Het gebruik van de telefoon- en internettap in de opsporing

Wetenschappelijk Onderzoek- en Documentatiecentrum

Voorwoord

Jaarlijks wordt door de minister van Veiligheid en Justitie bekend gemaakt hoeveel taps er door Nederlandse opsporingsdiensten worden ingezet ten behoeve van de opsporing van strafbare feiten. Over het jaar 2010 is voor het eerst ook het aantal IP- en e-mailtaps bekend gemaakt.
Sinds het laatste WODC-onderzoek naar het gebruik van de telefoontap, dat stamt uit 1996, is de wereld van de telecommunicatie sterk veranderd. Zo is het gebruik van de mobiele telefoon explosief gestegen en is het internet niet meer weg te denken uit het dagelijks leven. Mede daardoor is het aantal taps dat jaarlijks door opsporingsdiensten wordt ingezet sinds die tijd fors gestegen. Echter, de jaarlijkse cijfers over aantallen taps zeggen op zichzelf niet veel en krijgen pas kleur en betekenis als er inzicht bestaat in het feitelijk gebruik van de tap. Wat zijn de motieven en overwegingen die een rol spelen bij de beslissing om een tap aan te sluiten? En waarom wordt er zo vaak gekozen voor de tap en minder vaak voor andere heimelijke opsporingsmiddelen?
De politieke belangstelling voor het onderwerp lijkt vooral te zijn ingegeven door het belang dat wordt gehecht aan de bescherming van de persoonlijke levenssfeer. Met de inzet van een telefoon- of internettap maakt de overheid inbreuk op de persoonlijke levenssfeer van burgers, terwijl het gebruik van dit opsporingsmiddel zich niet beperkt tot verdachten. Ook niet-verdachte personen kunnen worden getapt.
Er is, onder andere door de Tweede Kamer, naar voren gebracht dat uit een vergelijking van tapstatistieken blijkt dat er in Nederland vaker telefoon- en internetgegevens worden afgetapt ten behoeve van de opsporing dan in veel andere Westerse landen. Deze bevinding heeft vragen opgeroepen over de wijze waarop de telefoon- en internettap in Nederland wordt ingezet en over de oorzaken van deze verschillen.

Dit rapport geeft een beeld van de wettelijke kaders en het gebruik van de telefoon- en internettap in de opsporing in Nederland en enkele ons omringende landen, te weten Engeland en Wales, Zweden en Duitsland. Hiermee worden de jaarlijkse tapstatistieken in een context geplaatst. In het onderzoek wordt inzichtelijk gemaakt hoe de cijfers tot stand komen en welke overwegingen een rol kunnen spelen bij het wel of niet inzetten van een telefoon- of internettap. Op basis van de analyse van informatie die is verkregen uit verschillende bronnen, waaronder vele tientallen interviews die zijn gehouden met respondenten vanuit de politie, het openbaar ministerie, de zittende magistratuur, de advocatuur en met enkele andere personen die beroepshalve te maken hebben met de tap, is een uniek beeld ontstaan van de wijze waarop de tap in Nederland en in enkele andere Westerse landen wordt ingezet als opsporingsinstrument.

Dit rapport had niet tot stand kunnen komen zonder de medewerking van velen. Mede namens de auteurs dank ik alle personen die door hun medewerking aan de interviews, het verlenen van toegang tot gegevens en het verstrekken van informatie hebben bijgedragen aan dit onderzoek.
Daarnaast gaat onze dank uit naar de leden van de begeleidingscommissie (zie bijlage 1) die met hun kritische vragen en hun zorgvuldige commentaar op de geschreven stukken een waardevolle bijdrage hebben geleverd aan dit rapport.

Prof. dr. Frans Leeuw
Directeur WODC

Inhoud

Afkortingen

AID	Algemene Inspectiedienst
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
ARPA	Advanced Research Projects Agency
BKA	Bundeskriminalamt
BOB	Bijzondere Opsporingsbevoegdheden
BoF	Bits of Freedom
BRD	Bondsrepubliek Duitsland
BVerfG	Bundesverfassungsgericht
BVO	Basis Voorziening Opsporing
CBP	College Bescherming Persoonsgegevens
CCP	Chief Crown Prosecutor
CEOP	Child Exploitation & Online Protection Centre
CHIS	Covert Human Intelligence Source
CIE	Criminele Inlichtingen Eenheid
CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
CoP	Code of Practice
CPIA 1996	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service
CRCA 2005	Commissioners for Revenue and Customs Act 2005
CSP	Communication Service Providers
CTC	Centrale Toetsingscommissie
CvPG's	College van procureurs-generaal
DDR	Duitse Democratische Republiek
DSRT	Dienst Specialistische Recherche Toepassingen
EHRM	Europese Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
FCO	Foreign and Commonwealth Office
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
FP	Functioneel Parket
FTP	File Transfer Protocol
GCHQ	Government Communications Headquarters
GG	Grundgesetz
GLA	Greater London Authority
GVG	Gerichtsverfassungsgesetz
Gw	Grondwet
HRA	Human Rights Act
HMRC	Her Majesty's Revenue and Customs
IGZ	Inspectie voor de Gezondheidszorg
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IOD	Inlichtingen- Opsporingsdienst
IP	Internet Protocol
IPT	Investigatory Powers Tribunal
IRT	interregionaal rechercheteam
IS	Intrusive Surveillance
ITU	International Telecommunication Union
KLPD	Korps Landelijke Politiediensten
LP	Landelijk Parket
MET	Metropolitan Police
MI5	Security Service
MI6	Secret Intelligence Service
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MP	Members of Parlement
NAW	Naam, Adres en Woonplaats

NN personen	onbekende personen
NOvA	Nederlandse Orde van Advocaten
OM	Openbaar Ministerie
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
OVC	opnemen van vertrouwelijke communicatie
OvJ	officier van justitie
PACE 1984	Police and Criminal Evidence Act 1984
PEO	Parlementaire Enquêtecommissie Opsporingsbevoegdheden
PIDS	Platform Interceptie, Decryptie & Signaalanalyse
PII	Public Interest Immunity
POA 1985	Prosecution of Offences Act 1985
Pw	Politiewet
RC	rechter-commissaris
RCoP	Revised Code of Practice
Rgb	Rättegångsbalken
RIPA 2000	Regulation of Investigatory Powers Act 2000
r.o.	Rechtsoverweging
SCDEA	Scottish Crime and Drug Enforcement Agency
SIM	Subscriber Identification Module
SIOD	Sociale Inlichtingen- en Opsporingsdienst
SIS	Secret Intelligence Service
SOCA	Serious Organised Crime Agency
SOCAP	Serious Organised Crime and Police Act
Sr	Wetboek van Strafrecht
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
Sv	Wetboek van Strafvordering
TGO	Team Grootschalig Onderzoek
TNO	Nederlandse Organisatie voor Toegepast-natuurwetenschappelijk onderzoek
Tw	Telecommunicatiewet
UKBA	United Kingdom Border Agency
ULI	Unit Landelijke Interceptie
VoIP	Voice over IP
Wiv	Wet op de inlichtingen- en veiligheidsdiensten
WLM	Windows Live Messenger
WOB	Wet Openbaarheid van Bestuur
WODC	Wettenschappelijk Onderzoek- en Documentatiecentrum
zwacri	zware criminaliteit

Samenvatting

Het onderzoek: aanleiding, onderzoeksvragen en gegevensverzameling

Aanleiding en de onderzoeksvragen
Regelmatig verschijnt er in de media berichtgeving over het tappen in Nederland. Deze berichten zijn echter niet gevoed door recent onderzoek naar het gebruik van de tap. Het is vooral het gebrek aan informatie dat de toon van de artikelen bepaalt. Jaarlijks publiceert de minister van Veiligheid en Justitie het aantal telefoontaps dat door Nederlandse opsporingsdiensten is ingezet. Naar aanleiding van vragen uit de Tweede Kamer over deze tapstatistieken heeft de toenmalige minister van Justitie een onderzoek toegezegd naar het gebruik van de telefoontap (*Kamerstukken II* 2009/10, 30 517, nr. 16). Dit onderzoek heeft als doel inzicht te bieden in het feitelijk gebruik van de telefoon- en internettap bij de opsporing van strafbare feiten. Dit rapport bestaat uit meerdere delen. In deel I wordt de inleiding en de telefoon- en internetmarkt behandeld, in deel II wordt een beeld geschetst van de inzet van de telefoon- en internettap in de Nederlandse opsporingspraktijk, deel III van dit rapport is gericht op de vraag hoe de tap wordt ingezet in enkele ons omringende West-Europese landen (Engeland en Wales, Zweden en Duitsland) en in deel IV worden de bevindingen uit dit onderzoek besproken in een slotbeschouwing. In het onderzoek wordt uitgegaan van een getrapte vraagstelling:

1 Hoe wordt in Nederland gebruik gemaakt van de telefoon- en internettap tijdens het opsporingsproces?
2 Hoe wordt in enkele andere West-Europese landen met dit opsporingsmiddel omgegaan?
3 Kunnen (grote) verschillen tussen deze landen in het gebruik van dit opsporingsmiddel worden verklaard?

Deze vraagstelling is uitgewerkt in verschillende onderzoeksvragen, die zich samen laten vatten als: hoe vaak, waarom en wanneer wordt de telefoon- en internettap ingezet, voor hoe lang wordt een tap aangesloten en wat voor een informatie levert het dan op?

Gegevensverzameling
Op bovenstaande vragen is antwoord gezocht door bestudering van de wet- en regelgeving, literatuuronderzoek en interviews. Om een breed beeld te kunnen schetsen van het gebruik van de tap in de opsporingspraktijk en van de overwegingen die daaraan ten grondslag liggen, zijn voor het Nederlandse deel van dit onderzoek 55 personen geïnterviewd die beroepshalve met de tap te maken hebben. Dit betroffen ondermeer opsporingsambtenaren, officieren van justitie, rechters-commissarissen en advocaten. Dit onderzoek is verricht op landelijk niveau en in twee regio's die van elkaar verschillen in het aanbod aan misdrijven, de personele bezetting en de wijze waarop activiteiten die gepaard gaan met de inzet van bijzondere opsporingsbevoegdheden zijn georganiseerd. Deze regio's zijn niet gekozen om ze te vergelijken, maar om een breed beeld te kunnen schetsen van de wijze waarop de tap wordt ingezet. Voor de buitenlandse delen van deze studie zijn in de geselecteerde landen gesprekken gevoerd met in totaal 14 deskundigen en 3 academici op het gebied van het (verzamelen van gegevens over) aftappen van telefoon- en internetverkeer.

De telefoon- en internetmarkt
In de afgelopen decennia is het (tele)communicatieverkeer explosief toegenomen. Naast een toename in telecommunicatieverkeer, door onder andere de vlucht die het gebruik van de mobiele telefoon heeft genomen, is ook de wijze waarop deze telefoons worden gebruikt veranderd. Steeds meer mobiele telefoons hebben mobiel internet en steeds meer communicatie verloopt over het internet. Communicatie raakt steeds meer versplinterd door de vele mogelijkheden en kanalen die er zijn om te kunnen communiceren (VoIP, mail, chat, fora, games, sociale media, etc.). Dit heeft grote gevolgen voor de wijze waarop de telefoontap kan worden ingezet in de opsporingspraktijk. De verwachting is dat er voor het onderscheppen van communicatie in de toekomst steeds vaker een beroep zal worden

gedaan op de internettap. Hoewel het grootste deel van de telecommunicatie momenteel nog aftapbaar is, maakt het snel veranderde aanbod aan communicatiediensten op internet het noodzakelijk om de mogelijkheden voor het aftappen regelmatig opnieuw te bezien (Stratix, 2009).

De regulering van het tappen in Nederland

De Wet Bijzondere Opsporingsbevoegdheden

Door telefoon- en internetverkeer af te tappen wordt inbreuk gemaakt op het recht op privacy, een grondrecht dat onder andere wordt gewaarborgd door het Europees Verdrag voor de Rechten van de Mens (art. 8 EVRM). Het openbaar gezag kan rechtmatig een inbreuk maken op dit grondrecht (zie lid 2), maar moet in dat geval aan een aantal eisen voldoen. In het kader van de nadere invulling van art. 8 lid 2 EVRM moet bij het gebruik van de telefoon- en innternettap ondermeer worden gedefinieerd welke categorieën mensen aan dit opsporingsmiddel kunnen worden onderworpen, hoe lang en bij welke misdrijven het middel kan worden ingezet en welke procedures in acht moeten worden genomen bij het uitwerken van de afgetapte communicatie. In Nederland heeft het aftappen van telefoon- en internetverkeer een wettelijke basis gekregen in de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB).

De telefoon- of internettap (art 126m Sv) is een bijzondere opsporingsbevoegdheid. In de Wet BOB is vastgelegd dat bijzondere opsporingsbevoegdheden kunnen worden ingezet op basis van drie titels: 1) op grond van een verdenking dat een misdrijf is begaan (titel VIa); 2) op grond van een redelijk vermoeden dat misdrijven als omschreven in artikel 67 lid 1 Sv in georganiseerd verband worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren (titel V); 3) op grond van aanwijzingen dat een terroristisch misdrijf wordt gepleegd (Titel Vb).

Een aantal bijzondere opsporingsbevoegdheden is in het gehele toepassingsbereik geregeld, andere alleen voor zover ze stelselmatig worden toegepast. De wettelijke voorwaarden die zijn gesteld aan de bijzondere opsporingsbevoegdheden geven enig zicht op de mate waarin ze als ingrijpend worden ervaren. Zo kunnen de verdenkingsgraad, de persoon tegen wie een opsporingsbevoegdheid kan worden ingezet, de duur van inzet, de toestemmingsprocedure en de gronden waarop een bijzondere opsporingsbevoegdheid kan worden ingezet, iets zeggen over de mate waarin het middel als ingrijpendheid wordt gepercipieerd.

De wetgever beoordeelde de tap bij de totstandkoming van de Wet BOB als één van de meest ingrijpende opsporingsbevoegdheden. De inzet ervan moet voldoen aan de vereisten van proportionaliteit en subsidiariteit. De tap kan enkel worden ingezet bij misdrijven als omschreven in artikel 67, eerste lid Sv. Daarnaast moet de aard van het misdrijf een ernstige inbreuk op de rechtsorde opleveren. Tot slot moet het onderzoek de inzet van de telefoontap dringend vorderen. De telefoontap mag alleen worden ingezet als niet met behulp van lichtere opsporingsbevoegdheden eenzelfde resultaat kan worden bereikt.

Geheimhouders

Voor een aantal beroepsgroepen (onder andere juridische en medische beroepen) geldt het verschoningsrecht. Dat wil zeggen dat gesprekken die met deze geheimhouders niet mogen worden afgeluisterd en opgenomen. In het verleden is het voorgekomen dat uitgewerkte gesprekken tussen verdachten en geheimhouders in het procesdossier terecht zijn gekomen. Een bekend voorbeeld hiervan is de strafzaak tegen leden van de Hells Angels. Om dit in de toekomst te voorkomen zijn sindsdien maatregelen getroffen. Deze maatregelen bestaan uit een instructie over de wijze waarop met geïntercepteerde gesprekken met geheimhouders moet worden omgegaan en een nummerherkenningssysteem. Dit systeem is op 1 september 2011 in gebruik genomen. In dit systeem staan opgegeven telefoon- en faxnummers van advocaten en daarvan afgeleide personen met het verschoningsrecht, in een filter geregistreerd bij de Unit Landelijke Interceptie (ULI). Wanneer een telefoonnummer wordt afgetapt, worden de verkeersgegevens (telefoonnummers, tijdstip, etc) langs een filter geleid. Als een telefoonnummer door het systeem wordt herkend, dan wordt de opname automatisch gestopt. Mocht er vertraging zitten in het doorkomen van de verkeersgegevens,

dan wordt de reeds opgenomen communicatie vernietigd. In dit nieuwe systeem, kan het opsporingsteam alleen de verkeersgegevens van de in het systeem geregistreerde geheimhoudergesprekken inzien. Deelname aan het nieuwe systeem is voor alle advocaten verplicht gesteld. Het is de verwachting dat met de ingebruikname van dit systeem, de problemen rond het opnemen van gesprekken met geheimhouders die zijn opgenomen in dit nummer herkenningsysteem zijn ondervangen. Echter, gesprekken met andere geheimhouders zoals artsen of geestelijken worden niet automatisch gefilterd. Voor gesprekken met dergelijke geheimhouders is de oudere regeling nog van toepassing.

