoek door een observatie-team heeft dit vermoeden bevestigd. Het slachtoffer kon worden bevrijd en de verdachten konden worden aangehouden.

Onderzoek van de historische gegevens van een zendmast voor telecommunicatie heeft in acht zaken een cruciale rol gespeeld, een mooi voorbeeld van het nut voor de bewijsvoering is een moordzaak in Rotterdam.

[19] Zie Bijlage 4.

MOORD. Op 24 december 2001 wordt een lijk aangetroffen in de kelder van een pand in Rotterdam. Aan de verwondingen is te zien dat het slachtoffer kennelijk door misdrijf om het leven is gekomen. Onderzoek naar het slachtoffer levert een langdurige historie op van seksueel misbruik, door het slachtoffer, van leerlingen van de scholen waar hij werkzaam was en van zijn beide, veel jongere, zusjes gedurende hun hele jeugd. Er zijn diverse taps gezet; daar kwam niets uit. Uit historische gegevens van de mobiele telefoon in gebruik bij de vriend van een van de jongere zusjes van het slachtoffer wel. Uit deze gegevens blijkt dat deze op grond van de historische locatiegegevens op de plaats delict gebracht kan worden op een tweetal tijdstippen: ten tijde van het plegen van het delict en enkele dagen daarvoor (vermoedelijke ten behoeve van een voorobservatie) samen met de medepleger. Uit de A-analyse blijkt dat kort na het plegen van het delict telefonisch contact is geweest met - naar later bleek - de medepleger.

De Rechtbank Rotterdam oordeelde in een bewijsoverweging in haar vonnis in deze zaak: "Kort voordat verdachte tot het plegen van deze brute moord is gekomen is hij in de buurt van de woning van het slachtoffer geweest. Ook is kort voor het plegen van het feit tweemaal met een (mobiele) telefoon van verdachte gebeld naar de telefoon van het slachtoffer."

Zoals reeds onder 2.3 is aangegeven is er in alle aangeleverde zaaksdossiers sprake van het gebruik van historische verkeersgegevens en zijn deze gegevens in alle zaken van belang geweest. Daarnaast is het niet mogelijk een duidelijk onderscheid te maken tussen direct en indirect bewijs en is het derhalve niet mogelijk om conclusies te trekken met betrekking tot percentages zaken waarin het onderzoek van telecommunicatie heeft geresulteerd in direct bewijs.

4.3 In welk percentage van de onderzochte zaken heeft het ontbreken van verkeersgegevens een negatieve invloed gehad op het verloop van het onderzoek, in termen van directe of indirecte bewijsgaring?

De door de opsporing gevraagde gegevens werden in nagenoeg alle onderzochte zaken geleverd. De politie heeft ervaren dat bepaalde verkeersgegevens gedurende een beperkte tijd in de systemen van de aanbieders beschikbaar zijn. Bij het opvragen van deze (set van) gegevens wordt bewust dan wel onbewust met deze termijnen rekening gehouden. Ten aanzien van de verkeersgegevens van prepaid-abonnementen bijvoorbeeld, bestaat er voor een beperkte set van gegevens slechts een bewaarplicht voor de duur van drie maanden. De gevorderde gegevens konden door de aanbieders in alle gevallen volledig worden geleverd. Het onderzoek geeft geen antwoord op de vraag welke andere, voor het onderzoek relevante gegevens niet werden geleverd omdat er door de politie niet naar die gegevens is gevraagd.

Met zekerheid is te stellen dat deze afwezigheid van verlies van gegevens binnen dat proces mede toe te rekenen is aan het anticiperend gedrag van de opsporingsautoriteiten op de op de tijdstippen van de opsporingsonderzoeken door de telecommunicatieaanbieders gehanteerde bewaar- c.q. levertermijn van drie maanden.

In een aantal onderzoeken heeft men over een langere periode gegevens gevorderd dan de gebruikelijke leeftijd van drie maanden. Deze vorderingen betroffen echter in geen van de onderzochte zaken een leeftijd die hoger was dan zes maanden. Deze onderzoeken betroffen over het algemeen langdurige opsporingsonderzoeken naar de georganiseerde criminaliteit met betrekking tot de handel in verdovende middelen.

Het antwoord op de vraag of de opsporingsdiensten de historische verkeersgegevens niet aangeleverd krijgen die betrekking hebben op gegevens ouder dan drie maanden, moet per aanbieder verschillend worden beantwoord. Sommige van de aanbieders van telefonie leveren de gegevens tot een jaar voor het tijdstip van vordering terug, andere aanbieders daarentegen hebben slechts beschikking over de gegevens over een periode van 3 maanden.

Uit de hierboven beschreven verschillen in termijn van opslag van gegevens door de verscheidene aanbieders van telefonie komt naar voren dat hierin een goed argument te vinden is om over te gaan tot het scheppen van eenduidige regels omtrent de bewaartermijn voor alle aanbieders van telefonie. Op deze wijze zou binnen de opsporingsdiensten meer duidelijkheid ontstaan omtrent de vraag over welke periode men gegevens zou kunnen vorderen en dientengevolge zou men ook de zekerheid hebben dat indien die gegevens uit zo een periode worden gevorderd deze daadwerkelijk geleverd zullen worden. Op die manier wordt tevens vastgelegd welke gegevens niet meer bewaard hoeven te worden.

Bij de vraag naar de mening van de opsporingsambtenaren over het nut voor de opsporing van een verruiming van de nu door de aanbieders van telefonie gehanteerde bewaartermijn, dat wil zeggen een termijn die langer is dan drie maanden, geeft het overgrote deel van de geïnterviewden aan dat zij moeite hebben om daar een eenduidig antwoord op te kunnen geven. De antwoorden die door de geïnterviewden op deze vraag werden gegeven zijn onder te verdelen in drie verschillende niveaus, namelijk het niveau van de Nationale Recherche, de regionale recherche en als laatste de districtrecherche.

In een aantal zaken dat bij de Nationale Recherche liep, werd bijvoorbeeld over een periode van drie tot zes maanden de historische verkeersgegevens van de betrokken deelnemers aan het criminele samenwerkingsverband gevorderd. Deze periode is langer dan de gebruikelijke periode waarover verkeersgegevens worden gevorderd.

Zware georganiseerde criminaliteit, fraudeonderzoeken en rechtshulpverzoeken kennen veelal een zeer lange looptijd, vaak meer dan zes maanden. Bij rechtshulpverzoeken geldt dat deze vaak pas na enige tijd na het gepleegde strafbare feit binnenkomen en dat, indien er naar verkeersgegevens wordt gevraagd, niet aan het verzoek kan worden voldaan omdat de ervaring leert dat deze gegevens bij de meeste aanbieders niet meer voorhanden zijn. In overweging 9 bij het Ontwerp Kaderbesluit[20] wordt expliciet verwezen naar de problemen voor de politiële en justitiële samenwerking in strafzaken.

RECHTSHULPVERZOEK XTC-SMOKKEL. Op 25 juli 2002 wordt een vrouw aangehouden op de luchthaven van Sydney (Australië) met ruim 19 kilo XTC tabletten in haar bezit. De vrouw had een Nederlands mobiel telefoonnummer bij zich dat zij direct bij aankomst diende te bellen. Voorts bleek dat door het Hilton-hotel in Sydney een fax was

[20] [20] Council of the European Union, Brussel 28 april 2004, 8958/04, overweging 9, p. 6.

ontvangen ter attentie van de vrouw dat A garant wilde staan voor de betaling van de hotelkosten. Deze fax was verzonden vanuit het Hilton-hotel in Rotterdam. Op de fax werd tevens een telefoonnummer gegeven. Naar aanleiding van vorenstaande werd door de Australische politie op 4 augustus 2002 een rechtshulpverzoek gedaan. Uit de opgevraagde historische verkeersgegevens blijkt dat met het telefoonnummer dat in de fax staat vermeldt in de dagen na het vertrek van de vrouw naar Australië met enige regelmaat midden in de nacht wordt gebeld met het telefoonnummer dat de vrouw bij zich draagt. Daarnaast blijkt er van contact tussen een aantal personen die ook worden gezien op een videoband van het Hilton-hotel te Rotterdam op het tijdstip dat de fax naar Australië wordt gestuurd.

Bij fraudeonderzoeken, onderzoeken naar zware georganiseerde criminaliteit en terreurzaken, worden de verkeersgegevens van alle relevante telefoonnummers die bij aanvang van het onderzoek aanwezig zijn opgevraagd om zo het verloren gaan van die gegevens te voorkomen. Bij telefoonnummers die in een latere fase van het onderzoek bekend worden, kan het dus voorkomen dat de verkeersgegevens van de relevante periode niet meer beschikbaar zijn en dat het onderzoek negatieve invloed ondervindt van het ontbreken van die gegevens.

Op het niveau van districtszaken blijken de opsporingsautoriteiten zich voornamelijk te richten op zaken met een betrekkelijk korte looptijd ('korte klappen') en er bestaat op het districtsniveau dan ook een geringere behoefte aan een ruime bewaartermijn dan die bestaat bij de wat uitgebreidere opsporingsonderzoeken, zoals die op regionaal of landelijk worden verricht. Bij de districten wordt aangegeven dat de termijn van drie maanden voldoende is. Dit komt voort uit het feit dat de zaken die lopen op districtsniveau zich kenmerken door een korte looptijd en aanvangsdatum die kort op de pleegdatum volgt. Dit in tegenstelling tot de zaken die op regionaal en op nationaal niveau worden onderzocht, waarbij de looptijd veelal (veel) langer is.

Daarnaast is uit de interviews gebleken dat op districtsniveau beperkingen in de capaciteit die ten behoeve van een onderzoek kan worden ingezet, volgens de betrokkenen er toe zou leiden dat het opvragen van (veel) meer gegevens momenteel niet gewenst zou zijn. Men zou eerder behoefte hebben aan de mogelijkheid tot concrete vorderingen ex art. 126n/u, bijvoorbeeld omdat niet onmiddellijk na aanvang van het onderzoek historische verkeersgegevens hoeven te worden gevorderd.

Een verruiming van de termijn waarbinnen het vorderen van verkeersgegevens mogelijk is zal hoogst waarschijnlijk leiden tot meer afgewogen vorderingen. Immers zal in de loop van het onderzoek meer duidelijkheid komen welke gegevens relevant kunnen zijn voor het onderzoek en welke niet.

Zoals hierboven reeds is aangegeven, wordt door de politie bij het vorderen van historische verkeersgegevens rekening gehouden met wat men verwacht dat door de aanbieders geleverd kan worden. Het is derhalve niet mogelijk om op basis van het dossieronderzoek onderbouwde conclusies te trekken met betrekking tot percentages zaken waarin het ontbreken van historische verkeersgegevens van invloed is geweest op het verloop van het onderzoek. Dit geldt te meer nu de onderzochte zaaksdossiers steeds strafrechtelijke onderzoeken betreffen waarin historische verkeersgegevens wel een rol hebben gespeeld in de bewijsgaring.