Notificatie, vernietigen en gebruik voor een ander doel

Betrokkenen tegen wie een bijzondere opsporingsbevoegdheid is ingezet dienen hierover, zodra het belang van het onderzoek het toelaat, ingelicht te worden. Op deze regel zijn een paar uitzonderingen. Er hoeft niet te worden genotificeerd wanneer de verdachte al inzage heeft gehad in zijn dossier, indien de mededeling redelijkerwijze niet mogelijk is, bijvoorbeeld omdat men de identiteit of de verblijfplaats van de betrokkene niet heeft kunnen achterhalen, of wanneer er een veiligheidsrisico gemoeid is met het notificeren. Het uitstellen van notificatie van betrokkenen is aan termijnen verbonden. Twee maanden na het notificeren, dient alle informatie die met een telefoon- of internettap is vergaard vernietigd te worden. Soms kan vernietiging worden uitgesteld omdat de officier van justitie (OvJ) de gegevens wil gebruiken in een ander onderzoek of omdat de OvJ de gegevens wil opslaan in een zogenaamd "register zware criminaliteit".

Wat is een tap en hoe komt deze tot stand?

Met een telefoontap wordt de communicatie van of naar een bepaald telefoonnummer of telefoontoestel afgetapt. Het aftappen van communicatie houdt in dat de inhoud (art 126m Sv) en verkeersgegevens (art 126n Sv) van gesprekken door de aanbieder worden doorgegeven aan de Unit Landelijke Interceptie (ULI) van het Korps Landelijke Politiediensten (KLPD). Met een internettap wordt al het internetverkeer (of alleen het e-mailverkeer indien het een e-mailtap betreft) dat over een bepaalde internetlijn loopt onderschept.

Verkeersgegevens

Het is ook mogelijk om alleen verkeersgegevens op te vragen. In dat geval wordt alleen informatie verkregen over het nummer van beller en gebelde, de datum, het tijdstip en de duur van het gesprek en de zendmastinformatie. Er kunnen twee soorten verkeersgegevens worden opgevraagd: historische en toekomstige verkeersgegevens.
Historische verkeersgegevens bieden inzicht in het belgedrag van iemand over een periode die in het verleden ligt terwijl toekomstige verkeersgegevens informatie geven over het belgedrag tijdens het opsporingsonderzoek. Verkeersgegevens kunnen van waarde zijn bij het in kaart brengen van sociale netwerken en een rol spelen bij de overwegingen om bepaalde nummers wel of niet te willen gaan tappen. Het opvragen van verkeersgegevens is een lichtere bijzondere opsporingsbevoegdheid dan de telefoontap en kan door de OvJ worden gevorderd zonder machtiging van de rechter-commissaris (RC). Het opvragen van verkeersgegevens aangaande internetcommunicatie levert onder ander inzicht op in het tijdstip van aanmelden, het IP-adres, informatie over e-mailcontacten van zender en ontvanger, het gebruikte protocol en IP-adressen van de opgevraagde internetpagina's.

Procedure

Het is de OvJ die, na machtiging van de RC, een tapbevel geeft aan de opsporingsambtenaar. Bij een tapaanvraag zijn twee toetsmomenten. Ten eerste is het de OvJ die controleert of is voldaan aan de wettelijke vereisten, zoals de verdenking, of er sprake is van een ernstige inbreuk op de rechtsorde en in hoeverre het onderzoek de inzet van de tap dringend vordert, hierbij rekening houdend met de eisen van proportionaliteit en subsidiariteit. Ten tweede is het de RC die toetst of de OvJ in redelijkheid had kunnen komen tot een vordering machtiging tap en andermaal toetst of is voldaan aan de gestelde eisen.

In urgente situaties is het mogelijk een 'spoedtap' aan te vragen. In dat geval vindt er telefonisch overleg plaats tussen de OvJ en RC en kan de tap, indien de RC een machtiging afstaat, in zeer korte tijd worden aangesloten. De tapaanvraag dient vervolgens wel schriftelijk bevestigd te worden. Een tapmachtiging wordt voor maximaal vier weken afgegeven, maar de RC kan ook besluiten de tap voor een kortere periode toe te staan. Dit laatste wordt vaak gedaan bij een spoedtap. Een tap kan voortijdig worden afgesloten, maar in het geval men het noodzakelijk vindt de tap voort te zetten, dient de OvJ een aanvraag voor verlenging voor te leggen aan de RC.

Notificeren en vernietigen

Het notificeren van betrokkenen die zijn getapt wordt in de praktijk overgelaten aan de 'BOB-kamer' (personen bij het openbaar ministerie (OM) die zorgen voor die administratieve afhandeling van de aanvragen en voor verlengingen van bijzondere opsporingsbevoegdheden, voor notificatie en voor vernietiging van gegevens). Zij administreren de namen en adressen, verzamelen de handtekeningen bij de OvJ en versturen uiteindelijk de notificatiebrieven. Processen-verbaal dienen twee maanden na notificatie te worden vernietigd. Ook dit wordt gecoördineerd door de BOB-kamer.

Centraal Informatiepunt Onderzoek Telecommunicatie

Voordat een tapaanvraag wordt ingediend, dient men zich ervan te vergewissen dat het betreffende telefoonnummer of IP-adres nog steeds in gebruik is. Dit kan worden achterhaald door middel van een CIOT-bevraging. Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is de schakel tussen opsporingsdiensten en telecombedrijven en draagt zorg voor opslag en gebruik van identificerende gegevens. Identificerende gegevens zijn naam, adresgegevens en woonplaats behorende bij telefoonnummers, e-mailadressen en IP-adressen. Aanbieders van telefonie- en internetdiensten zijn verplicht de gegevens elke 24 uur te verversen. De gegevens zijn via het CIOT opvraagbaar door geautoriseerde opsporingsdiensten. Bevragingen bij het CIOT mogen enkel plaatsvinden op grond van artikel 126n, 126na, 126u, 126ua, 126zh, 126zi, 126ii Sv, artikel 29 Wiv en artikel 10.10 TW in het kader van een concreet opsporingsonderzoek.

Statistieken

Jaarlijks publiceert het ministerie van Veiligheid en Justitie het aantal ingezette telefoontaps door de Nederlandse opsporingsdiensten. De statistieken komen tot stand door het aantal door een RC afgegeven tapbevelen te tellen. Voor elk afzonderlijk telefoonnummer, IMEI-nummer, IP- of emailadres dient een afzonderlijk tapbevel opgesteld te worden. Wanneer de tapstatistieken worden afgezet tegen het totaal aantal in gebruik zijnde telefoonnummers in Nederland blijkt dat jaarlijks voor ongeveer een op de duizend in gebruik zijnde telefoons een tapbevel is afgegeven. Het aantal taps op vaste lijnen is over de jaren ongeveer gelijk gebleven. De toename van het aantal telefoontaps vanaf 1998 is vooral toe te schrijven aan de opkomst van de mobiele telefonie. Het aantal taps is in 2010 uitgekomen op 22.006. Het aantal taps in Nederland neemt de laatste jaren af, zowel in absolute zin (met bijna 17% in 2010 t.o.v. 2008) als in relatie tot het totale aantal in gebruik zijnde telefoonaansluitingen. Over het jaar 2010 zijn voor het eerst het aantal internettaps bekend gemaakt (1704) en in de tweede helft van 2010 is 24.012 keer een aanvraag gedaan voor historische gegevens die betrekking hebben op zowel historische verkeersgegevens als op identificerende gegevens.

Ook het aantal CIOT-bevragingen wordt bijgehouden. Dit aantal is in de loop der jaren sterk toegenomen. Er is regelmatig kritiek op de hoeveelheid bevragingen bij het CIOT, omdat het opvragen van identificerende gegevens van allerlei personen, behorend bij bepaalde telefoonnummers of IP-adressen een schending van de privacy met zich brengt. Het grote aantal opgevraagde nummers is vooral te wijten aan bevragingen van zendmastgegevens (identificerende gegevens van alle nummers die op een bepaald tijdstip via een bepaalde zendmast hebben gebeld) en van contra- of tegennummers (nummers of IP-adressen die contact hebben met een nummer of adres dat wordt afgetapt, of waarvan de

verkeersgegevens zijn opgevraagd). Om met de informatie over die zendmastgegevens of contranummers iets te kunnen doen, wordt getracht de identiteit van de eigenaars van deze nummers of IP-adressen te achterhalen. Dit wordt echter bemoeilijkt door de grote aantallen in gebruik zijnde pre-paid telefoons waarvan de CIOT vaak geen identificerende gegevens voorhanden heeft.

Telefoontap in de praktijk

Misdrijven

Uit dit onderzoek blijkt dat de tap heel divers en met veel verschillende doelen wordt ingezet.
In geval van calamiteiten wordt de tap vaak snel en breed ingezet om vooral snel een onderzoeksrichting te kunnen bepalen. Bij meer voorkomende delicten zoals een gewelddadige straatroof van een mobiele telefoon, wordt de tap ook regelmatig ingezet. Omdat een gestolen telefoon doorgaans snel wordt doorverkocht is de inzet van de tap in dat geval heel gericht, snel en kort. Bij onderzoek naar zware criminaliteit wordt er daarentegen langdurig en veelvuldig gebruik gemaakt van de telefoontap. In dit soort zaken gaat het vaak om voortdurende criminaliteit, zoals drugshandel of mensensmokkel, waarover verdachten (telefonisch) met elkaar communiceren. De inhoudelijke opbrengst van de afgetapte gesprekken is in dit soort onderzoeken vooral ondersteunend. Zelden wordt er in deze zaken direct bewijs vergaard door middel van de tap. Doorgewinterde criminelen zijn zich goed bewust van het feit dat ze worden getapt en hebben de wijze waarop ze via de telefoon communiceren daarop aangepast. Het zijn vooral de verkeersgegevens die gebruikt worden om netwerken en organisaties in kaart te brengen.

Doelen en overwegingen

De doelstellingen die men met het tappen wil behalen zijn vaak: het verkrijgen van sturingsinformatie door het verzamelen van achtergrondinformatie over een persoon of netwerk, het verkrijgen van bewijs, het verkrijgen van locatiegegevens van een getapte persoon door het analyseren van de gespreksinhoud en verkeersgegevens of een combinatie van deze. Ook kan de tap worden ingezet ter ondersteuning van andere opsporingsmiddelen. Bij het besluit om te gaan tappen spelen verschillende overwegingen een rol. Allereerst moet worden bezien of is voldaan aan de proportionaliteits- en subsidiariteitseis. Staat de inzet van het middel in verhouding met de aard van het misdrijf, is de inzet noodzakelijk en is er geen lichtere opsporingsbevoegdheid voorhanden waarmee de benodigde informatie kan worden achterhaald? Daarnaast speelt de capaciteit van het opsporingsteam een rol. Het team moet voldoende mankracht beschikbaar hebben om de gesprekken te kunnen verwerken. Maar ook speelt de persoonlijke voorkeur van de teamleider en het gemak waarmee een tap kan worden gerealiseerd een rol in de besluitvorming over de inzet van de tap.
Niet alleen verdachten kunnen worden getapt, ook betrokkenen. RC's, OvJ's en ook een aantal politiefunctionarissen geven aan terughoudender te zijn met het plaatsen van een tap op een betrokkene dan op een verdachte. Het aantal taps per onderzoek is zeer verschillend en sterk afhankelijk van de hierboven besproken overwegingen. Uiteraard speelt ook het aantal verdachten dat bij een zaak betrokken is en het aantal telefoons en simkaarten dat zij in gebruik hebben hierbij een rol.

Opvragen verkeersgegevens

Verkeersgegevens leveren belangrijke inzichten op bij onderzoek naar diverse soorten misdrijven. Zo kan het inzicht geven in de contacten of het netwerk waarmee verdachte(n) en/of slachtoffer(s) in contact stond(en). Historische verkeersgegevens kunnen een rol spelen bij de overweging om een bepaald telefoonnummer wel of niet te willen gaan tappen. De gegevens maken inzichtelijk hoeveel, hoe lang met wie of welk bepaald nummer gebeld wordt. Op grond hiervan kan er een inschatting worden gemaakt van de capaciteit die nodig is om een tap uit te luisteren en te verwerken. Daarnaast worden historische verkeersgegevens soms aangevraagd als een OvJ het misdrijf niet zwaar genoeg vindt voor

de inzet van een tap. Aan de hand van de verkeersgegevens kan men dan toch zicht krijgen op de communicatiestromen van een persoon.
Een belangrijk voordeel van historische en toekomstige verkeersgegevens ten opzichte van de tap is dat er geen gesprekken hoeven te worden uitgeluisterd en uitgewerkt. Voor de RC is het van tevoren opvragen van verkeersgegevens geen voorwaarde voor het toe- of afwijzen van een tap. Of er eerst inzicht nodig is in de wijze waarop bepaalde telefoonnummers worden gebruikt valt onder de verantwoordelijkheid van de OvJ.

Opvragen CIOT-gegevens
Een nadeel van het gebruiken van verkeersgegevens is dat het lang niet altijd mogelijk is om identificerende gegevens te verkrijgen van de nummers die door het opvragen van deze gegevens in beeld zijn gekomen. Respondenten geven aan dat het opvragen van identificerende gegevens van deze nummers bij het CIOT vaak niets oplevert, omdat er veel gebruik wordt gemaakt van prepaid telefoonnummers, waarvan vaak geen identificerende gegevens bekend zijn bij het CIOT. Met een tap kan in dat geval makkelijker de identiteit van de gebruiker van een bepaalde telefoon worden achterhaald door informatie die voortkomt uit de gesprekken en de contacten die de beller heeft.
Politiekorpsen kunnen alleen informatie via het CIOT bevragen volgens een wettelijk vastgestelde procedure. Als korpsen niet aan de wettelijk vastgestelde eisen voldoen kunnen ze geen bevragingen doen. Op dit moment zijn alle opsporingsdiensten in staat om de CIOT-bevragingen te verrichten volgens de vastgestelde regels.

Uitluisteren en uitwerken
Het uitluisteren en uitwerken van tapgesprekken is arbeidsintensief en vergt veel capaciteit van het opsporingsteam. Het is specialistisch werk: ervaring in het uitwerken en interpreteren van telefoontaps speelt een grote rol bij de kwaliteit. Naast ervaring is continuïteit van de personele bezetting ook van belang. Men moet de gelegenheid krijgen bekend te raken met de stemmen die over de lijnen komen om stemherkenning op te kunnen bouwen. De respondenten uit de advocatuur vinden de kwaliteit van de uitgewerkte gesprekken wisselend. Wanneer de manier waarop een gesprek is uitgewerkt een bepaalde kleuring heeft die volgens de verdachte niet juist is, kan een advocaat vragen het bewuste gesprek zelf te mogen beluisteren.

Tolken
Bij het tappen van telefoongesprekken komt het geregeld voor dat de gesproken taal een andere is dan de Nederlandse .In dat geval wordt er een tolk ingeschakeld. De procedures betreffende de omgang en het werken met tolken wordt door de onderzochte regio's en parketten zelf ingevuld en verschillen dan ook op meerdere punten. Een door de respondenten genoemd voordeel van het werken met tolken is dat het extra mankracht oplevert. Het nadeel daarentegen is de afhankelijkheid van de tolk – vertalingen zijn vaak oncontroleerbaar voor het team. Bij twijfel kan een opsporingsteam een tweede tolk de inhoud van de gesprekken laten beluisteren, hetgeen overigens standaard gebeurt bij gesprekken die van groot belang worden geacht voor de zaak. De respondenten zijn overwegend positief over het werk dat tolken leveren. Voor bepaalde talen bestaat echter een schaarste aan tolken, waardoor opsporingsteams soms moeten wachten totdat er een tolk beschikbaar is, waardoor de opsporing vertraging kan oplopen.

Verlengen of afsluiten
De overweging om een tap af te sluiten of te verlengen is afhankelijk van de verhouding tussen de informatie die de tap oplevert en de capaciteit die het kost om die informatie te achterhalen. Als een lijn geen relevante informatie oplevert, geven de respondenten aan de tap voortijdig af te sluiten. Maar ook een tekort aan capaciteit om de lijnen uit te luisteren en uit te werken kan een reden zijn om een tap voortijdig te beëindigen. Ook komt het voor dat een getapte lijn 'dood' blijkt te zijn. Dat betekent dat het telefoonnummer niet wordt gebruikt en dat er dus geen informatie overheen komt. Wanneer een zaak ten einde is, worden taps ook afgesloten. De RC's geven aan dat hoe langer een tap loopt, des te kritischer ze worden bij het beoordelen van een aanvraag tot een verlenging. De mate

waarin een tap inbreuk maakt op de privacy van personen, speelt volgens respondenten een rol bij de overweging om een tap te verlengen of af te sluiten.

Privacy

Sinds de wetwijziging van 1 februari 2000 is tappen niet meer enkel voorbehouden aan communicatie waaraan de verdachte deelneemt. Ook betrokkenen, mensen die op één of andere manier in relatie staan tot de verdachte of mogelijk iets weten over het gepleegde misdrijf, kunnen worden getapt. Het besluit om de tap in te zetten is steeds een afweging van belangen die spelen en de te verwachten resultaten. Eén van die belangen is het recht op privacy dat regelmatig conflicteert met het opsporingsbelang. Wanneer de te tappen persoon een betrokkene is, wordt de lat volgens de respondenten hoger gelegd. Het opsporingsteam moet dan nog beter motiveren waarom ze deze betrokkene willen gaan tappen en wat het voor het onderzoek kan opleveren. Ook wordt de door de RC afgegeven termijn om te mogen tappen vaak korter gehouden bij een tap op een betrokkenen dan wanneer het een tap op een verdachte betreft. Toch kan een tap op een betrokkenen soms belangrijker zijn dan een tap op een verdachte. Dit omdat betrokkenen minder bedacht zijn op het feit dat ze getapt kunnen worden.
Dat de telefoontap inbreuk maakt op de privacy staat volgens de respondenten wel vast. Respondenten vinden zelf dat ze zorgvuldig omgaan met de tap en de tap alleen inzetten als er een groot belang mee is gemoeid en wanneer er resultaat van wordt verwacht. Wanneer de inzet van de telefoontap vergeleken wordt met de inzet van de internettap zijn de meningen verdeeld over de vraag welk opsporingsmiddel meer inbreuk maakt op de privacy. Het gebruik van internet en bellen vloeit, mede door de smartphone, steeds meer samen waardoor de discussie over de zwaarte van privacyschending op den duur niet meer uit maakt, aldus een respondent.

Geheimhouders

Informatie uit gesprekken met personen die vallen onder het verschoningsrecht mogen niet in het opsporingsproces terecht komen. Om dit te voorkomen is er zoals gezegd voor de gesprekken met advocaten een nummerherkenningssysteem opgezet. Navraag begin januari 2012 leert dat het nummerherkenningsysteem officieel in werking is getreden maar in de praktijk nog niet optimaal functioneert. Dit heeft te maken met het feit dat nog niet alle advocaten zich hebben kunnen registreren in het nieuwe systeem door een registratieprobleem. Wanneer dit probleem is opgelost is nog onduidelijk. Alhoewel het systeem van nummerherkenning is ingevoerd, zal de 'oude' werkwijze[1] omtrent geheimhoudersgesprekken nog moeten worden nageleefd.
De politie en het OM blijven, ook in de nieuwe situatie, verantwoordelijk voor het op een juiste manier vernietigen van geheimhoudergesprekken.

Opbrengsten

De telefoontap levert vooral sturingsinformatie op en informatie waarmee verdachten of slachtoffers kunnen worden opgespoord. Informatie die uit de tap naar voren komt, kan regelmatig worden gebruikt om de richting van het onderzoek te bepalen, om gericht andere opsporingsmiddelen in te zetten of om de locatie van personen te bepalen.
Daarnaast levert de tap, hoewel volgens de respondenten in steeds mindere mate, bewijs op. Tapgesprekken zijn volgens de respondenten vooral van belang vanwege het indirecte bewijs, informatie die ondersteunend is aan ander bewijsmateriaal. Het is een 'stukje van de puzzel'. Hoewel het niet wordt nagestreefd, levert de tap ook vaak restinformatie op over andere misdrijven of personen. Of en hoe daarop wordt gereageerd, is afhankelijk van de aard van de informatie en de ernst van het misdrijf waaraan deze informatie is gerelateerd, de capaciteit van het opsporingsteam en het belang van het oorspronkelijk onderzoek – dat door deze nieuwe informatie zou kunnen worden doorkruist.
Ten opzichte van 20 jaar geleden moet er volgens respondenten steeds meer moeite worden gedaan om hetzelfde resultaat uit de tap te halen. Verdachten zijn er steeds meer van doordrongen dat de politie telefoons afluistert en dat ze niet moeten praten via de telefoon.

[1] Instructie vernietiging geïntercepteerde gesprekken met geheimhouders

De opbrengst van het tappen is sterk afhankelijk van meerdere factoren: het gepleegde of te plegen feit, de doelgroep waartoe de verdachte behoort, of er al dan niet reuring wordt veroorzaakt, of er een analist betrokken is bij het onderzoek, het afnemend gebruik van spraaktelefonie en ook gewoon van het toeval.

Notificeren en vernietigen

In tegenstelling tot wat de onderzoeksresultaten uit 2004 laten zien, blijkt dat er anno 2011 in de onderzochte parketten doorgaans wordt genotificeerd. Hoewel de wettelijke regeling betreffende het notificeren duidelijk is,[2] geeft ieder parket er zijn eigen invulling aan. In één van de onderzochte regio's (regio A) zeggen meerdere respondenten dat het notificeren jarenlang een lage prioriteit heeft gehad, maar dat er vanuit justitie druk wordt uitgeoefend om deze plicht na te leven. Momenteel is een inhaalslag gaande om personen te notificeren en de politie de bevelen tot vernietiging te geven.

Respondenten uit een andere onderzochte regio (regio B) geven aan dat het notificeren strikt wordt nageleefd. Dat het in deze regio wel lukt om 'bij' te zijn met notificeren en geen achterstand te hebben, ligt volgens deze medewerker van de BOB-kamer aan het feit dat er in deze regio geld en tijd is vrijgemaakt voor het notificatie en vernietiging. Ook het kleiner aantal zaken dat jaarlijks in deze regio behandeld worden zal hieraan bijdragen.

In de onderzochte regio's wordt het notificeren gecoördineerd door de BOB-kamer. In regio A is de afspraak gemaakt dat een jaar na de start van een onderzoek door de administratie wordt gevraagd aan de desbetreffende OvJ hoe de stand van zaken is in dat onderzoek, en of er kan worden genotificeerd. In regio B wordt twee maanden na sluiting van een onderzoek op initiatief van de BOB-kamer en in samenspraak met de OvJ besloten om te notificeren.

De meerderheid van de respondenten, zowel op landelijk als op regionaal niveau, vinden de notificatieplicht een onzinnige regel. Men is bang dat opsporingstactieken op straat komen te liggen en men vindt dat de notificatiebrief meer vragen oproept dan het beantwoordt. Hoewel de respondenten dus overwegend negatief aankijken tegen de notificatieplicht, wordt het notificeren uitgevoerd, maar vaak zonder prioriteit.

Nadere informatie naar aanleiding van de door het OM verstuurde brief wordt niet verstrekt. Wanneer iemand zich wil beklagen over de notificatiebrief kan hij zich dus niet tot het OM wenden. In de notificatiebrieven van de onderzochte regio's wordt geen melding gemaakt van een klachtenregeling of van organisaties waartoe men zich kan wenden met vragen. De klachtenprocedure rondom de notificatiebrief is voor verbetering vatbaar.

Naast de getapte persoon zelf, die achteraf dus wordt genotificeerd, zijn er meer mensen die gecommuniceerd hebben met de getapte persoon en daardoor ook in hun privacy worden geschonden. Deze personen worden echter niet genotificeerd. Een respondent pleit voor uitbreiding van de notificatieplicht naar de personen die frequent contact hebben gehad met een 'afgetapte persoon'.

Twee maanden na het versturen van de notificatiebrief dient het OM de politie een bevel vernietiging te geven. Daarmee krijgt de politie de opdracht om alle informatie die met bijzondere opsporingsbevoegdheden is verzameld, te vernietigen. Uit de interviews blijkt dat men in regio A nog niet zo lang systematisch aan het vernietigen is. Sinds kort is er iemand binnen de politie aangesteld die de coördinatie op zich heeft genomen van het vernietigen van processen-verbaal. Regio B geeft aan dat zij zich een aantal jaar geleden hebben voorbereid op het notificeren en vernietigen. Door aan de voorkant zaken op een gestandaardiseerde wijze te borgen, is het vernietigen aan de achterkant zo gebeurd. Standaard wordt sinds een aantal jaar een zogenaamd 'nul dossier' opgemaakt, waarin alle ingezette bijzondere opsporingsbevoegdheden zijn weergegeven, zodat men niet het hele dossier door hoeft op zoek naar ingezette bijzondere opsporingsbevoegdheden.

In twee gevallen kan vernietiging worden uitgesteld. Wanneer gegevens die zijn verkregen door het opnemen van telecommunicatie gebruikt kunnen worden voor een ander strafrechtelijk onderzoek hoeven de gegevens niet te worden vernietigd totdat het andere onderzoek is beëindigd. Daarnaast kunnen gegevens worden bewaard die betrekking hebben op personen die, op een wijze bij de Wet politieregisters bepaald, betrokken zijn bij zware

[2] de Aanwijzing opsporingsbevoegdheden (2011A002), 14 februari 2011, *Staatscourant* 2011, 3240.

criminaliteit. Uit navraag blijkt dat zowel bij het landelijk parket als ook bij de arrondissementsparketten met enige regelmaat informatie verkregen met inzet van een tap, wordt opgeslagen op grond van dit artikel.

Knelpunten van de tap

Respondenten noemen de volgende knelpunten en/of verbeterpunten over het werken met de telefoon- en/of internettap: 1) het feit dat criminelen goed op de hoogte zijn van de opsporingstechnieken van de politie 2) het feit dat online telecommunicatie vaak met encryptieprogramma's wordt versleuteld waardoor deze minder gemakkelijk af te tappen is; 3) Het omvangrijke administratieproces dat gepaard gaat met het tappen. Volgens sommige respondenten wordt er teveel in de openbaarheid gebracht over de opsporingsmethoden die de politie hanteert. Dit heeft tot gevolg dat daders rekening houden met het feit dat er heimelijke opsporingsmiddelen tegen hen worden ingezet en daar op in spelen. Hierdoor komt de aftapbaarheid van communicatie in gevaar. Criminelen zoeken alternatieve manieren om te communiceren en manieren om een tap te ontwijken. Zo blijken doorgewinterde criminelen bijvoorbeeld gebruik te maken van technische mogelijkheden om hun communicatie te versleutelen. Verreweg de meeste opmerkingen die gemaakt zijn over knelpunten rond het tappen, hadden te maken met de bureaucratie en de papierwinkel die gepaard gaat met het aanvragen van een tap.

De internettap

Het aantal internettaps dat jaarlijks wordt ingezet bij opsporingsonderzoeken is, in vergelijking met het aantal telefoontaps, zeer bescheiden. Maar de verwachting van de internetexperts is dat de toepassing van het opsporingsmiddel flink zal toenemen. Vooral het groeiend aantal smartphones wordt door meerdere respondenten genoemd als een belangrijke drijfveer achter vernieuwingen van de internettap. De verwachting van meerdere respondenten is dan ook, dat in de toekomst een tap op een smartphone vanzelfsprekend een internettap zal zijn. Maar zover is het in de praktijk nog niet.
De inzet van een internettap gebeurt vaak naar aanleiding van informatie verkregen door de inzet van een telefoontap. De geïnterviewden geven aan tot inzet van een internettap over te gaan als blijkt dat een 'gewone' telefoontap op een smartphone te weinig oplevert en men het gevoel heeft een deel van de communicatie te missen.
Wat betreft het gebruik van de internettap valt er een drietal groepen te onderscheiden. Ten eerste is er een groep respondenten die tot nu toe nog nooit een internettap heeft ingezet en ook niet het idee heeft het opsporingsmiddel te missen, bijvoorbeeld omdat het niet bij de doelgroep past. Ten tweede is er een groep respondenten die zegt de internettap wel met enige regelmaat in te zetten. Deze respondenten zijn enthousiast over de inzet ervan. De derde en grootste groep respondenten heeft in het verleden wel eens te maken heeft gehad met de internettap maar probeert de inzet van de tap - door slechte ervaringen met het instrument - nu zoveel mogelijk te vermijden. Deze slechte ervaringen met de internettap heeft deze groep respondenten negatief beïnvloedt in hun bejegening van het opsporingsmiddel. Inmiddels is de programmatuur, zeker in vergelijking met jaren terug, sterk verbeterd maar volgens meerdere respondenten is het nog steeds behelpen. Naast de weinig gebruiksvriendelijke applicaties worden ook genoemd: de grote capaciteit die nodig is voor de uitwerking, een tekort aan digitale expertise binnen de teams en de grote hoeveelheid data die een internettap kan opleveren. Tevens blijkt uit de gesprekken dat duidelijke richtlijnen over de uitwerking en verbalisering van de internettap ontbreken en dat de respondenten hier grote behoefte aan hebben. Het ontbreekt de politie aan kennis over hoogwaardige analyse technieken om grote hoeveelheden data snel en grondig te doorzoeken, aldus een expert op het gebied van de internettap. Daarnaast bestaat er bij de internettap geen mogelijkheid om vooraf te kiezen welke informatie wel ondervangen en opgeslagen moet worden en welke informatie geweerd zou moeten worden uit de datastroom. Deze mogelijkheid zou de internettap gerichter en efficiënter kunnen maken. Daarnaast wordt deze uitbreiding genoemd als mogelijkheid om de privacyschending van een getapt persoon te verminderen.

Geheimhouders en de internettap

Voor communicatie met geheimhouders onderschept door middel van een internettap bestaan, in tegenstelling tot geheimhouders in de telefoontap, geen protocollen en zijn geen procedures afgesproken. Digitale specialisten zijn zich er van bewust dat dit een probleem is dat niet eenvoudig te repareren valt. Het uitgangspunt van de wet, dat de opsporingdiensten communicatie met geheimhouders moeten verwijderen uit de getapte data, is onuitvoerbaar bij een internettap omdat het te veel data betreft waarin men moet gaan zoeken naar informatie die opsporingsdiensten niet mogen zien. Daarnaast is het verwijderen van stukjes informatie uit de onderschepte data technisch een lastig probleem. Over de mogelijkheden van het filteren van geheimhouders uit de internettap wordt hard nagedacht. Bij de ULI is men bezig protocollen te ontwikkelen om het scannen naar geheimhouders automatisch te laten verlopen. Men hoopt op korte termijn een oplossing te vinden.

Aftapbaarheid

Door toename van encryptie wordt het steeds moeilijker om onlinecommunicatie inhoudelijk te onderscheppen. Encryptie wordt door een aantal respondenten gezien als een tool die wordt gebruikt wanneer iemand iets te verbergen heeft. Echter, betere beveiliging van het internet is van belang voor de veiligheid van personen, hun geld en hun goederen. Om ervoor te zorgen dat de opsporing toch bij de inhoud van communicatie over internet kan komen, wordt geopperd om mee te luisteren of te kijken voordat de encryptie of afscherming heeft plaatsgevonden. Het binnendringen van een computer of smartphone op afstand is een techniek die dit mogelijk maakt. Vanuit het OM is aan de minister van Veiligheid en Justitiegeadviseerd om de mogelijkheden van het op afstand betreden van computers te onderzoeken.

Alternatieven

Binnen een opsporingsonderzoek worden meestal meerdere opsporingsmiddelen ingezet. De keuze voor een bepaald opsporingsmiddel wordt bepaald door het soort misdrijf (proportionaliteitseis), de beschikbare capaciteit, persoonlijk voorkeur, kennis en ervaring, doorlooptijd van het onderzoek en door administratieve hobbels en stroperige procedures. Er zijn twee teams - één op landelijk niveau en één in een onderzochte regio - bezig om opsporingsonderzoeken te verrichten zonder (grootschalige) inzet van de tap. Deze respondenten geven aan dat de tap relatief gemakkelijk wordt ingezet en dat dit mogelijk van invloed is op de creativiteit waarmee gezocht wordt naar andere manieren om de benodigde opsporingsinformatie te kunnen achterhalen. Deze teams, die nog in de kinderschoenen staan, zijn minder dan traditionele opsporingsteams gericht op het oplossen van individuele strafzaken. De aanpak van deze teams is meer programmatisch/thematisch, waarbij het oplossen van een strafzaak ondergeschikt is gemaakt aan het oplossen van een groter maatschappelijk probleem, dat niet alleen met het strafrecht, maar ook met behulp van preventieve of bestuurlijke maatregelen kan worden aangepakt.