4.4 Wat is het effect van de verruiming van de bewaartermijn op de doorlooptijden van de onderzoeken?

Uit het onderzoek is naar voren gekomen dat er geen problemen worden ondervonden bij de verkrijging van de bij de aanbieders van telecommunicatienetwerken en -diensten opgevraagde historische gegevens. De periode waarover de historische gegevens worden opgevraagd betreft in het algemeen een periode van drie maanden. Deze gegevens worden over het algemeen zonder enig probleem verstrekt door de aanbieders van mobiele en vaste telefonie. Ten aanzien van het verruimen van de huidige gevorderde termijn blijkt dat er door de recherche wordt geanticipeerd op de termijn van drie maanden die door alle telefonie-aanbieders wordt gehanteerd. In de lijn van dit anticiperen, vordert men dientengevolge over het algemeen bij aanvang van het onderzoek direct de historische gegevens van de telefoonaansluitingen die op dat moment relevant lijken te zijn voor dat onderzoek. Iedere dag dat er wordt gewacht met het vorderen van de gegevens gaan er immers mogelijk relevante gegevens verloren. Het is onmogelijk om op een later tijdstip in het onderzoek de verkeersgegevens te verkrijgen die men kan verkrijgen bij de start van het onderzoek.

Tijdens een lopend onderzoek komt het zeer regelmatig voor dat er nieuwe telefoonnummers c.q. nieuwe verdachten naar voren komen waardoor dan wederom de noodzaak bestaat om de historische verkeersgegevens te vorderen. Algemeen kan worden gesteld dat naarmate onderzoeken langer lopen, men steeds verder verwijderd raakt van het tijdstip van het plegen van het delict en of de aanvang van het onderzoek en dit kan problemen veroorzaken met de huidige gebruikelijke termijn van drie maanden.

Voor de goede orde zij hier nogmaals vermeld dat aan de thans gebruikelijke bewaartermijn waarover de historische verkeersgegevens worden gevorderd geen wettelijke verplichting ten grondslag ligt. Met andere woorden, de aanbieders van telecommunicatienetwerken en –diensten zijn verplicht tot het verstrekken van de gegevens die zij hebben opgeslagen, maar niet verplicht tot het opslaan van de verkeersgegevens. Het feit dat aanbieders van telefonie de verkeersgegevens over de gevorderde periode leveren is geen garantie voor het feit dat dit in de toekomst zo zal blijven. Zij slaan deze gegevens op in verband met hun eigen klantenregistratie en de afwikkeling van facturering aan de clientèle van deze aanbieders. Een wettelijke verplichting tot bewaring van verkeersgegevens bestaat momenteel niet.

In het geval een vordering wordt gedaan door de opsporingsinstanties tot het verkrijgen van de verkeersgegevens van bepaalde gebruikers wordt door de aanbieders in voldoende mate aan deze vordering voldaan. De verstrekking zou, in de toekomst problematischer kunnen worden indien geen wettelijke plicht wordt gecreëerd om die gegevens ook daadwerkelijk voor een bepaalde periode op te slaan. Immers: indien er geen verkeersgegevens ten eigen bate beschikbaar zijn bij de aanbieders, wordt de strafvorderlijke bevoegdheid tot het verkrijgen van die gegevens een lege bevoegdheid

In het verleden werd bij de vaste telefoonaansluitingen de B-analyse (de inkomende telefoontjes) van die aansluiting niet meegeleverd door de telecommunicatie-aanbieder. Het

bewaren van deze gegevens is namelijk niet van belang voor de facturering. Dientengevolge moesten alle aanbieders worden aangeschreven om de gegevens van de abonneehouders te vorderen die naar het betreffende telefoonnummer hadden gebeld binnen de periode die werd gevorderd. Recentelijk levert een grote aanbieder de B-analyse wel aan bij een vordering van gegevens van een van zijn abonneehouders. Een verplichting op dit vlak voor alle aanbieders zou echter een efficiëntere aanlevering van gegevens op kunnen leveren, waardoor de opsporing in staat zal kunnen zijn kortere doorlooptijden van gelijksoortige onderzoeken te kunnen realiseren.

Vanuit deze optiek verdient het derhalve aanbeveling een eventuele wettelijke bewaarplicht zodanig vorm te geven dat deze mede een bewaarplicht voor de B-analyse gegevens omvat.

4.5 Wat is de leeftijd van verkeersgegevens op het moment van vordering?

De leeftijd van de verkeersgegevens zo blijkt uit de verrichte interviews is op het moment van vordering zeer uiteenlopend. In een aantal zaken zijn de gegevens die worden opgevraagd nog geen week oud. Dit is met name bij de straatroven het geval. De straatroven worden over het algemeen onderzocht door de districtsrecherche, waarbij het van belang is met een zo beperkt mogelijke politie-inzet zoveel mogelijk zaken ophelderen. In andere zaken worden gegevens gevorderd, die een periode van een half jaar bestrijken. Hierbij kan dan worden gedacht aan grootschalige opsporingsonderzoeken naar zware georganiseerde criminaliteit. Het is de onderzoekers gebleken dat de leeftijd van de historische verkeersgegevens die worden gevorderd over het algemeen gesproken hoger wordt naarmate de ernst van het gepleegde delict en de capaciteit die de opsporing inzet teneinde de zaak op te kunnen helderen, toeneemt.

In het overgrote deel van de onderzochte zaaksdossiers gaat de leeftijd van de gevorderde gegevens niet verder terug dan drie maanden. Uit de interviews is gebleken dat de politie terughoudendheid betracht in het vorderen van grote hoeveelheden historische verkeersgegevens in een zaak. Er wordt getracht een juiste balans te vinden tussen het niet overschrijden van de termijn van drie maanden en dus het "verliezen" van eventueel relevante gegevens enerzijds en het vorderen en verkrijgen van zeer veel, zowel relevante, als irrelevante gegevens anderzijds. Deze gegevens moeten immers allemaal geanalyseerd en verwerkt moeten worden. Daarenboven leeft bij de politie het idee dat het opvragen van verkeersgegevens van bepaalde aansluitingen een inbreuk op de privacy van die desbetreffende personen inhoudt. Er wordt bij de politie dan ook niet al te lichtvoetig met het vorderen van gegevens omgesprongen. De politie probeert voor zover dat binnen haar mogelijkheid ligt de leeftijd van de gevorderde gegevens zo beperkt mogelijk te houden omdat dit zowel de capaciteitsbenutting van de medewerkers van de politie als de inbreuk op de privacy van degene van wie de gegevens gevorderd worden zo beperkt mogelijk houdt.

4.6 In welk percentage van de onderzochte zaken zou een verruiming van de bewaarplicht een positieve invloed hebben gehad op het verloop van het onderzoek, in termen van directe of indirecte bewijsgaring?

De zaken die zijn bestudeerd zijn bijna allemaal opgelost, dankzij of mede dankzij de verkregen historische verkeersgegevens. Tijdens de interviews is gevraagd of men zich zaken kon herinneren waar het onderzoek is stukgelopen op het niet meer aanwezig zijn van historische verkeersgegevens in verband met het overschrijden van de gehanteerde termijn van de aanbieders. Het beeld dat uit de antwoorden ontstond is uit te splitsten naar type onderzoek.
Uit de interviews komt naar voren dat de behoefte aan een ruimere bewaartermijn van verkeersgegevens toeneemt naarmate de zwaarte van de onderzochte strafbare feiten toeneemt. Een bewaartermijn van één jaar, zoals waaraan in Europees kader wordt gedacht, van historische verkeersgegevens zou voornamelijk van belang zijn voor:

-langlopende onderzoeken (naar met name zware (georganiseerde) criminaliteit)
-grootschalige fraudeonderzoeken
-internationale rechtshulpverzoeken
-cold cases
-terrorisme onderzoeken

Uit de interviews komt naar voren dat de langlopende opsporingsonderzoeken voornamelijk uitgevoerd worden door de Nationale Recherche en de regionale recherche.

Tijdens de interviews binnen de Dienst Nationale Recherche Informatie (DNRI) kwam naar voren dat gezien het feit dat de onderzoeken die hier gedaan worden vaak langer dan een jaar duren en er in de loop van het onderzoek vele momenten bestaan van het vorderen van historische gegevens. Er is wel behoefte aan een ruimere termijn van het kunnen vorderen van historische gegevens. DNRI bestrijkt een groot aantal criminaliteitsvelden: onder andere moord en zeden, mensenhandel en mensensmokkel, fraude en overige financiële criminaliteit, milieudelicten, vuurwapens en voertuigcriminaliteit. In het kader van het nieuwe stelsel Bewaken en Beveiligen levert de dienst onder andere dreigingsanalyses en situatierapportages. Maar bovenal verzamelt DNRI nationale- en internationale politie informatie om te zoeken naar dwarsverbanden, zodat de bovenregionale criminaliteit kan worden opgepakt.

DRUGSTRANSPORT. In een van de onderzochte zaken kwam de Nationale Recherche een reeds afgerond drugstransport tegen waar al uitgebreid onderzoek naar was gedaan. Indien de historische verkeersgegevens op dat moment over een periode van één jaar beschikbaar waren geweest met betrekking tot de hoofdverdachte had men dit drugstransport naar alle waarschijnlijkheid direct aan deze verdachte kunnen koppelen. Wanneer dit het geval was geweest zou deze informatie zeer bezwarend zijn geweest voor de verdachte.

Ook uit de gehouden interviews bij de regionale recherche bleek dat er een behoefte bestaat aan een ruimere bewaartermijn. De Regionale Recherche Dienst (RRD) is belast met de

bestrijding van de georganiseerde criminaliteit. Hier is sprake van gecompliceerde misdrijven die min of meer 'bedrijfsmatig' worden gepleegd door criminele netwerken. Voorbeelden hiervan zijn verdovende-middelencriminaliteit, zware milieucriminaliteit, mensenhandel en grootschalige fraudes maar ook levensdelicten en zware zedendelicten. Naast het verrichten van operationele onderzoeken, verleent de RRD specialistische ondersteuning aan het totale rechercheproces.

Uit de onderzochte zaken op het niveau van de districtsrecherche blijkt dat er minder vraag is naar en behoefte aan een ruimere termijn voor de historische verkeersgegevens. Gezien de taakverdeling over de verschillende afdelingen is er binnen de districtsrecherche minder capaciteit voor het analyseren van grote hoeveelheden gegevens en is men meer gericht op de zaken die binnen korte tijd kunnen worden opgelost. Goede voorbeelden hiervan zijn onderstaande onderzoeken betreffende straatroven, diefstal en valse aangifte van GSM-toestellen.

VALSE AANGIFTE STRAATROOF. Na aangifte van diefstal met geweld van een gsm worden de historische verkeersgegevens van het toestel opgevraagd. Uit die gegevens blijkt dat kort voor de beroving de SIM-kaart is gewisseld. Dit impliceert dat het “slachtoffer” de SIM-kaart heeft gewisseld hetgeen kan duiden op een valse aangifte. Dit kan worden geverifieerd door de N.A.W.-gegevens de nieuwe SIM-kaart op te vragen. Degene op wiens naam de nieuwe SIM-kaart staat wordt gehoord door de politie. Deze mevrouw verklaart dat zij de telefoon van aangeefster heeft gekocht op de datum van de zogenaamde beroving. Later had aangeefster haar verteld dat zij aangifte van beroving had gedaan. Aangeefster werd driemaal ontboden maar reageerde niet op deze ontbiedingen. Proces-verbaal van valse aangifte is opgemaakt en de gemaakte kosten voor onderzoek worden op verdachte verhaald.