Naast de tap maken respondenten gebruik van andere heimelijke opsporingsmiddelen, maar in Nederland kent de tap niet echt een gelijkwaardig alternatief. Wanneer andere bijzondere opsporingsmiddelen worden ingezet, is de tap vaak nodig als input om het opsporingsmiddel adequaat in te kunnen zetten.
Daarnaast is de doelstelling bij de inzet van deze opsporingsmiddelen vaak anders dan bij de tap en is de fase waarin het onderzoek verkeert op het moment van inzet anders. Mogelijk kan met de inzet van deze bijzondere opsporingsmiddelen de inzet van de tap wel worden verkort.
De telefoontap is een opsporingsmiddel waarmee men ongezien dicht bij een verdachte kan komen. Zeker wanneer verdachten erg bedacht zijn op politieaandacht is het lastig bepaalde andere opsporingsmiddelen in te zetten omdat de kans op ontdekking, en daarmee het afbreukrisico van het onderzoek, erg groot is. De keuze voor de telefoontap is met name ingegeven door de snelheid waarmee het opsporingsmiddel kan worden ingezet en doordat er weinig risico’s verbonden zijn aan de inzet van de tap. Andere bijzondere opsporingsbevoegdheden vergen voorbereidingstijd, waardoor er een kans bestaat dat er in

de tussentijd kostbare opsporingsinformatie verloren gaat. Daarnaast kennen deze methoden zoals gezegd een groter afbreukrisico. Door het ontbreken van alternatieven voor de telefoontap is de subsidiariteitseis dus feitelijk een formaliteit en een juridische eis waarvan de uitkomst van te voren vaststaat.

Wet- en regelgeving in de vergelijkingslanden

In dit onderzoek is de wijze waarop de tap in Nederland wordt ingezet vergeleken met de wijze waarop de tap wordt ingezet in drie andere Europese landen, namelijk Engeland en Wales, Zweden en Duitsland. Omdat er door de inzet van de tap een inbreuk wordt gemaakt op het recht op privacy, een grondrecht dat door het Europees Verdrag voor de Rechten van de Mens wordt gewaarborgd, is de inzet van de tap met waarborgen omkleed. Evenals in Nederland, heeft het gebruik van de telefoon- en internettap in Engeland en Wales, Zweden en Duitsland een wettelijke basis gekregen. Op enkele aspecten die in deze wetten zijn vastgelegd gaan we hier nader in.
In Nederland, Duitsland en Zweden is de rechterlijke toetsing het sluitstuk van het autorisatieproces dat moet leiden tot een tapbevel. Het is hierbij steeds de openbaar aanklager (OvJ) die een verzoek tot het gebruik van de telefoon- of internettap voorlegt aan de (onderzoeks)rechter (RC). In Engeland en Wales blijft de openbaar aanklager buiten het autorisatieproces en wordt het gebruik van de telefoon- of internettap geautoriseerd door een Secretary of State in plaats van een rechter. Daarmee lijken Engeland en Wales niet letterlijk te voldoen aan de verdragsrechtelijke vereisten van de rechterlijke toetsing. Niettemin heeft het EHRM in de zaak *Kennedy tegen het Verenigd Koninkrijk* (18 mei 2010) geoordeeld dat er op dit punt geen sprake is van een tekortkoming in de Britse regeling (RIPA 2000).
Of het gebruik van de telefoon- of internettap wordt geautoriseerd, hangt in alle onderzochte landen af van de beoordeling van de ernst van het misdrijf – waarbij wordt nagegaan of de privacy-inbreuk opweegt tegen de ernst van het feit dat men wil onderzoeken - en de vraag of de informatie die met de tap kan worden achterhaald nodig is voor de voortgang van de opsporing en of deze informatie al of niet op een andere wijze verkregen kan worden die minder inbreuk maakt op de privacy van de burger (eisen van proportionaliteit en subsidiariteit). De misdrijven waarvoor de tap kan worden ingezet, worden in alle onderzochte landen bepaald in een wettelijke regeling. Hoewel de regelingen per land verschillen betreft het steeds ernstige delicten. Daarnaast geldt voor alle onderzochte landen dat de tap niet alleen ten aanzien van verdachten kan worden ingezet, maar ook voor niet verdachten (betrokkenen).
De maximale termijn waarvoor een tapbevel (en de eventuele verlenging van dat tapbevel) geldt verschilt per onderzocht land. In Nederland geldt een termijn van 4 weken, in Zweden een termijn van een maand. In Engeland en Wales geldt een termijn van 3 maanden. In Duitsland geldt eveneens een termijn van 3 maanden.
In Zweden en Duitsland mogen tapgesprekken, net als in Nederland, gebruikt worden als bewijsmiddel in een strafzaak. In Engeland en Wales mag dat niet indien de informatie is verzameld op basis van een Engels tapbevel. In 2008 is een door de Britse regering ingestelde commissie, de *Privy Council*, evenwel tot de conclusie gekomen dat informatie verkregen door gebruikmaking van de telefoon- of internettap in beginsel wel zou moeten worden gebruikt als bewijsmiddel in een strafzaak. Vooralsnog is deze aanbeveling niet overgenomen door de Britse regering. Komt het materiaal uit het buitenland, bijvoorbeeld Nederland en is het naar Nederlandse maatstaven rechtmatig verkregen dan mag het in een Engelse strafzaak wel als bewijs worden gebruikt.
In het kader van verdere waarborgen tegen de schending van de privacy (onder andere art. 8 EVRM) is in Nederland, Duitsland en Zweden een regeling van kracht waarbij een burger die is onderworpen aan een telefoon- of internettap achteraf moet worden genotificeerd over het gebruik van dit heimelijke opsporingsmiddel. In Engeland en Wales bestaat een dergelijke regeling niet. Naar aanleiding van een notificatie kan een burger vervolgens beklag doen over bijvoorbeeld een mogelijke schending van de privacy. Hoewel een notificatie natuurlijk geen constitutief vereiste is om (eventueel later) beklag te doen, kan het wel dienstbaar zijn aan de rechtsbescherming van een burger. Voor het doen van beklag

bestaan er in Engeland en Wales en Zweden onafhankelijke instanties die een klacht in behandeling kunnen nemen. Daarnaast kent Zweden de figuur van de Openbaar Vertegenwoordiger (*Offentliga Ombud*), die als taak heeft om in de opsporing de rechten en integriteitbelangen van individuen in het algemeen te bewaken. Daarbij dient deze vertegenwoordiger tevens toe te zien op de bescherming van de integriteit van derden.

Inzet van de tap in de vergelijkingslanden

Statistieken

De statistieken tussen de landen zijn niet één op één te vergelijken door de verschillende wijzen van administreren. Zo wordt het aantal taps in Engeland en Wales op persoonsniveau geregistreerd terwijl in Nederland en Duitsland per getapt telefoonnummer of toestelnummer wordt geteld. In Zweden kunnen er meerdere tapbevelen worden afgegeven op één persoon, en binnen elk bevel kunnen weer meerdere nummers of toestellen worden opgenomen. Daarnaast verschillen de periodes waarover de tapcijfers bekend zijn per vergelijkingsland. Desondanks kan uit de statistieken worden opgemaakt dat voor alle onderzochte vergelijkingslanden (Engeland en Wales, Zweden en Duitsland) geldt dat sprake is van een stijging van het aantal uitgegeven tapbevelen over de afgelopen jaren.
Voor Engeland en Wales geldt dat er niet veelvuldig van de telefoontap gebruikt wordt gemaakt. De (bescheiden) stijging in de periode van 2008 tot en met 2010 wordt toegeschreven aan een groei in het aantal gevallen van zware criminaliteit en bedreigingen van de nationale veiligheid van het Verenigd Koninkrijk. Ook in Zweden wordt in absolute zin niet frequent getapt en heeft een klein aantal omvangrijke opsporingsonderzoeken al snel een grote invloed op de jaarcijfers. In Zweden is het aantal tapbevelen in de periode van 1999 tot en met 2008 gestaag gestegen, en in 2009 – met een stijging van 67% ten opzichte van het jaar ervoor – zelfs zeer fors. De gemiddelde aftaptijd gerekend in dagen daalde in 2009 echter met 34% ten opzichte van het jaar ervoor. Als verklaring van de stijging van het aantal tapbevelen wordt gewezen op de nationale inzet tegen zware georganiseerde criminaliteit die in 2009 van start ging. Dit heeft geresulteerd in een stijging van het aantal opsporingsonderzoeken waarbij het aftappen van telecommunicatie is gebruikt. Hoewel op basis van de gerapporteerde cijfers blijkt dat er in Duitsland niet zoveel wordt getapt als in Nederland, is het beeld dat uit de interviews naar voren komt over de wijze waarop de tap in de praktijk wordt ingezet verder vergelijkbaar met dat in Nederland. Met betrekking tot het aantal tapbevelen voor vaste lijnen in de periode van 1998 tot en met 2007 valt een bescheiden groei te zien. Over dezelfde periode is het aantal tapbevelen betreffende mobiele telefoons evenwel exponentieel gestegen. Een verklaring voor de grote toename van uitgegeven tapbevelen voor mobiele telefoons over de periode 1998-2007 is vermoedelijk gelegen in de exponentiële groei in het gebruik van mobiele telefoons van de laatste jaren. Binnen de groep van afgetapte personen specificeert zich dit in het frequent wisselen van telefoonkaarten of mobiele telefoons. Met betrekking tot internettaps zijn geen cijfers bekend van de onderzochte vergelijkingslanden.

Ook voor het gebruik van verkeergegevens (inclusief abonneegegevens) is voor alle vergelijkingslanden een stijging te zien. Zo is er in Engeland en Wales over de periode van 2008 tot en met 2010 een beperkte groei te zien (van ongeveer 5%) van het aantal verzoeken om gebruik te kunnen maken van verkeersgegevens. In Zweden is het aantal machtigingen afgegeven voor het binnenhalen van verkeersgegevens in 2009 met 47% gestegen ten opzichte van 2008; maar het gemiddeld aantal dagen waarin verkeergegevens werden binnengehaald daalde in 2009 met 35% vergeleken met het jaar ervoor. De stijging van het binnenhalen van verkeersgegevens hangt nauw samen met het gestegen aantal machtigingen voor het aftappen van telecommunicatie. Met betrekking tot Duitsland is het aantal verzoeken om gebruik te kunnen maken van abonneegegevens in de periode van 2001 tot en met 2010 exponentieel gestegen. Dit lijkt samen te hangen met de stijging van het gebruik van mobiele telefoons en de stijging van het aantal tapbevelen voor mobiele telefoons, en met het opvragen van verkeersgegevens. Hoewel concrete en actuele cijfers vooralsnog ontbreken, lijkt het gebruik van verkeersgegevens in Duitsland steeds belangrijker te worden in de opsporing.

Waar in Nederland met name gebruik wordt gemaakt van de telefoontap als heimelijk opsporingsmiddel, valt uit de cijfers over Engeland en Wales af te leiden dat in de periode van 2006 tot en met 2010 veel meer gebruik is gemaakt van *Covert Human Intelligence Sources* (CHIS) dan van de telefoon- of internettap. In Zweden liggen die verhoudingen anders, omdat daar circa 75% van alle afgegeven machtigingen betreffende heimelijke opsporingsmethoden betrekking heeft op de telefoon- of internettap. Dit betekent wel dat nog altijd 25% van alle machtigingen in 2009 betrekking heeft op andere heimelijke opsporingsmethoden. Over Duitsland zijn met betrekking tot dit punt geen cijfers gevonden.

Gebruik in de praktijk

In de bestrijding en de opsporing van de zware en georganiseerde criminaliteit wordt in alle onderzochte landen het gebruik van de telefoon- en internettap en van verkeersgegevens hoog aangeschreven. In Engeland en Wales wordt het opvragen van verkeersgegevens veelal als eerste opsporingsmiddel ingezet om zodoende een beeld te schetsen van (de gedragingen van) de betrokkene voordat gebruik wordt gemaakt van de telefoon- of internettap. Ook in Duitsland blijkt de inzet van het opvragen van verkeersgegevens zich als een zelfstandig opsporingsmiddel te ontwikkelen. Verder lijkt de gecombineerde inzet van de telefoontap met andere opsporingsmiddelen, zoals informanten en/of afluisterapparatuur, in de vergelijkingslanden een vruchtbare methode te zijn. Omdat verdachten van zware en/of georganiseerde criminaliteit via de telefoon weinig prijs geven over hun handel en wandel met betrekking tot hun (vermeend) criminele activiteiten, is dat voor opsporingsdiensten een reden om naast de telefoontap ook gebruik te maken van andere opsporingsmiddelen. Bovendien heeft het aftappen van telecommunicatie een meerwaarde als het gaat om het vergaren van informatie aan de hand waarvan verder onderzoek kan worden gedaan. Voor Engeland en Wales vloeit dit logischerwijze voort uit de omstandigheid dat tapgesprekken en –verslagen (doorgaans) niet als bewijs in een strafzaak mogen worden gebruikt. Maar ook in Duitsland lijkt het er op dat tapgesprekken en/of –verslagen veelal niet als direct bewijsmiddel in een strafzaak worden gebruikt. De reden is dat ter zitting de betrouwbaarheid en/of volledigheid van de afgetapte telefoongesprekken nogal eens in twijfel wordt getrokken. In de landen waar tapgesprekken en –verslagen kunnen worden gebruikt als bewijsmiddel, wordt er door respondenten op gewezen dat de verslaglegging ervan een tijdrovende bezigheid is.

I

Introductie

1 Inleiding

De heersende gedachte is dat er in Nederland veel wordt getapt (Bureau Jansen & Jansen, 1999; Van de Pol, 2006). Dit beeld wordt ondersteund door internationaal onderzoek (Albrecht, Dorsch & Krüpe, 2003) waaruit naar voren komt dat er in Nederland vaker wordt getapt dan in de ons omringende Westerse landen. Met enige regelmaat verschijnen mediaberichten met koppen als 'Telefoontaps in Nederland; wordt Nederland een politiestaat?' (www.rechtennieuws.nl, 14-9-2010), 'Veel taps, weinig verantwoording' (Chavannes, 2008) of 'De politie tapt zich een ongeluk, of het helpt weet niemand' (www.depers.nl, 9-9-2009). In deze berichten is het vooral het gebrek aan informatie over het gebruik van de tap dat de toon bepaalt. Het beeld dat men heeft over de tap wordt dan ook niet gevoed door recent onderzoek dat voor de huidige praktijk van het tappen kan gelden. Dit geldt voor zowel de toepassing van de telefoontap als van de internettap. Het laatste WODC-onderzoek naar het gebruik van de telefoontap heeft plaatsgevonden in 1996 (Reijne, Kouwenberg & Keizer, 1996; Keizer & Kouwenberg, 1996)[3] en sindsdien is de wereld van de telefonie - mede door de explosieve toename van het gebruik van de mobiele telefoon - totaal veranderd (zie bijvoorbeeld; ITU, telecommunication/ ICT Indicator Database, 2011). Ten tijde van dat onderzoek hadden de meeste huishoudens slechts één koperen draad voor een vaste telefoonaansluiting en één abonnement op naam bij PTT Telecom (Bernardt & Canoy, 1997). Nu, anno 2012, zijn er meer mobiele telefoons in Nederland dan inwoners (OPTA, 2009) en wordt het onderscheid tussen vaste telefonie en het bellen via een internetlijn steeds kleiner. Naar aanleiding van vragen uit de Tweede Kamer over de jaarlijkse tapstatistieken heeft de toenmalige minister van Justitie een onderzoek naar het gebruik van de telefoontap toegezegd. De politieke belangstelling voor dit onderzoek lijkt vooral te zijn ingegeven door het belang dat wordt gehecht aan de bescherming van de persoonlijke levenssfeer (*Kamerstukken II* 2009/10, 30 517, nr. 16). De inzet van de tap beperkt zich namelijk niet tot verdachten. Voor de inwerkingtreding van de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB), moest men om te kunnen tappen een redelijk vermoeden hebben dat de verdachte aan het te tappen verkeer deelnam. Met de inwerkingtreding van de Wet BOB kunnen ook niet-verdachte personen, indien het onderzoek dit dringend vordert, worden getapt (zie hierover Bokhorst, De Kogel en Van der Meij, 2002, p. 45-46; Bokhorst, 2004; De Poot, Bokhorst, Van Koppen & Muller, 2004, p. 162-163). Hierdoor is de kring van personen die getapt kan worden verruimd. In 2010 werden er in Nederland 22.006 telefoon- en 1.704 internettaps aangesloten. Echter, cijfers over aantallen taps zeggen op zichzelf niet veel en krijgen pas betekenis en kleur als er inzicht bestaat in het feitelijke gebruik van de tap. Wat zijn bijvoorbeeld de motieven en afwegingen die een rol spelen bij de beslissing om een telefoon- of internettap aan te sluiten? En waarom wordt er gekozen voor een tap in plaats van een ander opsporingsmiddel dat mogelijk minder inbreuk maakt op de persoonlijke levenssfeer van de mensen die aan dit middel worden onderworpen? Het doel van dit onderzoek is dan ook het bieden van inzicht in het feitelijk gebruik van de bijzondere opsporingsbevoegdheid van de telefoon- en internettap bij de opsporing van strafbare feiten. Hierbij wordt tevens beoogd inzicht te bieden in de wijze waarop rechters-commissarissen (RC's) tegen dit opsporingsmiddel aankijken en in de redenen waarom en de mate waarin zij tapaanvragen toe- en afwijzen. De Wet BOB schrijft voor dat personen die zijn getapt hierover achteraf dienen te worden ingelicht, de zogenaamde notificatieplicht. Ook de mate waarin deze notificatieplicht wordt nageleefd, zal in dit onderzoek worden belicht.

[3] Sinds die tijd verschenen er in Nederland geen omvattende onderzoeken naar het gebruik van de tap in de opsporingspraktijk. Wel werd in het onderzoek van De Poot et al. (2004, p. 161-182) uitgebreid aandacht besteed aan het gebruik van de tap bij de opsporing en vervolging van ernstige misdrijven zoals drugshandel en levensdelicten (zie hierover ook Bokhorst, 2004) en verscheen er in 2006 een proefschrift waarin antwoord werd gezocht op de vraag of de wetgeving op het gebied van het aftappen van communicatie en het verzamelen van verkeersgegevens nog is toegesneden op nieuwe communicatietechnieken, zoals e-mail, sms en internettelefonie (Smits, 2006).

1.1 Probleemstelling en onderzoeksvragen

De studie die voor u ligt heeft als doel inzicht te bieden in het feitelijke gebruik van de telefoon- en internettap bij de opsporing van strafbare feiten. Van belang om te vermelden is dat een effectiviteitsmeting van telefoon- en internettaps geen onderdeel uitmaakt van dit onderzoek. De reden hiervoor is dat het niet haalbaar is om de effectiviteit van het tappen betrouwbaar en valide te meten. Telefoon- en internettaps worden ingezet om het oplossen van een misdrijf of het opsporen van een dader te bevorderen, maar dat betekent niet dat de tap pas geslaagd is als er een bekentenis over de telefoon te beluisteren is, of als er letterlijk gegevens worden uitgewisseld over de verblijfplaats van een gezochte persoon. De bijdrage van de tap aan het resultaat van het onderzoek ligt subtieler en is feitelijk alleen in samenhang en in wisselwerking met andere ingezette opsporingsmethoden goed te evalueren. Om een oordeel te kunnen geven over de effectiviteit van de tap in een opsporingsonderzoek is het nodig om de brede achtergrond van het onderzoek en van het doel van de tap te kennen. De ene tap is eenvoudigweg de andere niet. Om de effectiviteit van de tap te kunnen meten, zou het niet alleen nodig zijn om na te gaan hoe een X aantal getapte telefoon- en internetlijnen zich verhoudt tot een X aantal aanhoudingen, opgeloste zaken, veroordelingen of zaken waarin de onschuld van een verdachte persoon kon worden bewezen, maar zou ook onderzocht moeten worden wat de precieze bijdrage van de tap daarbij is geweest. Daarbij komt nog dat personen vaak via meerdere nummers en IP-adressen communiceren. Stel dat één van deze afgetapte lijnen zinvolle opsporingsinformatie oplevert, zijn de andere afgetapte lijnen daarmee dan niet effectief? Een dergelijke effectiviteitsmaat zou impliceren dat je van tevoren kunt bedenken met welke in gebruik zijnde telefoon een verdachte over bepaalde zaken zal communiceren. Het aantal telefoontaps per jaar laat zich eenvoudigweg niet vertalen naar een schaal of maat waaruit de effectiviteit blijkt. In hoeverre het gebruik van de tap tijdens de opsporing daadwerkelijk kan worden gekwalificeerd als (in)effectief valt daarmee buiten het bereik van dit onderzoek. Wel wordt bestudeerd op welke wijze de tap wordt ingezet, welke overwegingen en doelen daaraan ten grondslag liggen, welke resultaten daarmee kunnen worden bereikt, en welke opsporingsmiddelen als alternatief voor de tap zouden kunnen dienen.
Om de Nederlandse tapcijfers in een internationaal kader te kunnen plaatsen, is het tweede doel van dit onderzoek inzicht te verschaffen in de wijze waarop een aantal West-Europese landen gebruik maakt van de tap en van andere opsporingsmethoden die gericht zijn op het inwinnen van informatie over verdachten, misdrijven en relaties tussen verdachten onderling en met derden. In het onderzoek wordt daarom uitgegaan van een getrapte probleemstelling:

- Hoe wordt in Nederland gebruik gemaakt van de telefoon- en internettap tijdens het opsporingsproces?
- Hoe wordt in enkele andere West-Europese landen met dit opsporingsmiddel omgegaan?
- Kunnen (grote) verschillen tussen landen in het gebruik van dit opsporingsmiddel worden verklaard?

Om antwoorden te vinden op de hierboven gestelde vragen is onderzoek verricht naar 1) de mogelijkheden en beperkingen van de telefoon- en internettap in de praktijk; 2) het wettelijk kader en het gebruik van de tap in Nederland en 3) het wettelijk kader en het gebruik van de tap in drie vergelijkingslanden. Hiertoe formuleerden we de volgende onderzoeksvragen, die in verschillende delen van dit onderzoeksrapport worden beantwoord:

Wettelijk kader en procedurele aspecten in Nederland

- Hoe is het gebruik van de telefoon- en internettap voor de opsporing in Nederland gereguleerd?
- Welke spelers zijn er betrokken bij de inzet van een tap en welke procedures dienen hierbij te worden gevolgd?

Inzet van de tap in de Nederlandse opsporingspraktijk

- Bij welk soort zaken en in welke situaties besluit een opsporingsteam om in een opsporingsonderzoek gebruik te maken van de tap? En met welk doel gebeurt dit?
- Is bij benadering aan te geven hoeveel telefoon- en internetlijnen er deze verschillende situaties worden afgetapt en hoe lang de tap in deze zaken wordt ingezet?
- Welke rol spelen de politie, de officier van justitie (OvJ) en de RC in de praktijk bij het besluit om te gaan tappen, en wat is hun rol als de tap eenmaal is ingezet?
- Hoe worden de bevoegdheden en verplichtingen die voortvloeien uit de wet- en regelgeving betreffende het gebruik van de bijzondere opsporingsmethode van de tap in de praktijk ingevuld?
- Hoe worden de beginselen van proportionaliteit en subsidiariteit gewogen bij het besluit om te gaan tappen?
- In welke situaties kiest het opsporingsteam voor het gebruik van een 'spoedtap' en is het bij benadering aan te geven hoe vaak (in relatie tot het totale aantal zaken waarin een tap wordt ingezet) deze situaties zich voordoen?
- Wordt bij de toekenning van een tapaanvraag rekening gehouden met de vraag of het om een verdachte gaat of om een betrokkene?
- Hoe wordt in opsporingsonderzoeken gebruik gemaakt van de informatie uit de tap?
- Zijn er in situaties waarin gebruik wordt gemaakt van de tap ook andere opsporingsmiddelen beschikbaar waarmee de gewenste informatie kan worden achterhaald of waarmee hetzelfde doel kan worden bereikt? Zo ja, wat bepaalt in dat geval de keuze voor het gebruik van de tap?

Wettelijk kader en procedurele aspecten en inzet van de tap in de geselecteerde vergelijkingslanden
Hierin worden zoveel mogelijk dezelfde aspecten van het tappen onderzocht als in het Nederlandse deel van het onderzoek.

- Hoe is het gebruik van de telefoon- en internettap voor de opsporing in de geselecteerde vergelijkingslanden gereguleerd in de nationale wet- en regelgeving?
- Welke spelers zijn er betrokken bij de inzet van een tap en welke procedures dienen hierbij te worden gevolgd?
- Hoe wordt de tap in de praktijk ingezet bij de opsporing van strafbare feiten?

In de slotbeschouwing wordt ingegaan op in het oog springende overeenkomsten en verschillen tussen de vier bestudeerde landen als het gaat om de (on)mogelijkheden om de telefoon- en internettap in te zetten in de opsporing, en worden overeenkomsten en verschillen in de mate waarin de tap in de praktijk wordt ingezet nader geduid.

1.2 De opzet van het onderzoek

1.2.1 Gebruikte onderzoeksmethoden

Op bovengenoemde onderzoeksvragen is antwoord gezocht met behulp van verschillende onderzoeksmethoden.

Voor de beschrijving van de telefoon- en internetmarkt en de gevolgen van ontwikkelingen op dit gebied voor de mogelijkheden om telecommunicatie en dataverkeer af te tappen ten behoeve van de opsporing, is gebruik gemaakt van literatuuronderzoek en interviews met experts.

Voor de beschrijvingen van de wet- en regelgeving in Nederland en in de geselecteerde vergelijkingslanden is eveneens vooral gebruik gemaakt van literatuuronderzoek. Voor dit

deel van het onderzoek zijn de wetteksten en toelichtingen daarop, lagere regelgeving, kamerstukken, schriftelijke stukken van uitvoeringsinstanties en wetenschappelijke literatuur bestudeerd. Daarnaast is de vigerende wet- en regelgeving in elk van de onderzochte landen ook onderwerp geweest van gesprek tijdens interviews.

Om inzicht te kunnen bieden in de wijze waarop de telefoon- en internettap in de opsporing worden gebruikt, de overwegingen die aan de inzet van dit instrument ten grondslag liggen en de resultaten die ermee worden behaald, is gebruik gemaakt van verschillende onderzoeksmethoden. Naast de bestudering van nationale en internationale vakliteratuur, is kwantitatieve en kwalitatieve informatie verzameld over het gebruik van de tap. In Nederland zijn hierover gegevens verzameld bij onder andere de Unit Landelijke Interceptie (ULI), de politie, de rechterlijke macht (openbaar ministerie en zittende magistratuur) en de advocatuur. In de vergelijkingslanden werd vooral informatie verzameld bij de politie en de rechterlijke macht.

1.2.2 De vergelijkingslanden

Door de inzet van de telefoon- en internettap in Nederland te vergelijken met de inzet van de tap in enkele vergelijkingslanden, wordt getracht verschillen tussen deze landen als het gaat om de tapstatistieken te verklaren. Hiertoe is onderzocht op welke wijze het gebruik van de telefoon- en internettap in deze vergelijkingslanden wettelijk en praktisch is geregeld en op welke wijze de tap in deze vergelijkingslanden wordt ingezet in de opsporingspraktijk. Tevens is nagegaan op welke wijze de cijfers over het gebruik van de tap in deze landen tot stand zijn gekomen.

Voor deze vergelijking hebben we drie landen geselecteerd. Bij de keuze voor deze landen, hebben de variëteit in juridische verwantschap aan het Nederlandse strafrechtssysteem en het lidmaatschap van de Raad van Europa (*Council of Europe*) als selectiecriteria gediend. Een lidmaatschap geldt hier als regulerend element voor de te onderzoeken landen; De Raad van Europa (*Council of Europe*) – niet te verwarren met de Europese Unie of de Europese Raad – is een organisatie waar 47 Europese landen lid van zijn. De Raad is opgericht in 1949 met het Verdrag van Londen en heeft tot doel de ontwikkeling van democratische principes gebaseerd op het Europees Verdrag van de Rechten van de Mens (*EVRM*) en andere relevante regelgeving voor de bescherming van individuen (zie www.coe.int). Het Europese Hof voor de Rechten van de Mens (*EHRM*) is een orgaan van de Raad van Europa. Op grond van deze criteria zijn *Engeland en Wales*, *Zweden* en *Duitsland* als vergelijkingslanden gekozen.

1.2.3 De Nederlandse politieregio's

Voor het Nederlandse deel van het onderzoek zijn gegevens verzameld op landelijk niveau, maar ook op het niveau van de regio's, de districten en de wijkteams. De tap kan bij verschillende soorten opsporingsonderzoeken worden ingezet. Bij grote projectmatige onderzoeken die op landelijk en op regionaal niveau worden verricht, of die uitgevoerd worden door bijzondere opsporingsdiensten, bij ad-hoc onderzoeken naar middencriminaliteit die plaatsvinden op regionaal- en districtsniveau en bij vormen van criminaliteit waar wijkteams onderzoek naar verrichten – zoals straatroof. Om te kunnen onderzoeken op welke wijze de tap bij deze verschillende criminaliteitsvormen wordt ingezet en welke overwegingen aan de inzet van de tap ten grondslag liggen, zijn twee uiteenlopende politieregio's geselecteerd. De wijze waarop de tap in de opsporingspraktijk wordt ingezet hangt namelijk niet alleen af van de aard van het misdrijf dat wordt onderzocht en van het doel dat het opsporingsteam voor ogen staat (De Poot et al., 2004; Bokhorst, 2004), maar ook van het totale aanbod aan zaken waarmee men te maken heeft, de personele bezetting en de werkwijzen die men heeft ontwikkeld (De Poot et al., 2004). Dit kan per regio verschillen, vandaar dat het interessant is om het gebruik van de tap in twee uiteenlopende politieregio's te bestuderen. De keuze voor de onderzochte regio's is tot stand gekomen op basis van adviezen van experts die vanuit hun professie een centraal overzicht hebben van

de wijze waarop de tap in verschillende regio's wordt ingezet. Regio A is een regio in de Randstad. Regio B is een middelgrote regio, die opvalt door de manier waarop het proces rond het tappen is georganiseerd. Beide regio's hebben hun eigen kenmerken en werkwijzen. Een vergelijking van het aantal taps dat jaarlijks in de geselecteerde regio's wordt ingezet, levert geen opvallende verschillen op met andere vergelijkbare politieregio's. Er dan ook zijn geen redenen om aan te nemen dat de algemene bevindingen uit dit onderzoek niet gelden voor andere Nederlandse politieregio's. Het is nadrukkelijk niet de bedoeling om een vergelijking te maken tussen deze twee regio's, maar op punten zullen relevante verschillen tussen de regio's worden besproken. De geselecteerde regio's hebben de volgende kenmerken:

Regio A kan worden omschreven als een groot korps dat een grote stad en een aantal gemeenten omvat. Het gebied heeft bijna één miljoen inwoners en een hoge bevolkingsdichtheid.

Regio B kan worden omschreven worden als een kleiner korps dat een aantal gemeenten en twee middelgrote steden omvat. Het gebied telt bijna een half miljoen inwoners en heeft een lage bevolkingsdichtheid.

1.2.4 Het empirische onderzoek: de selectie van respondenten in Nederland

Bij een projectmatig onderzoek naar georganiseerde misdaad wordt de tap op een andere wijze gebruikt dan bij een ad-hoc onderzoek naar een moordzaak of een grote overval. Bij een grote overval wordt weer anders getapt dan bij een straatroof. Om een breed beeld te kunnen schetsen van het gebruik van de tap in de opsporingspraktijk en van de overwegingen die daaraan ten grondslag liggen, hebben we medewerkers geïnterviewd van de politie, de rechterlijke macht (openbaar ministerie en zittende magistratuur) en van bijzondere opsporingsdiensten. Dit onderzoek is verricht op landelijk niveau en in twee regio's die van elkaar verschillen in het aanbod aan misdrijven, de personele bezetting en de wijze waarop activiteiten die gepaard gaan met de inzet van bijzondere opsporingsbevoegdheden zijn georganiseerd.

Voor elk van de gebieden waarover informatie is verzameld werd eerst contact gezocht met een politiemedewerker met expertise op het specifieke gebied. Na afloop van het interview werd de respondent gevraagd met welke OvJ's zijn of haar team vaak samenwerkt. Voorts benaderden we één van hen om het beeld over de wijze waarop de tap op het specifieke gebied wordt ingezet en de factoren die een rol spelen bij de overwegingen en beslissingen daaromtrent verder in te kunnen vullen vanuit het perspectief van de magistratuur. Vervolgens voerden we gesprekken met RC's, parketsecretarissen en strafrechtadvocaten om dit beeld verder te kunnen completeren.