DIEFSTAL (WONINGINBRAAK). Bij deze woninginbraak zijn onder andere 2 mobiele telefoons weggenomen. De historische verkeersgegevens zijn op grond van de IMEI-nummers aangevraagd. Uit onderzoek van die gegevens bleek dat twee dagen na de woninginbraak voor het eerst wordt gebeld met een van de gestolen telefoons met gebruikmaking van een andere SIM-kaart. Uit het Bedrijfs Processen Systeem van politie blijkt dat het gebruikte 06-nummer gekoppeld staat aan een persoon X.

STRAATROOF/ HELING. In deze zaak loopt de aangever op straat te telefoneren met zijn gsm. Op een gegeven moment wordt de telefoon uit zijn handen gerukt en wordt het slachtoffer omver geduwd. Op grond van de bevoegdheid van artikel 126n worden de historische gegevens gevorderd op basis van het IMEI-nummer. Uit deze gegevens blijkt er dat 3 uur na de beroving met gebruikmaking van een SIM-kaart met nummer XA met de gestolen telefoon gebeld is. Van dit nummer worden de NAW opgevraagd, maar het blijkt een prepaid SIM-kaart te betreffen waar geen persoonsgegevens van beschikbaar zijn. Uit de historische gegevens blijkt dat er regelmatig telefonisch contact tussen bovengenoemd simkaartnummer (XA) en een ander telefoonnummer is (XB) waar ook de persoonsgegevens van worden opgevraagd en verkregen. Uit informatie uit de Gemeentelijk Basis Administratie blijkt op bovengenoemd adres een mevrouw X te wonen. Mevrouw X verklaart dat simkaartnummer XA van haar man is.

Opgemerkt dient te worden dat de hierboven gegeven voorbeelden slechts een afspiegeling vormen van vele soortgelijke zaken die zich op het districtsniveau binnen Nederland voordoen.

Een verruiming van de termijn voor de bewaarplicht zet het strafrechtelijk onderzoek minder onder druk omdat de termijn dat gegevens kunnen worden opgevraagd aan het verstrijken is. Blijkens de interviews worden door de termijn waarbinnen gegevens bewaard blijven nu vaak de verkeersgegevens van alle op het eerste gezicht relevant lijkende telefoonnummers opgevraagd. In een latere fase van het onderzoek zal blijken dat slechts een deel van deze gegevens daadwerkelijk van belang waren. Dat geldt zowel voor het tijdsbestek waarover de gegevens worden opgevraagd als voor bepaalde telefoonnummers waarvan de gegevens worden opgevraagd. Een langere bewaartermijn kan leiden tot een meer afgewogen, beperktere bevraging van de verkeersgegevens.

Ook ten aanzien van deze onderzoeksvraag geldt dat het uitdrukken van de beantwoording van de vraag zich niet laat uitdrukken in een percentage. Nu in de onderzochte zaken de historische verkeergegevens telkens van belang waren voor het onderzoek, valt niet aan te geven in welke percentage van de zaken een verruiming van de bewaarplicht een positieve invloed zou hebben gehad op het verloop van het onderzoek.

4.7 Uit welke componenten bestaat "de set" van gevorderde verkeersgegevens in de onderzochte dossiers?

Met betrekking tot vaste telefonie is uit het onderzoek naar voren gekomen dat de volgende gegevens relevant zijn voor de opsporing en in vrijwel alle onderzochte zaken, indien er een vordering naar historische gegevens wordt gedaan, standaard worden opgevraagd:

-de A-analyse;
-de B-analyse;
-datum, tijd en duur van de verbinding - gegevens omtrent de start en eindtijd van een gesprek.

Met betrekking tot de mobiele telefonie geldt de volgende "standaardset":

-de A-analyse;
-MSISDN (het telefoonnummer) van de betrokkene, en de daaraan gekoppelde unieke identiteit IMSI op de SIMkaart;
-IMEI – de identiteit van het toestel;
-de B-analyse;
-datum, tijd en duur van de verbinding – gegevens omtrent de start en eindtijd van een gesprek;
-de locatiegegevens;
-IMSI, IMEI en locatie van de telefoonnummers door wie de betrokkene wordt gebeld.

Uit de ten behoeve van het onderzoek verrichte interviews, is naar voren gekomen dat de hierboven opgesomde gegevens vrijwel in elk opsporingsonderzoek waarin daartoe een behoefte bestaat als "standaard" set door de opsporingsinstanties worden gevorderd.

Ook is gebleken dat er steeds vaker gegevens worden gevorderd van de, voor het desbetreffende onderzoek relevante, zendmasten voor mobiele telefonie. Op deze wijze kunnen mogelijke verdachten snel worden uitgesloten van verdenking omdat daarmee een indicatie kan worden gegeven dat deze personen zich niet op het relevante tijdstip op de plaats van het delict bevonden.

Uit de interviews kwam naar voren dat de volledigheid van de registratie van gesprekken van zowel de vaste als de mobiele telefonie te wensen overlaat. Voorts bleek tevens dat deze onvolledigheid meestal bij toeval werd ontdekt. De aanbieders van de mobiele telefonie hebben in geen van de gevallen dat de B-analyse onvolledig bleek te zijn, bij het aanbieden van de gegevens zelf melding gemaakt van de mogelijkheid dat de gegevens die werden overhandigd eventueel onvolledig waren. Een verklaring voor de onvolledigheid van de B-analyse gegevens kan zijn dat deze gegevens niet van belang zijn voor de bedrijfsvoering van de aanbieders van de telefonie. Dat wil zeggen dat voor het uitschrijven van facturen aan de desbetreffende abonneehouders het bijhouden van de inkomende gesprekken op een abonneenummer niet noodzakelijk is. Daarenboven worden door de aanbieders van telefonie de gegevens van oproepen die mislukt zijn of niet worden geaccepteerd door de abonneehouder niet bewaard.

Uit de hierboven beschreven verschillen in de volledigheid van afgeleverde gegevens door de aanbieders van de telefonie komt naar voren dat naast het in paragraaf 4.2 genoemde argument om eenduidige regels op te stellen met betrekking tot een vastomlijnde bewaartermijn van gegevens tevens regels dienen te worden gesteld omtrent de soorten van gegevens die binnen die termijn zouden moeten worden opgeslagen. Bovengenoemde duidelijkheid omtrent het opvragen van verkeersgegevens betreffende een bepaalde periode bestaat dan tevens omtrent de gevorderde 'set' van gegevens.

4.8 Wat is de bijdrage per "soort verkeersgegeven" in de onderzochte zaken, in termen van directe of indirecte bewijsgaring?

Gebleken is dat bij de onderzochte zaken voornamelijk de A- en B-analyse hebben geleid tot direct dan wel indirect bewijs . De A- en B-analyse blijken een belangrijk instrument te zijn voor het in beeld brengen van de deelnemers aan criminele organisaties of samenwerkingsverbanden. Bovendien is de onderzoekers gebleken dat een A-analyse en een B-analyse een significante bijdrage leveren bij het verifiëren van de verklaringen die door verdachte, getuigen en of slachtoffers worden afgelegd bij de politie. In termen van direct bewijs zijn de A-analyse- en B-analyse-gegevens met name van belang in het geval er onmiddellijke opsporing plaatsvindt. Voor wat betreft het indirecte bewijs kan worden gesteld dat de A-analyse- en de B-analyse-gegevens van waarde zijn voor het controleren van de verklaringen van betrokkenen zowel in belastende als ontlastende zin.

De locatiegegevens leveren in een aantal opsporingsonderzoeken een zeer nuttige bijdrage aan het bewijs zowel in directe als indirecte zin. Bij bewijs in directe zin dat wordt verkregen door middel van locatiegegevens kan worden gedacht aan het opsporen van gegijzelden bij gijzelingssituaties. Bij het bewijs in indirecte zin kan worden gedacht aan opsporingsonderzoeken waarbij de verklaringen van de betrokkenen kunnen worden gecontroleerd door het opvragen van de locatiegegevens van deze betrokkenen. Uit de interviews kwam naar voren dat de locatiegegevens in een negental opsporingsonderzoeken tot indirect en direct bewijs hebben geleid.

De mastgegevens kunnen slechts in specifieke opsporingsonderzoeken een nuttige bijdrage leveren aan het bewijs. Het betreft met name die gevallen waarbij er geen gebruikers bekend zijn op het moment van aanvang van het onderzoek maar wel bekend is wat de plaats en het tijdstip van het delict is. Hierdoor kunnen de gegevens van de dichtstbijzijnde mast over een zeer kort tijdsbestek worden opgevraagd, waardoor de eventuele gebruikers op die locatie en binnen dat tijdsbestek bekend worden. Vervolgens is het mogelijk op efficiënte en effectieve wijze het abonneenummer van de mogelijke verdachte te achterhalen.

AUTODIEFSTALLEN. In het opsporingsonderzoek naar meerdere diefstallen van zeer dure auto's die in Zeeland werden gepleegd, zijn mastgegevens in de omgeving van het gepleegde delict en rond het tijdstip waarop de auto's vermoedelijk waren weggenomen, opgevraagd. De abonneenummers die via deze mastgegevens werden verkregen konden vervolgens worden gevolgd door middel van het opvragen van de locatiegegevens van de desbetreffende nummers en hierdoor kon een aanzienlijk deel van het bewijs tegen de verdachte worden verzameld.

POGING MOORD. Op 24 juni 1998 wordt er getracht in Rotterdam een persoon te vermoorden. Uit getuigenverklaringen en nader onderzoek blijkt dat de vermoedelijke dader is weggereden in een witte bestelbus, dat hij deze wat verderop in brand heeft gestoken en dat hij vervolgens heeft getracht op een motorfiets te ontkomen. De verdachte kreeg echter de motor niet gestart en is vervolgens gaan liften. Uiteindelijk is hij door een getuige meegenomen vanaf een benzinestation naar Zevenhuizen, waar de verdachte is uitgestapt. Deze getuige verklaart later bij de politie dat de verdachte onderweg naar Zevenhuizen met een mobiele telefoon heeft gebeld.

Vervolgens zijn alle historische verkeersgegevens van de steunpalen (mastgegevens) voor mobiele telefonie gelegen op bovenbeschreven route op 24 juni 1998 tussen 14.00 en 15.00 opgevraagd. Uit analyse bleek dat er op 24 juni tussen 14.00 en 15.00 een viertal keren was gebeld met mobiele telefoon 06-A. met nummers van een "buzzer" en een taxibedrijf. Door het betrokken taxibedrijf wordt verklaard dat op deze dag een man om 15:10 is vervoerd naar de Geleenstraat te Den Haag. Uit het historisch overzicht van telefoonnummer 06-A blijkt tevens dat de gebruiker contact heeft gehad met een tandarts. Uit het patiëntenbestand van de tandarts kan dan de vermoedelijke dader worden geïdentificeerd. Tevens blijkt uit de historische verkeersgegevens dat er gesprekken zijn geweest met een deurwaarderskantoor, waar bij nader onderzoek wederom dezelfde personalia van de genoemde verdachte naar voren komen.