Voor het Nederlandse gedeelte van dit onderzoek zijn in totaal 55 personen geïnterviewd. In de politieregio's en bij de Nationale Recherche zijn vooral teamleiders en interceptiecoördinatoren geïnterviewd. Daarnaast hebben we experts geïnterviewd van de Unit Landelijke Interceptie (ULI) en van andere specialistische onderdelen van het Korps Landelijke Politiediensten (KLPD). Bij de parketten spraken we vooral met OvJ's en met een enkele parketsecretaris; bij het Kabinet van de RC spraken we met RC's. Voorts spraken we advocaten, een enkele expert van een bijzondere opsporingsdienst en van het functioneel parket en enkele experts die niet verbonden zijn aan de genoemde organisaties. Hieronder staat een overzicht van de organisaties waarbij de door ons geïnterviewde sleutelpersonen werkzaam zijn.

Unit Landelijke Interceptie (3)
Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) (1)
Platform Interceptie, Decryptie & Signaalanalyse (PIDS) (2)
Politie (26)
Openbaar Ministerie (OM) (12)
Fiscale Inlichtingen- en Opsporingsdienst (FIOD) (1)

Kabinet RC (4)
Advocatuur (4)
Nederlandse Orde van Advocaten (NOvA) (1)
Bits of Freedom (BoF) (1)

1.2.5 Selectie van respondenten in de vergelijkingslanden

In de geselecteerde landen zijn gesprekken gevoerd met deskundigen op het gebied van het (verzamelen van gegevens over) het aftappen van telefoon- en internetverkeer. In Zweden en Engeland en Wales zijn daarnaast ook gesprekken gevoerd met drie academische experts op het gebied van het strafprocesrecht en/of het politierecht.[4]

1.2.6 Werkwijze van het empirisch onderzoek

Ten behoeve van het Nederlandse onderzoek zijn in totaal 45 face-to-face en 3 telefonische interviews afgenomen in de periode van januari tot en met oktober 2011. Tijdens sommige interviews is gesproken met twee personen, wat heeft geleid tot een totaal van 55 geïnterviewden.

Voor de buitenlandse delen van het onderzoek zijn in totaal 14 mensen geïnterviewd. Het betroffen allemaal face-to-face interviews die plaatsvonden in de periode van april tot en met juni 2011. In Duitsland zijn gesprekken gevoerd met een openbaar aanklager (*Staatsanwalt*), deze functie is vergelijkbaar met die van OvJ in Nederland, en twee politiefunctionarissen van de Federale Politie (*Bundeskriminalamt*). In Zweden is gesproken met drie functionarissen van de Nationale Politie (*Rikskriminalpolisen*) en twee openbaar aanklagers van de Zweedse Vervolgingsautoriteit (*Åklagarmyndigheten*). In Engeland betrof het twee openbaar aanklagers (Public Prosecutors van de *Crown Prosecution Service*), een functionaris van de *Serious Organised Crime Agency* (SOCA), een functionaris van *Her Majesty's Revenue and Customs* (HMRC) en twee functionarissen van de *Home Office*.

Alle respondenten zijn geïnterviewd aan de hand van een semi-gestructureerde vragenlijst die een aantal vaste onderwerpen bevatte. Deze vragenlijst werd aangepast aan de functie of positie van de respondent. Daarnaast werd bij de meeste interviews uitgebreider stilgestaan bij specifieke thema's. De interviews namen gemiddeld anderhalf uur in beslag. Alle interviews zijn met toestemming van de respondenten opgenomen op audioapparatuur en voorts letterlijk uitgewerkt. Voor het Nederlandse deel zijn alle ingevoerde interviews geanonimiseerd en vervolgens gecodeerd door twee onderzoekers. De codelijst omvatte een puntsgewijze gedetailleerde uitwerking van alle onderwerpen die op de vragenlijst aan de orde zijn gekomen. Onderwerpen of uitspraken die niet of moeilijk te scoren waren zijn door de onderzoekers als "overig" gelabeld, en in een later stadium nader bekeken en waar relevant opgenomen in het rapport. Deze manier van werken maakt het mogelijk om met behulp van MaxQDa, een analyseprogramma voor kwalitatieve data analyse, de uitspraken van de respondenten over een bepaald onderwerp te selecteren en te analyseren. De codelijst heeft als uitgangspunt gediend bij het schrijven van de hoofdstukken 6, 7 en 8. De citaten die in deze hoofdstukken worden weergegeven staan niet op zichzelf. Ze zijn zorgvuldig gekozen en representeren steeds de mening van meerdere respondenten. Ze dienen om de in de tekst beschreven onderwerpen te illustreren.
Voor het buitenlandse deel geldt dat de interviews nadat ze letterlijk zijn uitgewerkt opnieuw zijn voorgelegd aan de respondenten die daar vervolgens, eventueel na kleine tekstuele aanpassingen, hun akkoord op hebben gegeven. Hierna is de informatie door één van de

[4] In Zweden betrof dat experts verbonden aan de Stockholm University en de Zweedse Nationale Raad voor Criminaliteitspreventie (Brottsförebyggande rådet, afgekort Brå). In Engeland is gesproken met een expert van het Institute of Criminal Justice Studies van de University of Portmouth.

onderzoekers geanalyseerd en gebruikt bij het schrijven van de hoofdstukken die handelen over het gebruik van de tap in de geselecteerde landen.

1.3 De opbouw van dit rapport

Dit rapport bestaat uit vier delen. In deel I is de inleiding besproken en zullen we in het volgende hoofdstuk (hoofdstuk 2) de ontwikkelingen op het gebied van de telefoon- en internetmarkt schetsen en de gevolgen daarvan voor de mogelijkheden om telecommunicatie en dataverkeer af te tappen ten behoeve van de opsporing. Voorts volgen het Nederlandse deel van het onderzoeksrapport (deel II), en het deel dat handelt over het gebruik van de tap in Engeland en Wales, Zweden en Duitsland (deel III). In de slotbeschouwing (deel IV) geven we een analyse van de overeenkomsten en verschillen in het gebruik van de tap in de vier onderzochte landen en plaatsen we de Nederlandse conclusies in internationaal perspectief.

2 De telefoon- en internetmarkt

Ten tijde van het voorgaande WODC-onderzoek naar het gebruik van de telefoontap in de opsporingspraktijk (Reijne et al., 1996) was de wereld van de telecommunicatie relatief eenvoudig. In Nederland was PTT Telecom destijds de enige aanbieder op de markt die telefoondiensten aanbood. De meeste huishoudens waren in het bezit van één telefoonnummer dat netjes op naam en adres stond geregistreerd voor de maandelijkse verrekening van de kosten. In Duitsland, Zweden en Engeland en Wales was dit niet anders. De explosieve toename van het telecommunicatieverkeer en de verandering van de wijze waarop telefoons tegenwoordig worden gebruikt heeft grote gevolgen voor de wijze waarop de telefoontap kan worden ingezet in de opsporingspraktijk. Aan de ene kant vindt er tegenwoordig veel meer communicatie plaats via de telefoon, aan de andere kant is de wijze waarop telefoons worden gebruikt ook meer versplinterd geraakt. Veel mensen hebben meerdere telefoons en maken daarnaast ook nog gebruik van internet om op afstand met anderen te kunnen communiceren. Hierdoor zal de politie vermoedelijk zowel breder moeten zoeken als dieper moeten graven om relevante informatie uit al deze communicatiestromen te kunnen achterhalen.
Ook het internet heeft zich de afgelopen twintig jaar sterk ontwikkeld. Deze ontwikkeling heeft het mogelijk gemaakt om voor opsporingsdoelen een internettap te plaatsen. Daarmee kunnen allerlei vormen van communicatie via het internet, zoals e-mails en chatgesprekken worden afgevangen en kan het internetgedrag van de gebruiker worden gevolgd.
Voor zover kon worden nagaan is er in geen van de onderzochte landen eerder onderzoek verricht naar het gebruik van de internettap in de opsporingspraktijk.

In dit hoofdstuk wordt de huidige situatie van de telefoon- en internetmarkt geschetst en wordt beschreven welke gevolgen ontwikkelingen hierin hebben voor het gebruik van de tap in de opsporingspraktijk.

2.1 Telefoniemarkt

De telecommarkt is de afgelopen jaren drastisch veranderd. Mobiele telefonie heeft het laatste decennium een enorme vlucht genomen en het mobieltje is niet meer weg te denken uit het dagelijks leven. In Nederland betrof het aantal mobiele telefoonaansluitingen in december 2010 19,8 miljoen naast de 6,8 miljoen vaste telefoonaansluitingen (TNO, 2011). Dit komt neer op 116 mobiele en 43 vaste telefoonaansluitingen per 100 inwoners in Nederland. In de andere onderzochte landen zijn dit 130 mobiele en 54 vaste lijnen in het Verenigd Koninkrijk, 114 mobiele en 53 vaste lijnen in Zweden, en in Duitsland 127 mobiele en 55 vaste lijnen per 100 inwoners (ITU, World Telecommunications/ICT indicator databast, 2011). Vroeger richtte de telecommarkt zich vooral op spraak, maar tegenwoordig richt deze sector zich steeds meer op data. Data worden al lang niet meer alleen via het internet op een computer verzonden, maar ook met mobiele telefoons. Een mobiele telefoon wordt niet meer alleen gebruikt om te bellen, maar kan bijvoorbeeld ook worden gebruikt om berichten mee te versturen, te fotograferen, muziek te beluisteren en om verbinding te maken met het internet. Verbinding met het internet is noodzakelijk om e-mails te kunnen verzenden en ontvangen en om in contact te blijven met vrienden door middel van diverse social media. Eind 2010 waren er in Nederland zoals gezegd 19,8 miljoen mobiele telefoonaansluitingen in gebruik. Meer dus dan het aantal inwoners (OPTA, 2011; TNO, 2011). Er is in Nederland een hoogwaardige infrastructuur nodig en aanwezig om dit te kunnen dragen. Om een vaste telefoonlijn te kunnen gebruiken moet er een abonnement worden afgesloten bij een aanbieder die de gewenste diensten levert. Er zijn verschillende aanbieders waaruit men kan kiezen. Bij het afsluiten van een abonnement moet de gebruiker zich laten registeren. Vervolgens wordt het maandelijkse bedrag verrekend met de abonnementhouder. Voor het activeren van een mobiele telefoon kan eveneens een abonnement worden afgesloten bij een aanbieder. Hiervoor zal de eigenaar van de mobiele telefoon zich, net als bij een abonnement op een vaste lijn, moeten registreren en legitimeren bij de aanbieder. De aanbieder levert

vervolgens een SIM-kaart. Nadat deze in de mobiele telefoon is geplaatst, is het toestel gebruiksklaar en kan er maandelijks een bedrag worden afgerekend. Mobiele telefoons kunnen echter ook worden gebruikt zonder dat er een abonnement wordt afgesloten. Zo wordt bij 31% van de mobiele telefoons in Nederland gebruik gemaakt van een zogenaamde prepaid SIM-kaart (OPTA, 2011). Dit is een SIM-kaart die een bepaalde waarde vertegenwoordigt. Na plaatsing in een telefoon kan met deze kaart contact worden gemaakt met het netwerk van de aanbieder. Deze kaarten worden door verschillende telecombedrijven op veel plaatsen te koop aangeboden en kunnen, nadat het tegoed is opgebruikt, op een later tijdstip opnieuw worden opgehoogd met een beltegoed. Hiervoor is geen registratie nodig en de gebruiker van het telefoonnummer dat aan de prepaid SIM-kaart is gekoppeld, is dan ook vaak niet bekend bij de aanbieder. Wanneer het beltegoed op is en men ervoor kiest het beltegoed op te hogen op dezelfde SIM-kaart, blijft de klant bij dezelfde aanbieder en blijf hetzelfde telefoonnummer in gebruik. Voor sommige gebruikers is het behouden van een telefoonnummer echter van ondergeschikt belang. Vaak wordt er bij de aanschaf van een nieuwe prepaid SIM-kaart extra beltegoed weggegeven. Dat kan een reden zijn om een nieuwe SIM-kaart aan te schaffen en er niet voor te kiezen om het beltegoed van een reeds in gebruik zijnde SIM-kaart op te hogen. Door een nieuwe prepaid SIM-kaart te kopen heeft men opnieuw toegang tot het netwerk van een aanbieder, maar wijzigt het telefoonnummer van de gebruiker. Door het gebruik van prepaid SIM-kaartjes is het bijzonder makkelijk om anoniem te bellen.
Elk mobiel toestel heeft, naast een telefoonnummer dat gekoppeld is aan de SIM-kaart, een uniek IMEI-nummer. Dit nummer wordt meegestuurd in de uitgaande datastroom van de telefoon. Wanneer de gebruiker van een telefoon regelmatig van SIM-kaart en van telefoonnummer wisselt, kan dit IMEI-nummer worden gebruikt voor de aanvraag van een telefoontap.

2.2 Het internet

Eind jaren zestig ontwikkelde het Advanced Research Projects Agency (ARPA) in opdracht van het Amerikaanse ministerie van Defensie een netwerk van meerdere computers. Dit netwerk, genaamd ARPANET, is de voorloper van het huidige internet en was uitsluitend bedoeld voor universitaire afdelingen voor computerwetenschap en particuliere onderzoeksinstituten die door dit ministerie werden gesubsidieerd (Universiteit Utrecht, z.j.). Inmiddels is het internet een wereldwijd netwerk waarvan het gebruik vooral sinds de jaren negentig een enorme vlucht heeft genomen. Zo'n 91% van de Nederlanders heeft toegang tot internet. Het gebruik van internet is dan ook populair, tweederde van de gebruikers bekijkt dagelijks de e-mail en bijna 20 % bezoekt dagelijks online communities, chat en bekijkt online video's. In Zweden maakt 90% van de inwoners gebruik van internet. In Duitsland en het Verenigd Koninkrijk is dit respectievelijk 82% en 85% (ITU, World Telecommunications/ICT indicator databast, 2011).
Wereldwijd is het aantal internetgebruikers tussen 2005 en 2010 verdubbeld. In een rapport van TNO werd geschat dat er in 2010 wereldwijd meer dan twee miljard internetgebruikers zouden zijn (TNO, 2010). Ook het gebruik van mobiel internet neemt fors toe. Volgens de OPTA was het totale dataverbruik in de eerste zes maanden van 2010 verachtvoudigd ten opzichte van het eerste halfjaar van 2008 (OPTA, 2011; TNO, 2011). Eind 2009 had 32% van de personen met een mobiele telefoon in Nederland een toestel met de mogelijkheid om contact te maken met het internet (TNO, 2010), en dat percentage neemt gestaag toe. Het internet wordt onder andere gebruikt om te winkelen, informatie op te zoeken, te bellen, e-mails te versturen, te gamen en gebruik te maken van social media. Inmiddels is het mogelijk om persoonlijke data op te slaan en te bewerken in 'the cloud'. Dit houdt in dat bijvoorbeeld foto's of andere gegevens bewaard en bewerkt kunnen worden op het internet in plaats van op de harde schijf van een personal computer (pc) of telefoon. Kortom, naast de fysieke wereld is er het internet: een digitale wereld waar veel mensen op acteren en die op heel veel verschillende manieren wordt gebruikt.
Wij hebben er bij het schrijven van dit rapport voor gekozen om het gebruik van de telefoontap en van de internettap apart te beschrijven, omdat dit onderscheid in alle onderzochte landen nog duidelijk zichtbaar is in de huidige opsporingspraktijk. Het is echter

te verwachten dat het onderscheid tussen telecommunicatie en dataverkeer op termijn zal komen te vervallen (CBP, 2007; Koops, Bekkers, Bongers & Fijnvandraat, 2005; Winkelhorst, 2006).
De afgelopen jaren is in de gepubliceerde tapstatistieken steeds onderscheid gemaakt tussen vaste en mobiele telefonie, maar dit onderscheid is in de tapstatistieken over het jaar 2010 komen te vervallen omdat deze verschillen door technologische veranderingen niet meer zo scherp zijn. Zoals de grenzen tussen vaste telefoonlijnen en mobiele telefoons zijn vervaagd, zo is ook de vervaging van grenzen tussen het telecommunicatie- en dataverkeer door het gebruik van internet momenteel goed zichtbaar. Tegenwoordig wordt er veel via het internet gebeld door gebruik te maken van Voice over IP (VoIP). In eerste instantie werd bellen via internet vooral gebruikt voor internationale contacten, omdat het een goedkope manier van bellen is. Maar doordat er steeds meer telefoons zijn met internetaansluitingen en het dus steeds eenvoudiger wordt om met een mobiele telefoon via het internet te bellen, wordt er ook steeds meer gebruik gemaakt van deze mogelijkheid voor dagelijkse binnenlandse communicatie. Deze diensten worden dikwijls vanuit het buitenland aangeboden waarbij de gesprekken vaak worden versleuteld. Het aftappen van de communicatie wordt hierdoor bemoeilijkt.