Bij aanvang van het strafrechtelijk onderzoek is het niet mogelijk aan te geven welk verkeersgegeven een rol gaat spelen. Dat leidt ertoe dat telkens een complete set van verkeersgegevens wordt gevorderd. Het is daarom niet mogelijk om tot algemene conclusies te komen over het belang van een bepaald verkeersgegeven uit de set verkeergegevens die wordt gevorderd en geleverd. Op basis van het dossieronderzoek en de interviews kan niet worden geconcludeerd dat er een reden zou zijn om een bewaartermijn te differentiëren per soort verkeersgegeven.

4.9 Welke gegevens, die in de "de set" van de gevorderde verkeersgegevens ontbraken, zouden een positieve invloed op het verloop van de onderzochte zaken hebben gehad, in termen van directe of indirecte bewijsgaring?

Over het algemeen wordt, zoals hierboven reeds is opgemerkt, 'de set' van gevorderde gegevens door de aanbieders van telefonie ook als zodanig aangeleverd. Dit komt doordat 'klassieke' telefonie (zowel vast als mobiel) nog steeds per tijdseenheid wordt afgerekend. De aanbieders hebben de verkeersgegevens nodig voor het in rekening brengen van hun diensten. Zolang de informatie bij de aanbieders beschikbaar is, kan deze voor opsporingsdoeleinden worden gevorderd.

In één geval bleek dat de locatiegegevens ontbraken bij de 'set' terwijl deze wel gevorderd waren. Als oorzaak hiervoor werd door de aanbieder destijds aangegeven dat het niet mogelijk was om locatiegegevens van de mobiele telefoongesprekken te verstrekken. Indien de gegevens wel waren verstrekt, dan was de doorlooptijd van het strafrechtelijk onderzoek mogelijk korter geweest. In de actuelere opsporingsonderzoeken is echter geen sprake meer van het ondervinden van problemen met het aangeleverd krijgen van incomplete 'sets' door de aanbieders van mobiele telefonie. De door de geïnterviewden aangegeven incompleetheid van de 'sets' mag als achterhaald worden aangemerkt.

5. Historische verkeersgegevens met betrekking tot Internet

5.1 Inleiding

In het voorgaande hoofdstuk is het dossieronderzoek naar het nut en de noodzaak van de verruiming van de bewaartermijn van historische verkeersgegevens met betrekking tot het verkeer via telecommunicatienetwerken en –diensten uitgebreid aan de orde gesteld. In het onderhavige hoofdstuk zullen de onder 2.2 geformuleerde onderzoeksvragen met betrekking tot historische verkeersgegevens van het verkeer via internet service providers aan de orde komen. Het ontwerp kaderbesluit van 28 april 2004 (8958/04) stelt immers in artikel 2 lid 3 onder c dat data zoals bedoeld in het kaderbesluit in ieder geval data omvat die wordt gegenereerd door diensten binnen de volgende communicatie-infrastructuren:

c) Internetprotocollen, met inbegrip van e-mail, "voice over internet"-protocollen, World Wide Web, "file transfer"-protocollen, "network transfer"-protocollen, "hyper text"-protocollen, "voice over broadband" en ondergroepen van internetprotocolnummers – "network adress translation"-gegevens.

Daarna wordt nog expliciet aangegeven dat het kaderbesluit niet van toepassing is op de inhoud van de uitgewisselde communicaties.[21]

Alvorens kan worden ingegaan op de bevindingen zoals deze onder meer zijn gebleken aan de hand van het dossieronderzoek en de interviews met betrokken opsporingsambtenaren, verdient een aantal aspecten nadere aandacht.

In de onderzoeksopdracht staat beschreven dat het onderzoek geschiedt op basis van dossieronderzoek en interviews. Het merendeel van de strafzaken waar deze dossiers betrekking op hebben, betreft zaken die onherroepelijk zijn. Een klein aantal zaken is nog niet in alle instanties afgedaan. Nu het voornamelijk strafzaken betreft die reeds zijn afgedaan, houdt dit automatisch in dat het gaat om strafzaken die minimaal een jaar oud zijn. Het is gebleken dat er zich binnen de eerste selectie van zaaksdossiers zoals deze door de opdrachtgever is verricht, slechts een gering aantal zaken bevond waarin historische verkeersgegevens van het internet een rol hebben gespeeld.

Bovendien werd in het kleine aantal zaken waarin verkeersgegevens met betrekking tot internet een rol spelen, veelal slechts een aantal specifiek benoemde gegevens opgevraagd. Hierdoor bleek het op basis van de dossiers en de daaraan gekoppelde interviews onmogelijk om alle onderzoeksvragen te beantwoorden. Zulks heeft onvermijdelijk tot gevolg gehad dat het aantal zaken waarin historische verkeersgegevens met betrekking tot het verkeer via internet service providers een rol heeft gespeeld te gering is gebleken om een wetenschappelijk verantwoorde conclusie te kunnen trekken, op basis van dossieronderzoek, met betrekking tot het nut en de noodzaak van het verruimen van de bewaartermijn van historische verkeersgegevens met betrekking tot internetverkeer. Om toch enige conclusies

[21] Verslag van de Groep justitiële samenwerking in strafzaken, Brussel, 24 februari 2005 (6566/05).

te kunnen trekken, is het onderzoek uitgebreid met een aantal interviews met internetdeskundigen van de politie.

5.2 (Aanloop tot) de huidige werkwijze van de politie

Zoals in het voorgaande reeds vermeld (paragraaf 3.2: juridisch kader) is de vigerende regeling van de artikelen 126n in verbinding met artikel 126na Sv op 1 september 2004 in werking getreden. Tot aan 1 september 2004 stond er geen, althans geen expliciete, bevoegdheid in het Wetboek van Strafvordering noch in enige ten opzichte daarvan bijzondere wet, die aangewend kon worden ter verkrijging van N.A.W.-gegevens. Toch werden in de praktijk wel N.A.W.-gegevens gevraagd en verkregen, al dan niet ingevolge of krachtens enige wettelijke titel.

De opsporingspraktijk bewandelde ter verkrijging van N.A.W.-gegevens verschillende wegen. Gewezen kan worden op het doen van een (tot niets verplichtend) verzoek, waarbij de bevraagde instantie in het verzoek werd gewezen op bepalingen uit (eerst) de Wet persoonsregistraties dan wel (later) de Wet bescherming persoonsgegevens.[22] Ook werden N.A.W.-gegevens wel gevorderd op basis van (eerst) artikel 125f (oud) Sv en (later) artikel 126n (oud) Sv, terwijl die bepaling – ook blijkens jurisprudentie – daartoe geen bevoegdheid bood.[23] Een derde mogelijkheid werd gevonden in de bepaling van artikel 125i Sv, het 'bevel uitlevering geautomatiseerde gegevens'. Deze bevoegdheid was wat omslachtig, nu het bestaan van een gerechtelijk vooronderzoek en – in het kader daarvan – een bevel van de rechter-commissaris vereist waren, terwijl 'slechts' behoefte bestond aan N.A.W.-gegevens en niet aan meer gevoelige gegevens, waartoe een beschermend juridisch kader meer op zijn plaats is.

Vanaf 1 februari 2000 – de datum waarop de Wet herziening GVO in werking is getreden – werd ook wel gebruik gemaakt van artikel 96a Sv, de bevoegdheid tot het doen van een bevel uitlevering ter inbeslagneming, of zelfs van artikel 96c Sv, waarbij de doorzoekingsbevoegdheid dan als een 'goudgerand' uitleveringsbevel dienst deed. Ook deze constructies deden wat gewrongen (want: daar niet voor bedoeld) aan.

Het onderhavige onderzoek, waarbij overwegend afgeronde strafzaken zijn bekeken, heeft logischerwijs betrekking op zaken, die hebben plaatsgevonden op tijdstippen waarop de thans geldende regeling nog niet in werking was getreden.

Zowel tijdens het dossieronderzoek als tijdens de gesprekken die gevoerd zijn met opsporingsambtenaren, hebben de onderzoekers zich (mede) gericht op historische

---

[22] De Wbp (en ook reeds diens voorganger, de Wpr) legt de bevraagde instantie de verplichting op, voordat de gevraagde gegevens worden verstrekt, een belangenafweging te maken tussen enerzijds het (privacy-) belang van de persoon op wie de N.A.W.-gegevens betrekking hebben, anderzijds het belang van de opsporing bij verkrijging van de gegevens. Genoemde wet(ten) bevat(ten) uitdrukkelijk geen bevoegdheid voor de opsporing om gegevens te vorderen o.i.d. ('vragen staat vrij').

[23] Mede de reden voor de totstandkoming van de Wet vorderen gegevens telecommunicatie. Zie ook *Gegevensvergaring in strafvordering*, rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (Commissie-Mevis), mei 2001.

verkeersgegevens met betrekking tot internet. Daarbij is gebleken dat ter verkrijging van het IP-adres (Internet Protocol-adres) vrijwel steeds gebruik is gemaakt van de bevoegdheid van artikel 126n Sv. Via het IP-adres konden de N.A.W.-gegevens van (een) verdachte(n) worden verkregen. Op basis daarvan kon(den) de verdachte(n) worde gelokaliseerd en – vervolgens – worden aangehouden. Ter gelegenheid van de aanhouding kon tevens een doorzoeking plaatsvinden en/of kon de computer in beslag worden genomen, waarmee de strafbare feiten waren begaan.

De internet providers waren in den beginne – wegens het ontbreken van een expliciete bevoegdheid voor de opsporing om IP-adressen dan wel N.A.W.-gegevens te vorderen – minder bereid mee te werken aan verzoeken zijdens de opsporing. Dat leidde tot knelpunten in de opsporing, ook waar het (zeer) ernstige feiten betrof. Tegen die achtergrond zijn tussen de opsporing enerzijds en de providers anderzijds, afspraken gemaakt. Op basis van die afspraken werkten de providers wel steeds mee aan opsporingsonderzoeken naar (het aanbieden dan wel verspreiden van) kinderpornografisch materiaal.

Om vorenstaande reden, betreft het gros der onderzochte zaken onderzoeken naar kinderpornografie (artikel 240b Wetboek van Strafrecht). Daarbij wordt aangegeven dat er wordt gewerkt met 'korte klappen'. Zodra bekend is waar de verdachte zich bevindt, wordt getracht over te gaan tot, in ieder geval, inbeslagneming van de computer van verdachte. In de interviews wordt aangegeven dat het onderzoek in het merendeel van de zaken waarbij historische verkeersgegevens met betrekking tot internetverkeer een rol spelen, aanvangt door een melding via het Landelijk Meldpunt Kinderporno of door meldingen door buitenlandse opsporingsdiensten met betrekking tot de betrokkenheid van Nederlanders bij het aanbieden of verspreiden van kinderporno. Naar aanleiding daarvan wordt binnen het Nederlandse opsporingsonderzoek (kort) naspeuring gedaan naar internetgegevens, waarna over het algemeen wordt ingegrepen. Slechts in een aantal zaken waarin het gaat om het vermoeden van het bestaan van een netwerk van pedofielen, wordt gebruik gemaakt van uitgebreider onderzoek waarbij ook zwaardere opsporingsbevoegdheden worden gebruikt zoals het opnemen van internetverkeer met een technisch hulpmiddel (de internettap, artikel 126m/t Sv). Hierbij wordt opgemerkt dat de politie met het opvragen van de historische verkeersgegevens van het internet, in vergelijking met het vorderen van historische verkeersgegevens van de reguliere telefonie, minder ervaring heeft. Deze bevoegdheid en de verdere technische ontwikkeling van het middel geven nu reeds een toename te zien van het vorderen van historische verkeersgegevens.

Naast onderzoeken naar kinderpornografie spelen historische verkeersgegevens tevens een rol bij onderzoeken naar bedreigingen die via het internet worden geuit. Daarbij kan worden gedacht aan dreigende e-mail berichten, maar ook aan bedreigende teksten op internetsites of discussiefora op het internet. Ook bij deze onderzoeken is het van belang dat het IP-adres van waar de bedreiging is geuit dient te kunnen worden achterhaald. Het is uit dossieronderzoek echter gebleken dat zulks niet altijd mogelijk is.

ANONIEME BEDREIGINGEN. In een aantal zaken waarin via internet bedreigingen zijn geuit (waaronder een tweetal zaken waarbij leden van de Staten-Generaal zijn bedreigd), bleek uit de verkregen IP-adressen dat de bedreigingen op het internet waren geplaatst vanaf openbare plaatsen (scholen, internetcafés). Door het opvragen van de URL's die rond het tijdstip van het plaatsen van de bedreiging waren bezocht, bleek dat even te voren vanaf

hetzelfde IP-adres een Hotmail-adres was bezocht. Door het opvragen van de persoonsgegevens en de IP-adressen die eerder waren gebruikt bij het bezoeken van het Hotmail-adres bij Microsoft (de aanbieder van MSN), kon een huisadres worden achterhaald. Daardoor konden de verdachten worden aangehouden. Geconfronteerd met de onderzoeksbevindingen werd vervolgens door de verdachten een bekennende verklaring afgelegd.

LUCHTHAVEN EELDE. Een zeer sprekend voorbeeld van een soortgelijke zaak heeft gespeeld met betrekking tot een aantal bedreigende mails gericht aan de Luchthaven Eelde. Via de website van de luchthaven was één bericht ontvangen waarin, in gebrekkig engels en ondertekend met een Arabische naam, werd gevraagd om informatie met betrekking tot vlieglessen. Het andere mailbericht betrof een bommelding. Door middel van het opvragen van de IP-adressen van de proxy-servers waarvan de e-mails waren gestuurd, kon worden achterhaald dat de berichten waren gestuurd vanaf computers van een school in Groningen. Daar liep het onderzoek echter vast. De computers konden door alle leerlingen worden gebruikt en er werden geen gegevens bewaard met betrekking tot de tijdstippen waarop door de leerlingen werd ingelogd. Door het opvragen van de logfiles van de proxy-servers kon worden vastgesteld welke websites er waren bezocht voor en na het moment dat de bedreigende e-mail was verzonden. Onder de bezochte websites bevond zich de website van Hotmail met daarbij een inlognaam. Door vervolgens Microsoft te bevragen, konden een aantal gebruikersgegevens worden achterhaald, alsmede de IP-adressen van waar het betreffende Hotmail-adres was bezocht. Onder die IP-adressen bevond zich een "huisadres", op welk "huisadres" één van de leerlingen van de betreffende school woonachtig bleek te zijn. Geconfronteerd met genoemde onderzoeksresultaten werd door de verdachte een bekennende verklaring afgelegd.

Ten aanzien van strafrechtelijke onderzoeken waarbij communicatie via Internet Service Providers plaatsvindt wordt, in vergelijking met onderzoeken waar gegevens met betrekking tot het telefoonverkeer een rol spelen, veelal op andere wijze gebruik gemaakt van de bevoegdheid van artikel 126n/u. Uit de onderzochte dossiers blijkt dat geen gegevens worden gevorderd met betrekking tot de duur van de communicatie, maar dat wel gegevens worden gevorderd met betrekking tot de internetvariant van de A- of B-analyse zoals deze bestaan bij telefoonverkeer. Dit vorderen van de internetvariant van de A- en B-analyse zal volgens de geïnterviewden in de toekomst steeds vaker gaan voorkomen. Uit een aantal onderzochte zaaksdossiers is gebleken dat zonder deze historische verkeersgegevens de identiteitsgegevens van de verdachte niet achterhaald had kunnen worden. Ten aanzien van historische verkeersgegevens met betrekking tot communicatie via Internet Service Providers richten de vorderingen zich in ieder geval op het IP-adres.

Uit het dossieronderzoek bleek dat de door de politie gevorderde gegevens door de Internet Service Providers werden verstrekt, dat daarbij geen praktische beperkingen werden ondervonden en dat de doelstelling van de vordering, het achterhalen van de locatie van de verdachte werd bereikt. De reden daartoe lijkt te zijn gelegen in het feit dat het dan steeds zaken betrof waarin sprake was van zeer schokkende feiten (kinderporno) of waarbij sprake was van grote maatschappelijke onrust. Bovengenoemde zaak 'Luchthaven Eelde' speelde bijvoorbeeld zeer kort na de aanslagen van 9/11.

In interviews werd aangegeven dat de politie een aantal keren om meer verkeersgegevens heeft gevraagd maar dat deze niet werden verstrekt. De betrokken Internet Service Providers verklaarden de gevraagde gegevens niet meer te hebben. Voor de politie is het onmogelijk om na te gaan of de Internet Service Providers inderdaad niet meer in het bezit zijn van die gegevens.
Inmiddels heeft de politie haar vraag afgestemd op hetgeen de providers zeggen te kunnen leveren. Zoals eerder al ten aanzien van de historische verkeersgegevens met betrekking tot telefonie werd opgemerkt, blijkt ook hier sprake van anticiperend gedrag bij de opsporing. In de interviews wordt aangegeven dat de opsporing behoefte kan hebben aan meer verkeersgegevens maar dat er niet om deze gegevens wordt gevraagd nu deze toch niet worden geleverd.

In één dossier wordt melding gemaakt van een vordering tot het verstrekken van actuele inlichtingen op grond van artikel 126n Sv, waarbij door de Internet Service Provider telkens, met een vertraging van enige uren, de gegevens werden geleverd met betrekking tot e-mailverkeer van de verdachte. Daarbij werd door de Internet Service Provider ongevraagd de inhoud van het e-mailverkeer meegeleverd.

In paragraaf 5.4 zal nader worden ingegaan op de mogelijkheden en wensen die binnen de opsporing bestaan ten aanzien van een verplichting tot het bewaren van gegevens met betrekking tot communicatie door middel van Internet Service Providers.

Door de politie werd benadrukt dat een bewaartermijn ten aanzien van de IP-adressen, die noodzakelijk zijn ter identificatie, van groot belang is en dat er jaarlijks een aantal zaken is dat door het niet bewaren van de IP-adressen niet tot vervolging leidt. In een interview werd voorts aangegeven dat in 2004 ongeveer 20 zaken onoplosbaar waren gebleken door het niet bewaren van het IP-adres door de Internet Service Providers. Ten aanzien van deze zaken is geen nader dossieronderzoek verricht. Dit omdat het zeer de vraag is of op basis van onderzoek naar dossiers waar historische verkeersgegevens ontbreken conclusies te trekken zijn ten aanzien van het effect dat het wel aanwezig zijn van de verkeersgegevens zou hebben gehad op de bewijsgaring.

Bij sommige Internet Service Providers blijken gegevens met betrekking tot het IP-adres te verkrijgen die drie maanden oud zijn. Andere aanbieders bewaren deze gegevens niet langer dan een maand. Momenteel lopen er diverse strafrechtelijke onderzoeken waarbij het verkrijgen van de historische verkeersgegevens van internetverkeer, waaronder de internetvariant van de A- en B-analyse en de IP-adressen, van belang is bij het onderzoek.

5.3 Ronde tafel-gesprekken

Naast het dossieronderzoek en de daarbijbehorende interviews met opsporingsambtenaren, is een aantal gesprekken gevoerd met bij de opsporing werkzame deskundigen op het gebied van opsporing op het internet. Nu op basis van het dossieronderzoek geen valide conclusies kunnen worden getrokken ten aanzien van nut en noodzaak van een (verruiming van de) bewaartermijn is besloten om door middel van interviews en een ronde tafel-gesprek meer inzicht te verkrijgen in de problemen die binnen

de opsporing worden ondervonden ten aanzien van het verkrijgen van historische verkeersgegevens met betrekking tot communicatie via internet service providers. Daarbij werd aangegeven dat de vordering ex artikel 126n/u Sv momenteel met name wordt gebruikt om het IP-adres en de N.A.W.-gegevens van de verdachte te verkrijgen.
Door de internetdeskundigen van de politie werd, evenals door de geïnterviewden naar aanleiding van de zaaksdossiers, aangegeven dat er veel discussie plaatsvindt met Internet Service Providers over welke gegevens kunnen worden geleverd. Enige controle of datgene wat geleverd wordt ook inderdaad datgene is wat geleverd zou kunnen worden, is onmogelijk. Volgens de deskundigen van de politie zouden door de Internet Service Providers naast de N.A.W.-gegevens en de gegevens met betrekking tot IP-adressen ook gegevens met betrekking tot de hoeveelheid dataverkeer, het mailverkeer, de soort diensten waarvan gebruik is gemaakt, de inlog op mailboxen en het gebruik van Peer to Peer-diensten, URL's en dergelijke kunnen worden vastgelegd.

Er wordt aangegeven dat de vorderingen qua aantal en qua gevorderde set gegevens beperkt blijven doordat men sterk afhankelijk is van de bereidwilligheid van de Internet Service Providers. Er wordt door de opsporing bij het vorderen van de verkeersgegevens geanticipeerd op wat men verwacht te krijgen. Derhalve kan geen wetenschappelijk onderbouwd oordeel worden gegeven met betrekking tot de binnen de politie bestaande behoefte. Over het algemeen worden er geen gegevens gevraagd die ouder zijn dan drie maanden omdat binnen de opsporing er van wordt uitgegaan dat oudere gegevens door de ISP's in ieder geval niet (kunnen) worden verstrekt. Of deze gegevens wel worden bewaard, is voor de betrokken opsporingsambtenaren niet duidelijk. Daarnaast wordt aangegeven dat de organisatie van de Internet Service Providers, anders dan bij de aanbieders van telecommunicatienetwerken en –diensten, in veel gevallen niet is ingericht op het verlenen van bijstand aan de opsporing. Voor de Internet Service Providers geldt veel minder dan voor de telefonie aanbieders, dat zij ingebed zijn in een systeem waarbij de vastlegging van verkeersgegevens en verstrekking van deze gegevens ten behoeve van de opsporing plaatsvindt. Daarbij geldt te meer dat Internet Service Providers geen verkeersgegevens bewaren ten behoeve van facturering. Of de providers de gegevens eventueel voor andere bedrijfsmatige doeleinden gebruiken is onbekend.