2.3 Grenzen aan de aftapbaarheid

Op verzoek van het ministerie van Economische Zaken onderzocht Stratix Consultancy hoe de aftapbaarheid van communicatiediensten het best gewaarborgd kan worden (Koops et al., 2005). 'Aftapbaar' duidt op het veiligstellen van gegevens ten behoeve van een onderzoek daarnaar met behulp van de telefoon- en internettap en door het vorderen van gebruikers- en verkeersgegevens. Eén van de conclusies in dit rapport is dat door diverse technische en marktontwikkelingen, de effectiviteit en efficiëntie van de aftapbaarheid van gegevens afneemt. Dit geldt in het bijzonder voor mobiele telefonie en internetverkeer. Het afluisteren van een verbinding wil niet zeggen dat bij al het communicatieverkeer over een lijn daadwerkelijk meegeluisterd kan worden. Veel gegevens worden versleuteld verstuurd en zijn daardoor moeilijk of niet te interpreteren. E-mail bijvoorbeeld, is goed te tappen bij een aanbieder. Maar veel internetgebruikers hebben een e-mailaccount bij webmaildiensten zoals Hotmail, Gmail of Yahoo waarvan de aanbieder een buitenlands bedrijf is. In dat geval is er een internationaal rechtshulpverzoek nodig om inzage in de communicatie te krijgen. Daarnaast wordt er veel gecommuniceerd met social mediadiensten zoals Twitter, Windows Live Messenger[5] Hyves, Facebook, Ping en Whatsapp. Dit zijn diensten waarvan de communicatie veelal via servers in het buitenland verloopt. Men kan ook communiceren via bepaalde games. Bij deze vorm van communicatie wordt er geen server als tussenstation gebruikt, maar gaat de communicatie rechtstreeks van gebruiker naar gebruiker. Ook telefonie via internet, VoIP, blijkt lastig te tappen. De inhoud van de gesprekken wordt bij deze vorm van telefonie veelal versleuteld over het internet verstuurd. Dit is bij Nederlandse aanbieders geen probleem omdat de dienst aftapbaar moet zijn zoals omschreven in hoofdstuk 13 van de Telecommunicatiewet. Maar online telecommunicatiediensten worden ook aangeboden door buitenlandse aanbieders die buiten de aftapplicht vallen. Bij een eventuele tap is dan wel zichtbaar wie met wie contact heeft, maar de inhoud van het gesprek kan niet worden achterhaald omdat de encryptie niet ontsleuteld kan worden. Daarnaast wordt het ook steeds moeilijker om een identiteit te koppelen aan een internetgebruiker. Bij het registreren voor een dienst worden opgegeven namen of pseudoniemen namelijk niet gecontroleerd. Een IP-adres kan regelmatig veranderen en e-mailadressen zijn eenvoudig te wijzigen, ook door de gebruiker zelf. Tappen van een internetlijn is dus geen heilig middel waarmee alle communicatie eenvoudig onderschept en afgeluisterd kan worden.
De onderzoekers van het Stratix rapport concluderen dat het overgrote deel van de openbare telecommunicatie vooralsnog aftapbaar lijkt te zijn (Koops et al., 2005, p. 32). Ze vermelden dat mobiele telefoniediensten en onderliggende netwerken zo goed als volledig aftapbaar

[5] Voorheen MSN geheten.

zijn. Vooral de oudere generaties mobiele telefoons zijn, behoudens bepaalde specifieke diensten en dienstvarianten goed te tappen. Ook provider- en e-maildiensten zijn volgens de auteurs goed aftapbaar. In 2009 heeft Stratix nader onderzoek verricht naar dat deel van de openbare telecommunicatie dat volgens het rapport uit 2005 moeilijk aftapbaar zou zijn (Stratix, 2009). Dat onderzoek laat zien dat het grootste deel van de telecommunicatie nog steeds goed aftapbaar is, en dat er vooral enkele operationele problemen voorkomen. In dit rapport wordt geconcludeerd dat een deel van de beperkingen waar men tegenaan loopt technisch op te lossen is, maar dat dit niet alleen technische aanpassingen vergt. In sommige gevallen zijn ook veranderingen in de wet- en regelgeving vereist. Daarnaast blijken de definities in de Telecommunicatiewet bij sommige type telecommunicatiediensten en netwerken voor grijze gebieden te zorgen. Het snel veranderende aanbod aan communicatiediensten op internet maakt het kortom noodzakelijk om de mogelijkheden voor het aftappen regelmatig opnieuw te bezien. Het moge duidelijk zijn dat de enorme toename van diensten op het internet en de opkomst van de smartphone maakt dat de kunst van het tappen aan veranderingen onderhevig is, of zou moeten zijn.

II

Het gebruik van de tap in Nederland

Inleiding

In dit deel van het rapport gaan we allereerst in op de regulering van het tappen in Nederland (hoofdstuk 3) en op de Nederlandse tapprocedures (hoofdstuk 4). In hoofdstuk 5 bieden we een overzicht van de Nederlandse tapstatistieken, waarna we ingaan op het empirische onderzoek in Nederland. Hoofdstuk 6 geeft een schets van het gebruik van de tap bij verschillende soorten misdrijven, van de doelen waarmee de tap bij dit soort zaken wordt ingezet en van de overwegingen die aan het gebruik van de tap ten grondslag liggen. Voorts geven we in dit hoofdstuk een beschrijving van de wijze waarop de telefoontap in de praktijk wordt ingezet. In hoofdstuk 7 gaan we in op de wijze waarop de internettap in de praktijk wordt gebruikt. In hoofdstuk 8 behandelen we de vraag of er alternatieven zijn voor de tap.

3 Regulering van het tappen in Nederland

De telefoon- of internettap (artikel 126m Sv) is een bijzondere opsporingsbevoegdheid en valt onder de Wet bijzondere opsporingsbevoegdheden (Wet BOB) die op 1 februari 2000 in werking is getreden. In dit hoofdstuk zal de Wet BOB nader uiteen worden gezet en zal de telefoontap gepositioneerd worden tussen de andere bijzondere opsporingsbevoegdheden. Daarom wordt in dit hoofdstuk de Wet BOB besproken en gaan we in op de ontstaansgeschiedenis, de uitgangspunten en de verschillende bijzondere opsporingsbevoegdheden die zijn opgenomen in deze wet.[6]

3.1 De Wet Bijzondere Opsporingsbevoegdheden

De ontstaansgeschiedenis van de Wet BOB is nauw verbonden met de zogenaamde *'IRT-affaire'* en de naar aanleiding daarvan ingestelde *Parlementaire Enquêtecommissie Opsporingsmethoden* (PEO), ook wel de *commissie-Van Traa* genoemd; vernoemd naar haar voorzitter (Kruisbergen & De Jong, 2010, p. 37).
De IRT-affaire speelde zich af in de jaren negentig van de vorige eeuw, met als startpunt de opheffing van het interregionaal rechercheteam Noord-Holland/Utrecht (IRT), dat was opgericht om de zware, georganiseerde criminaliteit te bestrijden. De aanleiding was onenigheid over de onconventionele opsporingsmethoden die het team toepaste. Zo maakte het IRT, om door te kunnen dringen tot de top van de criminele organisatie die werd onderzocht, gebruik van (criminele) burgerinformanten/-infiltranten. Om die burgerinfiltranten binnen de criminele organisatie 'carrière' te laten maken, en zo bewijsmateriaal tegen de top te verzamelen, kregen de infiltranten de mogelijkheid om, onder regie van de politie en het OM, grote partijen verdovende middelen het land binnen te smokkelen en die ook op de markt te brengen. Daarvoor bestond op dat moment geen wettelijke regeling. Aangezien de Amsterdamse driehoek (de burgemeester, de hoofdofficier van justitie en de korpschef) toen die in kennis werden gesteld van de gebruikte methoden, daarvoor geen verantwoordelijkheid wilden dragen werd het IRT opgeheven (Kruisbergen & De Jong, 2010; *Kamerstukken II* 1995/96, 24 072, nrs. 10-11, p. 77-79).
De IRT-affaire leidde uiteindelijk tot een parlementaire enquête. De ingestelde commissie kreeg onder andere de opdracht om onderzoek te doen naar de toepassing, rechtmatigheid, deugdelijkheid en effectiviteit van de opsporingsmethoden, naar de organisatie en het functioneren van de opsporing en naar de controle daarop. De PEO concludeerde naar aanleiding van het door haar uitgevoerde onderzoek, dat er sprake was van een drieledige crisis in de opsporing: 1) een *normeringscrisis*, er was sprake van een gebrek aan adequate normering betreffende het optreden van politie en justitie; 2) een *organisatiecrisis*, er was sprake van gebrek aan duidelijkheid binnen de organisatie van de opsporing over wie waarvoor verantwoordelijk was; 3) een *gezagscrisis*, waarbij het openbaar ministerie zijn gezag over de politie dreigde te verliezen.

De conclusies van de PEO hebben geleid tot een aantal concrete aanbevelingen (*Kamerstukken II* 1995/96, 24 072, nrs. 10-11, p.448-449), onder andere:

- opsporingsmethoden dienen een wettelijke basis te hebben;
- het gebruik van opsporingsmethoden moet expliciet worden vastgelegd, zodat controle te allen tijde mogelijk is;
- hoe groter de inbreuk op de privacy is, des te hoger dient de autoriteit te zijn die toestemming verleent voor het gebruik ervan;
- toetsing van de inzet van een opsporingsmethode dient vooraf plaats te vinden aan de hand van objectieve criteria;

[6] Voor een uitgebreide bespreking van de ontstaansgeschiedenis, uitgangspunten en de opgenomen opsporingsbevoegdheden van de Wet BOB, zie Bokhorst et al. (2002), Beijer, Bokhorst, Boone, Brants & Lindeman (2004), en Kruisbergen & De Jong (2010).

- het OM heeft het gezag over de opsporing en beslist daarmee over de inzet van opsporingsmethoden.

De aanbevelingen komen voort uit het idee dat opsporing centraal via de wet en door versterking van het hiërarchisch gezag van het openbaar ministerie dient te worden aangestuurd. Dit zou bovendien controleerbaar en dus transparant dienen te zijn (Commissie- Van Traa, 1996).
Bovenstaande aanbevelingen zijn grotendeels door de Tweede Kamer overgenomen. Het rapport *Inzake Opsporing*, dat op 1 februari 1996 verscheen, is aanleiding geweest voor nieuwe wetgeving op het gebied van opsporingsmethoden, waaronder de Wet BOB. Het wetsvoorstel werd in mei 1999 door de Eerste Kamer aanvaard en trad zeven maanden daarna in werking.

3.2 Uitgangspunten van de wet BOB

In de drie uitgangspunten die de Wet BOB kent, zijn de aanbevelingen van de PEO goed te herkennen (*Kamerstukken II* 1996/97, 25 403, nr. 3, p. 3). Het eerste uitgangspunt is *codificatie van opsporingsmethoden*. Opsporingsmethoden waaraan integriteitrisico's kleven of die een inbreuk maken op grondrechten van burgers dienen een wettelijke basis te hebben. Het maken van een inbreuk op fundamentele rechten van burgers mag slechts plaatsvinden op basis van wettelijk gegeven bevoegdheden.
Het tweede uitgangspunt dat de Wet BOB kent is dat de *OvJ* de *centrale autoriteit* is bij de opsporing. De OvJ geeft formele leiding aan de opsporing (artikel 148 Sv) en beslist over de inzet van opsporingsmethoden. Hiermee wordt de gezagspositie van de OvJ in het opsporingsonderzoek benadrukt. Voordat de politie gebruik mag maken van één van de bijzondere opsporingsbevoegdheden, dient de OvJ daartoe uitdrukkelijk en schriftelijk "bevel" te hebben gegeven, tenzij de bevoegdheid aan de opsporingsambtenaar zelf is toegekend. Voor sommige bijzondere opsporingsbevoegdheden moet de OvJ een machtiging voor de toepassing van de bevoegdheid vorderen bij de RC. En voor een aantal bevoegdheden moet de OvJ zich voor toestemming wenden tot het College van Procureurs Generaal (CvPG's) en vindt er een interne toetsing plaats (Krommendijk, Terpstra & Van Kempen, 2009, p. 15).
Het derde uitgangspunt is de *controleerbaarheid* van de opsporing. Van de inzet van opsporingsbevoegdheden dient proces-verbaal opgemaakt te worden om controle te bewerkstelligen (artikel 152 Sv). Naast verslaglegging van de inzet van bijzondere opsporingsbevoegdheden wordt controleerbaarheid van de opsporing ook bewerkstelligd door de in de Wet BOB opgenomen verplichting tot *notificatie* (artikel 126bb lid 1 Sv). Dit houdt in dat een betrokkene 'zodra het belang van het onderzoek dat toelaat' ervan op de hoogte moet worden gebracht dat er tegen hem een bijzondere opsporingsbevoegdheid is ingezet (zie paragraaf 3.6) (Bokhorst, et al., 2002: 3; Krommendijk et al., 2009: 10; Kruisbergen & De Jong, 2010: 41-42; *Kamerstukken II* 1996/97, 25 403, nr. 3).

3.3 De bijzondere opsporingsbevoegdheden

In de Wet BOB, dat wil zeggen: In titel IVA, titel V en titel VB Sv, wordt een aantal opsporingsbevoegdheden geregeld die uitsluitend door opsporingsambtenaren (na schriftelijk bevel van de OvJ) uit te oefenen zijn. Het gaat om stelselmatige observatie (artikel 126g en 126o Sv); het stelselmatig inwinnen van informatie (artikel 126j en 126qa Sv); pseudokoop/-dienstverlening (artikel 126i en 126q Sv); infiltratie (artikel 126h en 126p Sv); het betreden van besloten plaatsen om die te bekijken, een technisch middel te plaatsen of sporen op te nemen, vroeger bekend als inkijkoperatie (artikel 126k en 126r Sv); het opnemen van vertrouwelijke communicatie (OVC) (artikel 126i en 126s Sv); het opnemen

van communicatie (tappen) (artikel 126m en 126t Sv)[7] en het opvragen van gegevens over het communicatieverkeer met betrekking tot een gebruiker (opvragen verkeersgegevens) (artikel 126n en 126u Sv). Ten tweede wordt bijstand aan de opsporing door burgers wettelijk geregeld: het stelselmatig inwinnen van informatie door een burgerinformant (artikel 126v Sv); pseudokoop/-dienstverlening door burgers (artikel 126ij en 126z Sv); en burgerinfiltratie (artikel 126w en 126x Sv).
Bijzondere opsporingsbevoegdheden kunnen worden toegepast bij het bestaan van een *verdenking* dat een misdrijf is begaan (Titel IVA). Daarbij zijn voor de meeste bevoegdheden nadere eisen gesteld wat betreft de zwaarte van het misdrijf (zie paragraaf 2.3.2). Het toepassen van bijzondere opsporingsbevoegdheden op grond van een verdenking wordt ook wel 'klassieke' of 'traditionele' opsporing genoemd. Daarnaast kunnen de bijzondere opsporingsbevoegdheden worden ingezet indien uit feiten of omstandigheden een *redelijk vermoeden* voortvloeit dat misdrijven als omschreven in artikel 67 lid 1 Sv in georganiseerd verband worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren (Titel V). Met het toepassen van bijzondere opsporingsbevoegdheden op grond van een redelijk vermoeden is een ruimer criterium ontstaan voor het gebruik van bijzondere opsporingsbevoegdheden. Dit werd van belang geacht om te komen tot een effectievere bestrijding van georganiseerde criminaliteit (Krommendijk et al., 2009).
Op 1 februari 2007 is het Wetboek van Strafvordering (Sv) wederom verruimd met de inwerkingtreding van de 'Wet ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven'. In geval van (dreiging van) een terroristisch misdrijf achtte de wetgever de verdenkingseis die geldt voor klassieke opsporing te hoog en heeft hiertoe de wetgeving verruimd door een lichter criterium voor de toepassing van bijzondere opsporingsbevoegdheden te introduceren, namelijk het bestaan van *aanwijzingen* dat een terroristisch misdrijf wordt gepleegd (Titel VB). Dit stelt de politie en het OM in staat om in een zo vroeg mogelijk stadium strafvorderlijk op te treden, om zodoende terroristische aanslagen te voorkomen (De Poot, Bokhorst, Smeenk & Kouwenberg, 2008).
Uit onderzoek blijkt echter dat bijzondere opsporingsbevoegdheden op basis van Titel V en VB op beperkte schaal worden ingezet (Beijer et al., 2004; De Poot et al., 2008; Krommendijk et al., 2009; Van Gestel, De Poot, Bokhorst & Kouwenberg, 2009; Van Gestel, De Poot & Kouwenberg, 2010). In het onderhavige onderzoek beperken we ons tot de toepassing van de bijzondere opsporingsbevoegdheden (met name de tap) op basis van Titel IVA.