5.4 Toekomst

Binnen de opsporing[24] wordt gesteld dat de politie veel meer de nadruk zal gaan leggen op technisch sporenonderzoek. Het rapport stelt: "dat met de ontwikkelingen van nieuwe technologieën en de onbetrouwbaarheid van de verklaringen van getuigen of verdachten forensische opsporing in termen van bewijsvoering een steeds grotere rol in het strafproces speelt. Technisch bewijs is meer waard dan de verklaring van mensen. Mensen maken fouten, verdachten beroepen zich op hun zwijgrecht, maar de verklaring van technische sporen zijn veel zo niet alles zeggend."

[24] Spelverdeler in de opsporing, Projectgroep Forensische Opsporing, Raad van Hoofdcommissarissen, december 2004.

Het onderzoek naar digitale sporen van een verdachte op het internet is, nu nog, minder gemeengoed. In onderzoeken waarbij materiaal via het internet wordt verspreid, zoals het geval is bij strafbare feiten als de verspreiding van kinderporno, is het al wel een veelgebruikt middel. Ook in andere onderzoeken is een stijgende lijn in het gebruik van onderzoek naar digitale sporen te bespeuren en het valt te verwachten dat dit gebruik in de nabije toekomst zal toenemen. Zoals in het rapport 'Spelverdeler in de opsporing' wordt gesteld, zal het beleid van de opsporing er immers op gericht zijn dat in de nabije toekomst deze sporen een prominentere rol gaan spelen in het strafrechtelijk onderzoek.

Daarbij wordt door de deskundigen van de politie aangegeven dat het internet steeds meer gebruikt wordt bij het plegen van strafbare feiten. Daarbij wordt aangegeven dat het aantal opsporingsonderzoeken waarin historische verkeersgegevens van internetverkeer een rol speelt steeds groter wordt. Een groot aantal nu lopende onderzoeken richt zich op criminaliteit via het internet, waarbij het ontbreken van historische verkeersgegevens een belangrijke belemmering zou kunnen opleveren voor het opsporingsonderzoek. Teneinde de opsporing naar deze strafbare feiten mogelijk te maken, zou het voor de opsporing van belang kunnen zijn als gegevens met betrekking tot dit gebruik van internet gedurende een bepaalde periode bewaard zouden blijven.

Een zeer belangrijke technische ontwikkeling is de opkomst van VoIP, telefonie over het internet. Steeds meer consumenten bellen via hun computer in plaats van via hun vaste of mobiele telefoon. De historische verkeersgegevens die behoren bij dit telefoonverkeer worden, anders dan bij het 'gewone' telefoonverkeer niet door de aanbieders van telefonie opgeslagen. Uit de interviews blijkt dat deze ontwikkeling een belangrijke belemmering opwerpt voor het onderzoek naar strafbare feiten, nu het vaststellen van (telefonische) contacten door het gebruik van VoIP niet mogelijk is, doordat niet duidelijk is of gegevens met betrekking tot dit gebruik bewaard blijven. Een andere technische ontwikkeling die op dit vlak tot belemmeringen zou kunnen leiden, is de opkomst van WiFi (Wireless Fidelity), de techniek waarmee op willekeurige plaatsen ('hot spots' zoals cafés, restaurants, openbare plaatsen) door middel van een laptop-computer contact met het internet kan worden gezocht.

Door de politie wordt aangegeven dat de mogelijkheden die artikel 126n/u Sv momenteel geeft wellicht in de toekomst niet meer voldoende aanknopingspunten biedt voor de opsporing. Daarbij wordt door de deskundigen aangegeven dat steeds vaker gebruik wordt gemaakt van proxy-servers die zich in het buitenland bevinden. Het is dus van belang dat er op internationaal vlak regels worden gesteld ten aanzien van verplichtingen om deze gegevens te bewaren.

Voorts wordt door de politie gesteld dat het opleggen van de bewaarverplichting aan slechts de Internet Service Providers[25] onvoldoende is. Uitgangspunt van de bevoegdheid van art. 126n/u is het behouden blijven van digitale sporen en de mogelijkheid deze te kunnen vorderen ten behoeve van de opsporing. De ISP's kunnen een deel van de benodigde informatie verstrekken, met name ten aanzien van IP-adressen en wellicht ten aanzien van de duur van de communicatie en de hoeveelheid data waaruit de communicatie heeft bestaan. De ISP's hebben veelal geen inzicht in de bezochte URL's of de soort communicatie die

[25] Met de term Internet Service Provider wordt in dit kader gedoeld op Internet Access Providers.

heeft plaatsgevonden, waardoor het met het oog op de opsporing van strafbare feiten zeer nuttig zou zijn als de bewaarverplichting niet slechts ten aanzien van Internet Service Providers zou gelden maar juist ook ten aanzien van andere aanbieders van internettoegang of internetdiensten zoals webhosting-bedrijven, internetcafés, e-mail-diensten en VoIP-diensten. Daarbij wordt aangegeven dat met name een bewaarverplichting ten aanzien van logfiles zou kunnen zorgen voor een veel duidelijker gericht opsporingsonderzoek.

Uit de ronde tafel-bijeenkomst is gebleken dat er binnen de opsporing met name behoefte bestaat aan de volgende gegevens:

-IP-adres: zowel de A-analyse als de B-analyse; daarmee wordt gedoeld op zowel de IP-adressen waar de gebruiker van de internetdienst contact mee heeft gezocht alswel de IP-adressen die contact hebben gezocht met het IP-adres van de gebruiker;
-Datum en tijd van de communicatie;
-Duur van de connectie: dit is van belang bij bijvoorbeeld het gebruik van skype (VoIP) of MSN;
-De hoeveelheid data die wordt ge-upload of gedownload;
-Het soort verkeer; de soort dienst en de gebruikte poorten en nummers;
-De gebruikte e-mailadressen en waar en wanneer het e-mailadres is aangemaakt;
-Logfiles indien gebruik wordt gemaakt van wisselende IP-adressen door het gebruik van een modem;
-Webbezoek (URL).

De bovengenoemde lijst beoogt geen uitputtende opsomming te geven van alle gegevens die van belang zouden kunnen zijn voor de opsporing. Daarbij wordt door de deskundigen aangegeven dat het gebruik van de historische verkeersgegevens met betrekking tot internetverkeer steeds belangrijker zal worden, nu technologische ontwikkelingen het steeds vaker onmogelijk zullen maken om over de inhoud van de communicatie te beschikken. De deskundigen hebben de overtuiging dat een goed overzicht van de historische verkeersgegevens er toe leidt dat het gebruik van zwaardere opsporingsmiddelen, die een grotere inbreuk op de privacy maken, minder (snel) noodzakelijk wordt voor de opsporing van strafbare feiten.

6. Conclusies en aanbevelingen

6.1 Inleiding

Het onderzoek is verricht op basis van vijfenzestig zaakdossiers welke zijn geselecteerd uit een door de behoeftestellers aangeleverd bestand met zaken waarin verkeersgegevens zijn opgevraagd. De zaaksdossiers zijn bestudeerd en er hebben interviews plaatsgevonden met de bij die onderzoeken betrokken opsporingsambtenaren. De conclusies die op basis van dit onderzoek kunnen worden getrokken geven een beeld van de praktijk ten aanzien van het gebruik van de bevoegdheid tot het vorderen van inlichtingen terzake van alle verkeer dat over een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten heeft plaatsgevonden.

De onderzoeksmethode leidt tot een aantal beperkingen die bij de interpretatie van de uitkomsten in het oog moeten worden gehouden. Onderzoek vond plaats op basis van zaaksdossiers waarin gegevens op deels inmiddels gewijzigde wetgeving werden vergaard. Met het vergaren van internetverkeersgegevens is, als gezegd, wel ervaring opgedaan, maar zijn er slechts weinig afgeronde strafzaken ter beschikking. Het is dan ook niet mogelijk gebleken een antwoord te geven op de vraag of historische verkeersgegevens van direct of wellicht van indirect belang voor het bewijs in strafzaken bleken te zijn. Ten slotte schuilt in de onderzoeksvraag ook een voorspellend element: wat zou het verloop en de uitkomst van concrete strafrechtelijke opsporingsonderzoeken zijn geweest als meer mogelijkheden voor vergaring van gegevens voorhanden zouden zijn geweest. Het antwoord op die vraag is onvermijdelijk deels enigszins speculatief.

Nadrukkelijk moet worden opgemerkt dat de vraag naar de wenselijkheid van een bewaarplicht van gegevens gedurende een bepaalde termijn in het onderzoek slechts vanuit een oogpunt van behoefte van de opsporingspraktijk is onderzocht. Het onderzoek geeft geen antwoord op de vraag of zo'n bewaarplicht ook daadwerkelijk invoering verdient. Voor de beantwoording van die algemene vraag dienen meer factoren dan in het onderhavige onderzoek aan de orde zijn gekomen in de afweging te worden betrokken.

Het verdient daarnaast opmerking dat het voor een aantal van de onderzoeksvragen niet mogelijk is onderbouwde conclusies te trekken met betrekking tot de gevraagde percentages van bijvoorbeeld direct en indirect bewijs. Daartoe zou een uitgebreide studie naar de strafvonnissen in de onderzochte zaken noodzakelijk zijn.

6.2 Op welke wijze wordt uitvoering gegeven aan de bevoegdheid tot het vorderen van gegevensverkeer en welke knelpunten openbaren zich in dit verband?

Uit het onderzoek is gebleken dat binnen de opsporing veelvuldig gebruik wordt gemaakt van de bevoegdheid tot het vorderen van historische gegevens ex art. 126n/u Sv. Benevens de door de onderzoekers bestudeerde zaaksdossiers geven de betrokken opsporingsambtenaren in de interviews aan in velerlei zaken de historische gegevens met betrekking tot telecommunicatieverkeer te vorderen.

In nagenoeg alle onderzochte zaken wordt een "standaardset" aan gegevens gevorderd. Deze gevorderde set wordt in bijna alle gevallen ook verkregen. De set bestaat uit informatie over de identiteit van het toestel (IMEI) (bij mobiele telefonie), het telefoonnummer van waar de communicatie plaatsvindt (vast of SIM-kaart), de A-analyse, de B-analyse, het tijdstip en de duur van de verbinding en de locatiegegevens behorende bij de A- en B-analyse (bij mobiele telefonie).

In alle bestudeerde dossiers hebben de historische verkeersgegevens een belangrijke rol gespeeld. Daarbij viel op dat door de politie bij het vorderen van historische verkeersgegevens rekening gehouden wordt met wat men verwacht dat door de aanbieders geleverd kan worden.

Uit het onderzoek is gebleken dat er binnen de opsporing wordt uitgegaan van een, pragmatisch gegroeide, termijn van drie maanden. Gegevens die binnen deze periode worden opgevraagd worden door de telefonieaanbieders nagenoeg altijd verstrekt. Een ruimere bewaartermijn dan deze drie maanden, waarbij de onderzoekers binnen de vraagstelling steeds de in Europees kader voorgestelde minimale termijn van één jaar hebben gehanteerd, zal voornamelijk voor de langlopende opsporingsonderzoeken een gunstig resultaat op kunnen leveren. Ook de zaken waarbij men verder terug in het verleden moet rechercheren, zoals fraudeonderzoeken, hebben baat bij het feit dat men oudere verkeersgegevens kan vorderen.

Om niet het risico te lopen dat verkeersgegevens, die mogelijk belangrijk zijn voor het onderzoek kwijt raken omdat de gebruikelijke bewaartermijn voor deze gegevens drie maanden betreft, worden door de opsporing meer verkeersgegevens gevorderd dan achteraf nodig waren. Dit knelpunt kan worden opgelost door een langere bewaartermijn voor de verkeersgegevens verplicht te stellen. Een langere bewaartermijn zal resulteren in meer afgewogen en specifiekere vorderingen van historische verkeersgegevens.

Een ander knelpunt dat zich voordoet is het niet aanleveren van de B-analyse door de aanbieder van het telefoonnummer waar de vordering op gericht is op het moment dat het een vaste aansluiting betrof. Dit betekent dat de opsporing ten behoeve van het verkrijgen van een B-analyse in een aantal gevallen alle aanbieders diende te benaderen met de vordering tot het verstrekken van die verkeersgegevens waarbij de verdachte betrokken is geweest.

Ten aanzien van historische verkeersgegevens met betrekking tot internetverkeer kan worden gesteld dat momenteel met name gebruik lijkt te worden gemaakt van de mogelijkheid het IP-adres en de daarbij behorende N.A.W.-gegevens te vorderen. Het belang van de A- en B-analyse lijkt echter steeds groter te worden. Deze keuze lijkt echter niet zo zeer te zijn ingegeven door de behoefte die er binnen de opsporingspraktijk bestaat, als wel op de anticipatie op hetgeen momenteel aan gegevens kan worden verkregen. Door de opsporingsambtenaren wordt er, op basis van eerdere ervaringen, vanuit gegaan dat Internet Service Providers niet in staat zullen zijn te voldoen aan een vordering die verder strekt dan ter verkrijging van het IP-adres en de N.A.W.-gegevens. Daarnaast kan worden gezegd dat door de Internet Service Providers aan een vordering ex. art. 126n/u niet altijd wordt voldaan. Er wordt melding gemaakt van een aantal gevallen waarin de gegevens niet bleken te zijn bewaard door de ISP. De leeftijd van de gevorderde IP-adressen was niet hoger dan drie maanden, maar ook aan die vordering kon desondanks niet altijd worden voldaan

De behoefte aan digitaal sporenonderzoek is groot. De toename van het internetgebruik zal leiden tot een toename van het aantal bevragingen van historische verkeersgegevens. Die toename wordt ook ingegeven door technische ontwikkelingen als VoIP, waardoor er een verschuiving optreedt van de klassieke telefonie naar internettelefonie. Bovendien gaat het internetverkeer van verdachten, in de vele gevallen dat er geen internettap loopt, zonder historische verkeersgegevens voor de opsporing verloren. Het ontbreken van die gegevens heeft reeds geleid tot het niet opstarten en het voortijdig afbreken van opsporingsonderzoeken.

6.3 Noopt de praktijk tot verruiming van de bewaringstermijn?

Uit het onderzoek is gebleken dat de opsporingsautoriteiten anticiperend gedrag vertonen in het geval zij een vordering tot het verstrekken van historische gegevens doen. Opsporingsambtenaren blijken zich te laten leiden door de termijn waarvan zij weten dat gegevens door de aanbieders van telecommunicatienetwerken en –diensten worden bewaard. Daarenboven staan opsporingsinstanties huiverig tegenover het vorderen van historische gegevens over een lange termijn. Dit heeft te maken met het besef dat er voor een dergelijke vordering, die immers een inbreuk op de persoonlijke levenssfeer oplevert, een zekere noodzaak aanwezig moet zijn. Voorts leeft binnen de opsporing sterk het besef dat beperkte menskracht met betrekking tot de verwerking en analyse van de gegevens en de politieke druk om veel zaken te behandelen automatisch leidt tot een beperkte tijd om een onderzoek te verrichten. Het verzamelen van (zeer) grote hoeveelheden informatie is dan ook veelal niet van belang voor het oplossen van een concrete strafzaak.

Voor de praktijk kan worden gesteld dat nut en noodzaak van de verruiming van de bewaringstermijn in een op drie niveaus te verdelen antwoord resulteert. De behoefte aan een ruime bewaringstermijn bestaat vooral op het niveau van de Nationale Recherche en mogelijk ook op het niveau van de regionale recherche. Met name op deze niveaus worden de zwaardere zaken behandeld met een bovenregionaal dan wel landelijk karakter zoals onderzoeken naar verdovende- middelencriminaliteit, zware milieucriminaliteit, mensenhandel en grootschalige fraudes maar ook levensdelicten en zware zedendelicten.

Wat geldt ten aanzien van de Nationale Recherche kan ook gelden ten aanzien van buitenlandse rechtshulpverzoeken en voor het onderzoek naar cold cases. Ten aanzien van rechtshulpverzoeken geldt dat de uitvoering van het rechtshulpverzoek veelal een langere periode beslaat dan drie maanden, waardoor de huidige praktijk beperkend kan werken. Dit wringt te meer waar het onderzoeken naar zogenaamde cold cases betreft. Daarvan kan echter worden gezegd dat geen enkele wettelijke bewaartermijn zal voldoen aan de wensen van de praktijk. Ten aanzien van cold cases geldt immers dat te allen tijde sprake is van misdrijven die in een (vaak) ver verleden zijn gepleegd, waardoor zelfs een zeer ruime bewaartermijn altijd het aanzienlijke risico in zich houdt dat er zich een geval zal voordoen waarin de gestelde bewaartermijn niet voldoet.

Op het districtsniveau bestaan de meeste opsporingsonderzoeken die worden verricht daarentegen uit kortlopende onderzoeken. De gevorderde historische verkeersgegevens bestrijken over het algemeen dan ook geen periode die meer tijd omvat dan drie maanden. Daaraan bestaat ook geen behoefte. Voor het oplossen van de strafzaak voldoen over het algemeen de historische verkeersgegevens over een periode van drie maanden. Daarnaast kosten meer gegevens zoveel menskracht dat het rendement van deze gegevens afneemt

Op basis van het verrichte dossieronderzoek kunnen geen conclusies worden getrokken ten aanzien van de vraag of de praktijk van het vorderen van historische verkeersgegevens met betrekking tot internetverkeer noopt tot de vastlegging van een verplichte bewaartermijn voor een bepaalde duur. Uit het onderzoek is wel gebleken dat er binnen de opsporing behoefte bestaat aan uniforme regels met betrekking tot het vastleggen van historische verkeersgegevens van internetverkeer teneinde invulling te kunnen geven aan het gebruik van de bevoegdheid van art. 126n/u. Er zijn momenteel nauwelijks afgeronde zaaksdossiers beschikbaar waaruit kan worden geconcludeerd dat de bevoegdheid van art. 126n/u ten aanzien van Internet Service Providers veel wordt gebruikt. Uit de gehouden interviews is echter een ander beeld gerezen met betrekking tot de huidige situatie. De bevoegdheid van art. 126n/u wordt in lopende onderzoeken ook ten aanzien van Internet Service Providers regelmatig gebruikt.

Er is wel gebleken dat binnen de opsporing een aantal wensen leeft ten aanzien van een bewaarverplichting van historische verkeersgegevens met betrekking tot internetverkeer. Daarbij wordt expliciet aangegeven dat deze verplichting er toe zou kunnen leiden dat de inzet van zwaardere opsporingsmiddelen in voorkomende gevallen achterwege zou kunnen blijven als het opsporingsonderzoek op basis van historische verkeersgegevens zou kunnen worden verricht.

6.4 Aanbevelingen

Uit het onderzoek blijkt dat er binnen de opsporing behoefte bestaat aan uniforme regels met betrekking tot het vastleggen van historische verkeersgegevens van telefonie- en internetverkeer ten einde invulling te kunnen geven aan het gebruik van de bevoegdheid van art. 126n/u.

Doordat er momenteel geen verplichting bestaat voor de aanbieders van telecommunicatie en Internet Service Providers tot het opslaan van verkeersgegevens bestaan er verschillen tussen de geleverde gegevens van de verschillende aanbieders. Het verdient dan ook aanbeveling een eenduidige verplichting te scheppen voor alle aanbieders van telecommunicatie en internettoegang en –diensten tot het opslaan van een "standaardset" aan verkeersgegevens. Gelet op de internationale wens tot ontwikkeling van een standaardset verdient het de voorkeur om de set van gegevens in ieder geval de momenteel reeds gevorderde gegevens te laten bevatten.

Uit het dossieronderzoek en de interviews is gebleken dat de door de opsporing gewenste set van gegevens bestaat uit:

Voor telefonie via het vaste net:

- A-analyse;
- B-analyse;
- Datum, tijd en duur van de verbinding - gegevens omtrent de start en eindtijd van een gesprek.

Voor mobiele telefonie:

- A-analyse
- B-analyse
- Datum, tijd en duur van de verbinding – gegevens omtrent de start en eindtijd van een gesprek;
- MSISDN (het telefoonnummer) van de betrokkene, en de daaraan gekoppelde unieke identiteit IMSI op de SIMkaart;
- IMEI – de identiteit van het toestel;
- De locatiegegevens;
- IMSI, IMEI en locatie van de telefoonnummers door wie de betrokkene wordt gebeld.

Voor internetverkeer:

- IP-adres: zowel de A-analyse als de B-analyse; daarmee wordt gedoeld op zowel de IP-adressen waar de gebruiker van de internetdienst contact mee heeft gezocht alswel de IP-adressen die contact hebben gezocht met het IP-adres van de gebruiker;
- Datum en tijd van de communicatie;
- Duur van de connectie: dit is van belang bij bijvoorbeeld het gebruik van skype (VoIP) of MSN;
- De hoeveelheid data die wordt ge-upload of gedownload;
- Het soort verkeer; de soort dienst en de gebruikte poorten en nummers;
- De gebruikte e-mailadressen en waar en wanneer het e-mailadres is aangemaakt;
- Logfiles indien gebruik wordt gemaakt van wisselende IP-adressen door het gebruik van een modem;
- Webbezoek (URL);
- Webhosting;

Het creëren van een bewaarplicht voor deze "standaardset" wordt door de geïnterviewden noodzakelijk geacht om er voor zorg te dragen dat deze gegevens ook in de toekomst nog geleverd (kunnen) worden.

Het grootste verschil tussen de aanbieders voor wat betreft de geleverde gegevens ligt in de termijn die de gegevens beslaan. Alle aanbieders van telefonie leveren de gevorderde "standaardset" als het gegevens betreft die niet ouder zijn dan drie maanden. Wil men verder terug in de tijd, dan is de aanvragende opsporingsinstantie afhankelijk van welke aanbieder het betreft. Het verdient vanuit opsporingsoogpunt aanbeveling om dit verschil weg te nemen en een eenduidige termijn te scheppen voor het kunnen vorderen van verkeersgegevens.

Zoals hierboven in 6.2 aangegeven, zal een bewaringstermijn van drie maanden in veel opsporingsonderzoeken voldoende zijn. Ten aanzien van de onderzoeken die worden verricht bij de Nationale Recherche, langlopende onderzoeken bij de regionale recherchediensten, bij internationale rechtshulpverzoeken en bij het onderzoek naar cold cases kan zich echter de situatie voordoen dat een bewaringstermijn van drie maanden niet voldoet aan de behoeften van de opsporingsdiensten. Het strekt dan ook tot aanbeveling aansluiting te zoeken bij de in het kaderbesluit voorgestelde bewaartermijn van één jaar. Die termijn lijkt voldoende voor het merendeel van de opsporingsonderzoeken. Eén van de voordelen van een ruimere bewaartermijn dan de nu gegroeide termijn van drie maanden is gelegen in het feit dat een langere termijn een meer afgewogen bevraging van de aanbieders van telecommunicatienetwerken en –diensten en Internet Service Providers mogelijk maakt.

Op basis van het verrichte dossieronderzoek kunnen geen conclusies worden getrokken ten aanzien van de vraag of de praktijk van het vorderen van historische verkeersgegevens met betrekking tot internetverkeer noopt tot de vastlegging van een verplichte bewaartermijn voor een bepaalde duur. Uit het onderzoek is wel gebleken dat er binnen de opsporing behoefte bestaat aan uniforme regels met betrekking tot het vastleggen van historische verkeersgegevens van internetverkeer teneinde invulling te kunnen geven aan het gebruik van de bevoegdheid van art. 126n/u.

Ten aanzien van de verkeersgegevens van telefonie over het Internet (VoIP) is voor de opsporing wel van belang dat de bewaartermijn van deze gegevens gelijk is aan de bewaartermijn van de verkeersgegevens van de klassieke telefonie. Er valt te verwachten dat er een verplaatsingseffect zal optreden als het gebruik van VoIP zal toenemen. Het gebruik van 'klassieke' telefonie zal dan afnemen. Niet goed valt in te zien waarom ten aanzien van deze gegevens een andere bewaartermijn zou worden gehanteerd, nu slechts het medium door middel waarvan de communicatie plaatsvindt, verschilt.

Tot slot dient te worden opgemerkt dat uit de interviews is gebleken dat binnen de opsporing niet slechts behoefte bestaat aan een bewaarverplichting ten aanzien van Internet Service Providers, maar dat deze verplichting zich juist ook zou dienen uit te strekken tot andere aanbieders van internettoegang en –diensten, zoals webhostingservices en internetcafé's en dergelijke.

Bijlage 1

Vragenlijst interviews onderzoek historische verkeersgegevens

Naam:

Functie:

Naam onderzoek:

Aanvangsdatum onderzoek:

1. Algemeen

1.1 Geef een korte omschrijving van het onderzoek

1.2 Door hoeveel personen is er direct aan het onderzoek gewerkt?

1.3 Op welke wijze wordt uitvoering gegeven aan de bevoegdheid tot het vorderen van historische verkeersgegevens en welke knelpunten openbaren zich in dit verband?

2. Vordering verkeersgegevens ex art. 126na

2.1 Op welk tijdstip is er besloten historische verkeersgegevens te vorderen?

2.2 Wat was op dat moment de stand van het onderzoek?

2.3 Wat was de reden historische verkeersgegevens te vorderen?

2.4 Welke 'set' historische verkeersgegevens is er gevorderd?

2.5 Is deze keuze (mede) bepaald door praktische beperkingen?

2.6 Wat is de leeftijd van de gevorderde gegevens?

2.7 Is deze keuze (mede) bepaald juridische/praktische beperkingen?

3. Gebruik van de gevorderde verkeersgegevens

3.1 Welke 'set' historische verkeersgegevens is er verkregen?

3.2 Is deze 'set' gelijk aan de gevorderde gegevens? Zo nee, waarin wijkt de verkregen 'set' af?

3.3 Wat is de reden van deze afwijking?

3.4 Wat is de leeftijd van de verkregen verkeersgegevens?

3.5 Is de leeftijd van de verkregen verkeersgegevens in overeenstemming met de leeftijd van de gevorderde gegevens? Zo nee, waarin wijkt de leeftijd af?

3.6 Wat is de reden van deze afwijking?

3.7 Heeft de vordering van verkeersgegevens de loop van het onderzoek bevorderd?

4. Bewijs

4.1 Hebben de verkregen verkeersgegevens geresulteerd tot direct bewijs?

4.2 Hebben de verkregen verkeersgegevens geresulteerd tot indirect bewijs? Zo ja, op welke wijze?

4.3 Wat is de bijdrage per soort gegeven in termen van direct of indirect bewijs?

5. Gevoelen

5.1 Zou een verruiming van de bewaarplicht een positieve invloed hebben gehad op het verloop van het onderzoek, in termen van directe of indirecte bewijsgaring?

5.2 Zou het ontvangen van bepaalde, nu ontbrekende, verkeersgegevens van invloed zijn geweest op het verloop van het onderzoek, in termen van directe of indirecte bewijsgaring?

Bijlage 2

Literatuurlijst:

- Corstens G.J.M., *Het Nederlands Strafprocesrecht,* Kluwer Deventer, 4de druk 2002.

- Cleiren, C.P.M. en Nijboer, J.F. , *Tekst en Commentaar Strafvordering*, Kluwer Deventer, 5de druk 2003.

- Koops, B.J. , *Verkeersgegevens en strafrecht: een agenda voor discussie*, in: Asscher, L.F. en Ekker, A.H.(red.)Verkeersgegevens. Een juridische en technische inventarisatie, Otto Cramwinckel Uitgever Amsterdam, 2003.

- Kamp, S.J.A. , *Internet technologie en beveiligingsmaatregelen*, SKM & C, Rotterdam, 2005.

- Steenbruggen, W.A.M., *I know what you did last summer!*, in : JAVI, 2002, nr. 3, p. 89 – 97.

Rapporten

- Eindrapport van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Justitie, Onderzoek "Bewaren Verkeersgegevens door Telecommunicatieaanbieder", uitgebracht door Stratix Consulting Group B.V., Schiphol, 2003.

- Onderzoek naar de opslag van historische verkeersgegevens van telecommunicatieaanbieders, Ministerie van Justitie Platform Interceptie, Decryptie en Signaalanalyse, uitgebracht door KPMG Informatie Risk Management, Amstelveen 2004.

- Onderzoek naar het gebruik van (historische) verkeersgegevens in de opsporingspraktijk, uitgebracht door de Regionale Recherchedienst Rotterdam, Rotterdam, 2003.

- Rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, Gegevensvergaring in strafvordering, Ministerie van Justitie, 's Gravenhage, 2001.

- Spelverdeler in de opsporing, Projectgroep Forensische Opsporing, Raad van Hoofdcommissarissen, december 2004.

Bijlage 3

Gebruikte afkortingen

ADSL	Asymmetric Digital Subscriber Line
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
DNR	Dienst Nationale Recherche
DNRI	Dienst Nationale Recherche Informatie
GPRS	General Packet Radio Service
GSM	Global System for Mobile communication
HTTP	Hyper Text Transfer Protocol
IMAP	Internet Mail Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-address	Internet Protocol address
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
KLPD	Korps Landelijke Politiediensten
MMS	Multimedia Message Service
MSISDN	Mobile Station ISDN
MSN	Microsoft netwerk
NAW	Naam, Adres, Woonplaats
PC	Personal Computer
P2P	Peer to Peer
PEC	Parlementaire Enquête Commissie
PIDS	Platform voor Interceptie, Decryptie en Signaalanalyse
RRD	Regionale Recherche Dienst
SIM	Subscriber Identity Module
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
TGO	Team Grootschalige Opsporing
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
VoIP	Voice over IP
WAP	Wireless Application Protocol
Wet BOB	Wet Bijzondere Opsporingsbevoegdheden
Wbp	Wet bescherming persoonsgegevens
WiFi	Wireless Fidelity

Bijlage 4

Begrippenlijst

A-analyse	Alle aansluitingen die worden gebeld vanuit de aansluiting die wordt opgevraagd
B-analyse	De telefoonnummers van degenen die bellen naar een opgevraagde aansluiting.
Direct bewijs	Hetgeen als bewijsmiddel in de strafzaak is gebruikt of kan worden gebruikt
Domein	Een domein is een eigen gebied op het World Wide Web
IMEI	Hardware code van het gebruikte mobiele apparaat
IMSI	De unieke identificatiecode van een abonnee in het GSM/GPRS netwerk. De IMSI is opgeslagen op de SIM-kaart
Indirect bewijs	Hetgeen dienstig is aan het onderzoek, maar niet als direct bewijs in de strafzaak is gebruik of kan worden gebruikt
Internet Service Provider	Organisatie die via eigen servers andere organisaties en privé-gebruikers toegang biedt tot internet
IP-adres	Uniek adres in de vorm van getallen, waarmee een computer geïdentificeerd kan worden
Locatiegegevens	De gegevens omtrent de locatie van een bepaalde aansluiting op het moment dat er via die aansluiting daadwerkelijk communicatie plaatsvindt
Logfiles	Bestand waarin alle handelingen met betrekking tot programmagebruik, computer en diensten worden bewaard
Mastgegevens	De aansluitingen die via een bepaalde zendmast verbinding met een andere aansluiting verkrijgen
MMS	Set van gegevens die middels een mobiele telefoon wordt verzonden
MSISDN	Mobile Station ISDN. Het nummer waarmee een mobiel station bereikbaar is. Het is door de aanbieder direct gekoppeld aan de IMSI code

N.A.W.-gegevens	Naam, adres, postcode en woonplaats die horen bij een bepaalde aansluiting
Peer to peer	Twee computers die met elkaar verbonden zijn: het kleinst mogelijke netwerk
Proxy-server	Een proxy-server is een server die een compleet bedrijfsnetwerk via één verbinding toegang geeft tot internet
Server	Informatieleverende computer. Bij internet is een server rechtstreeks met internet verbonden. De andere kant is de gebruiker van de server. Het internet is op dit principe van server-gebruiker gebaseerd
SIM	Identiteitskaart in het mobiele apparaat
Skype	Technologie voor Voice over IP
SMS	Tekstbericht dat middels een mobiele telefoon wordt verzonden
URL	Standaardmanier waarop informatiebronnen op internet geadresseerd zijn
Voice over IP	Telefoneren via internet
Webhosting	Provider die serverruimte biedt voor websites
Website	Het totaal aan informatie op een domein