3.3.1 De ingrijpendheid in de persoonlijke levenssfeer

Opsporingsbevoegdheden die slechts een beperkte inbreuk maken op de persoonlijke levenssfeer, zoals niet-stelselmatige observatie, kunnen worden toegepast op grond van artikel 2 Politiewet 1993 (Pw) en artikel 141 en 142 Sv. Bevoegdheden die een grotere inbreuk op de persoonlijke levenssfeer kunnen maken, zoals stelselmatige observatie en de tap, zijn opgenomen in de Wet BOB.
Een aantal van deze zogenaamde *bijzondere* opsporingsbevoegdheden is in hun gehele toepassingsbereik geregeld (infiltratie, pseudokoop/-dienstverlening, de tap en bevoegdheden in een besloten plaats), andere bevoegdheden alleen voor zover ze stelselmatig worden toegepast (observatie en het inwinnen van informatie) (Bokhorst et al., 2002).
De opsporingsbevoegdheden die in de Wet BOB worden geregeld, worden als *bijzonder* gekarakteriseerd vanwege de inbreuk die de toepassing ervan kan maken op de persoonlijke levenssfeer en het risico voor de integriteit en de beheersbaarheid van de opsporing (Cleiren & Nijboer, 2009). Het is moeilijk om in abstracto te bepalen of deze bevoegdheden een schending inhouden van het recht op de persoonlijke levenssfeer. De memorie van toelichting van de Wet BOB stelt dat niet elke bemoeienis van de politie met de persoonlijke levenssfeer van de burger leidt tot een schending van diens privacy. Hiervan zal sprake zijn

[7] Op basis van deze wetsartikelen kan ook een internettap worden aangesloten.

vanaf een bepaald niveau van betrokkenheid, afhankelijk van de concrete omstandigheden van het geval. Wat wel vaststaat volgens vaste jurisprudentie, is dat bij het afluisteren van een telefoongesprek inbreuk wordt gemaakt op het telefoongeheim zoals is vastgelegd in artikel 13 Grondwet (Gw) (*Kamerstukken II* 1996/97, 25 403, nr. 3, p. 9-11).

Het recht op privacy wordt ook beschermd door artikel 8 EVRM. De inmenging van het openbaar gezag in het privé-, familie- en gezinsleven, de woning en correspondentie van burgers is volgens artikel 8 lid 1 EVRM niet toegestaan. Uit de (vaste) rechtspraak van het Europese Hof voor de Rechten van de Mens (EHRM) komt naar voren dat een telefoontap een inbreuk oplevert op zowel het recht op privéleven als dat van de correspondentie. Het recht op bescherming van de persoonlijke levenssfeer, zoals geformuleerd in artikel 8 EVRM, en de daarop betrekking hebbende rechtspraak van het EHRM, wordt nader uitgewerkt in de hoofdstukken in Deel III van dit onderzoeksrapport. Niettemin verdienen de volgende aspecten hier kort te worden benoemd.

Zo is in artikel 8 lid 2 EVRM een uitzondering geformuleerd op bovengenoemde regel, in de zin dat er door het openbaar gezag inbreuk mag worden gemaakt op de privacy van burgers indien aan drie voorwaarden wordt voldaan: De inbreuk van het openbaar gezag moet zijn gebaseerd op een wettelijke regeling, in het belang zijn van de nationale veiligheid, de openbare orde of het economisch welzijn van het land, wanordelijkheden en strafbare feiten voorkómen, of de gezondheid of de goede zeden de rechten en vrijheden van anderen beschermen en noodzakelijk zijn in een democratische samenleving.

Het EHRM heeft twee criteria ontwikkeld om het overheidsoptreden binnen het eigen nationaal rechtsstelsel te beoordelen. Het betreft hier de toegankelijkheid van het nationale recht (*accessability*)en de voorzienbaarheid (*foreseeability*) van het recht. Het EHRM beoordeelt de kwaliteit van het recht in het kader van de voorzienbaarheid met betrekking tot het aftappen van telefoongesprekken aan de hand van een zestal voorwaarden (vergelijk *Valenzuela Contreras tegen Spanje*, EHRM 30 juli 1998, r.o. 46):

1. A definition of the categories of people liable to have their telephones tapped by judicial order;
2. The nature of the offences which may give rise to such an order;
3. A limit on the duration of telephone tapping;
4. The procedure for drawing up the summary reports containing intercepted conversations;
5. The precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence;
6. The circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court.

Hieronder wordt ingegaan op de verschillende wettelijke aspecten van de Nederlandse regeling, waarin concrete invulling is gegeven aan de hierboven geformuleerde algemene door het EHRM geformuleerde voorwaarden.

3.3.2 Verdenkingsgraad

De inzet van een bijzondere opsporingsbevoegdheid vereist een bepaalde verdenkingsgraad. Deze is niet voor elke bijzondere opsporingsbevoegdheid gelijk. De wetgever heeft een onderscheid gemaakt in drie verdenkingsgraden waarin de bijzondere opsporingsbevoegdheden kunnen worden toegepast:

- misdrijf;
- misdrijf als bedoeld in artikel 67 lid 1 Sv;
- misdrijf als bedoeld in artikel 67 lid 1 Sv dat gezien zijn aard of de samenhang met andere

door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.

De minder ingrijpende opsporingsbevoegdheden kunnen worden toegepast bij verdenking van een misdrijf (bijvoorbeeld misdrijven als mishandeling en verduistering). De opsporingsbevoegdheden stelselmatige observatie (artikel 126g lid 1 Sv) en stelselmatig inwinnen van informatie (artikel 126j lid 1 Sv) zijn toepasbaar bij verdenking van een misdrijf.
De meer ingrijpende opsporingsbevoegdheden kunnen pas worden toegepast indien sprake is van een verdenking van een misdrijf als omschreven in artikel 67 lid 1 Sv (bijvoorbeeld diefstal en valsheid in geschrifte). Bij dit soort misdrijven kunnen de opsporingsbevoegdheden pseudokoop/-dienstverlening (artikel 126i lid 1 Sv), bevoegdheden in een besloten plaats (artikel 126k lid 1 Sv) en opvragen verkeersgegevens (artikel 126n lid 1 Sv) worden ingezet.
Voor de zeer ingrijpende opsporingsbevoegdheden is een verdenking van een misdrijf als omschreven in artikel 67 lid 1 Sv, dat gezien zijn *aard* of de *samenhang* met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert vereist (bijvoorbeeld moord en mensenhandel). Ook minder ernstige misdrijven kunnen een ernstige inbreuk maken op de rechtsorde, doordat zij in combinatie met andere misdrijven worden gepleegd, bijvoorbeeld valsheid in geschrifte in combinatie met omkoping van ambtenaren met het oog op verkrijging van vergunningen voor bedrijven. Of een misdrijf een ernstige inbreuk op de rechtsorde oplevert is dus niet slechts uit de wettelijke delictsomschrijving op te maken, maar is ook afhankelijk van de ernst van de feiten en omstandigheden waaronder het misdrijf is gepleegd of wordt beraamd. Zo zijn het gewelddadig karakter van het misdrijf of de omvang en de gevolgen voor de samenleving indicatief (*Kamerstukken II* 1996/97, 25 403, nr.3, p. 24-25; Buruma, 2001). De opsporingsbevoegdheden waaraan deze zware verdenkingsgraad is gesteld zijn stelselmatige observatie waarvoor een besloten plaats moet worden betreden, niet zijnde een woning (artikel 126g lid 2 Sv), infiltratie (artikel 126h lid 1 Sv), OVC (artikel 126l lid 1 Sv) en de tap (artikel 126m lid 1 Sv).

3.3.3 Tegen wie ingezet

De ingrijpendheid van een opsporingsbevoegdheid wordt niet alleen uitgedrukt in de vereiste verdenkingsgraad, maar kan ook tot uitdrukking komen in de persoon tegen wie de bijzondere opsporingsbevoegdheid kan worden ingezet. Hoewel het in de lijn der verwachting ligt dat de meest ingrijpende opsporingsbevoegdheden enkel tegen verdachten kunnen worden ingezet, blijkt dat inmiddels niet meer zo te zijn. Zo zijn bijvoorbeeld tappen en OVC, de meest ingrijpende bijzondere opsporingsbevoegdheden, niet beperkt tot communicatie waaraan de verdachte deelneemt. De inzet van andere bijzondere opsporingsbevoegdheden is ook niet beperkt tot een verdachte (behalve bij pseudokoop/-dienstverlening) en kunnen worden ingezet tegen een bredere kring van niet-verdachte personen. Dit zijn bijvoorbeeld personen waarvan wordt vermoed dat ze in contact staan met de verdachte.

3.3.4 Duur

De termijn waarbinnen een opsporingsbevoegdheid kan worden ingezet, kan ook iets zeggen over de gepercipieerde ingrijpendheid ervan. In een aantal gevallen wordt de termijn waarbinnen de opsporingsbevoegdheid kan worden ingezet in duur beperkt. Deze termijn kan wel telkens worden verlengd. Zo kan OVC en de tap voor de duur van maximaal vier weken worden ingezet. Na het verstrijken van die periode dient opnieuw een aanvraag tot verlenging te worden overlegd aan de RC. Stelselmatige observatie en stelselmatige informatie-inwinning kunnen voor de duur van maximaal drie maanden worden ingezet. De andere bevoegdheden (pseudokoop/-dienstverlening en bevoegdheden in een besloten plaats) zijn (door hun eenmalige karakter) niet aan een termijn gebonden.

3.3.5 Toestemmingsprocedure

Voor de toepassing van bijna alle bijzondere opsporingsbevoegdheden is een bevel van de OvJ vereist, waarbij deze zich dient te laten leiden door de wettelijke voorwaarden die aan

de bevoegdheden zijn gesteld (Buruma, 2001). Enkele zeer ingrijpende opsporingsbevoegdheden en/of bevoegdheden waaraan risico's zijn verbonden vereisen nadere toetsing door en/of toestemming van een hogere autoriteit. De toepassing van een aantal bijzondere opsporingsbevoegdheden (zoals (burger)infiltratie, burgerpseudokoop/-dienstverlening en OVC) moet vooraf worden voorgelegd aan het CvPG dat op advies van de Centrale Toetsingscommissie (CTC) beslist over de inzet ervan.
Bij de twee, naar de mening van de wetgever, meest ingrijpende bevoegdheden – de tap en OVC – is vooraf machtiging van de RC vereist. Deze dient de vordering te toetsen aan de wettelijke voorwaarden (*Kamerstukken II* 1996/97, 25 403, nr.3, p. 103; Beijer et al., 2004). Het gaat hier dan ook om opsporingsbevoegdheden die direct ingrijpen op de in artikel 13 Gw beschermde belangen (Hoge Raad, 11 oktober 2005, *LJN* AT4351; *Kamerstukken II* 1997/98, 25 403, nr. 7, p. 23-24).

3.3.6 Gronden

De gronden waarop een bijzondere opsporingsbevoegdheid mag worden toegepast variëren enigszins. Een aantal bijzondere opsporingsmiddelen mag worden ingezet 'in het belang van het onderzoek' (stelselmatige observatie, stelselmatig inwinnen van informatie, pseudokoop/-dienstverlening, bevoegdheden in een besloten plaats en aanvragen verkeersgegevens), terwijl andere bevoegdheden slechts mogen worden ingezet 'indien het onderzoek dit dringend vordert' (infiltratie, OVC, tap). In het laatste geval is de subsidiariteitstoets (zijn er geen andere, minder zware opsporingsbevoegdheden voorhanden die tot hetzelfde resultaat kunnen leiden) strenger en moet nog beter bekeken worden of met een minder ingrijpend middel niet hetzelfde resultaat kan worden behaald.
De mate van ingrijpendheid van bijzondere opsporingsbevoegdheden komt ook naar voren in jurisprudentie waarin soms, naast de geldende wettelijke voorwaarden, extra voorwaarden worden gesteld aan de toepassing van bepaalde bijzondere opsporingsbevoegdheden.[8]

3.4 Specifiek voor de tap

De wetgever bezag bij de totstandkoming van de Wet BOB de tap als één van de meest ingrijpende opsporingsbevoegdheden, daarom is de inzet ervan aan een aantal voorwaarden verbonden (*Kamerstukken II* 1996/97, 25 403, nr. 3, p. 23). Allereerst dient de inzet van de tap te voldoen aan het *proportionaliteitsbeginsel*, dat wil zeggen dat de ingrijpendheid van de opsporingsbevoegdheid in verhouding moet staan tot de ernst van het misdrijf. Dit komt onder meer tot uitdrukking in het wettelijke vereiste dat de tap enkel kan worden ingezet bij misdrijven als omschreven in artikel 67, lid 1 Sv. Daarnaast moet de aard van het misdrijf een ernstige inbreuk op de rechtsorde opleveren, dat wil zeggen dat enkel de delictsomschrijving dus niet voldoende is voor inzet van de telefoontap, maar dat tevens de ernst van het feit en omstandigheden waaronder het misdrijf is gepleegd of beraamd moeten worden meegewogen bij de beoordeling of sprake is van een ernstige inbreuk op de rechtsorde. De memorie van toelichting van de Wet BOB heeft nagelaten het begrip 'ernstige inbreuk' concreet in te vullen. Wel somt het een aantal voorbeelden op als moord, handel in drugs, mensenhandel, omvangrijke milieudelicten, wapenhandel maar ook ernstige financiële misdrijven. Het gaat om misdrijven die door hun gewelddadige karakter of door hun omvang en gevolgen voor de samenleving de rechtsorde schokken (*Kamerstukken II* 1996/97, 25 403, nr. 3, p. 24-25).

[8] In een zaak waarin een undercoveragent is ingezet om stelselmatig informatie in te winnen bij een verdachte die zich in een penitentiaire inrichting bevindt, stelt de Hoge Raad dat dit in beginsel toelaatbaar is maar dat dit het gevaar met zich brengt dat de verdachte feitelijk in een verhoorsituatie komt te verkeren zonder de waarborgen die bij een formeel verhoor gelden. Het op deze wijze inzetten van een undercoveragent kan dan ook pas plaatsvinden na een verzwaarde proportionaliteits- en subsidiariteitstoets: er moet sprake zijn van een bijzonder ernstig misdrijf en andere wijzen van opsporing mogen redelijkerwijs niet aanwezig zijn. Wanneer hieraan is voldaan moet worden bekeken of de verklaringsvrijheid niet is geschonden (Kruisbergen & De Jong, 2010; Noot Mevis bij arrest Hoge Raad, 21 november 2006, *LJN* AY9673).

Een meer concrete invulling van het begrip 'ernstige inbreuk op de rechtsorde' heeft de wetgever dus aan de rechter overgelaten. Maar ook de jurisprudentie biedt geen houvast en is hieromtrent erg casuïstisch. Zo oordeelt het Hof Amsterdam dat uitkeringsfraude de inzet van de telefoontap niet rechtvaardigt (Hof Amsterdam, 24 juni 2004, *LJN* AP9856) en de Rechtbank 's-Gravenhage dat een woninginbraak niet voldoende is voor de inzet van de telefoontap (Rechtbank 's-Gravenhage, 30 december 2003, *NJ* 2004, 276). Maar opzetheling van printercardridges ter waarde van €200.000,- was wel een feit dat naar het oordeel van de Hoge Raad kon worden aangemerkt als een ernstige inbreuk op de rechtsorde, door de financiële gevolgen ervan (Hoge Raad, 30 maart 2010, *LJN* BL2828). En hoewel de Rechtbank Amsterdam van mening was dat het kweken van hennep niet is aan te merken als een misdrijf dat door zijn aard een ernstige inbreuk op de rechtsorde vormt, is dit oordeel door het Hof Amsterdam en de Hoge Raad verworpen (Hoge Raad, 11 oktober 2005, *LJN* AT4351).
Tot slot moet het onderzoek de inzet van de telefoontap dringend vorderen. Met deze voorwaarde wordt gedoeld op het *subsidiariteitsbeginsel*. De telefoontap mag alleen worden toegepast als niet met behulp van lichtere opsporingsbevoegdheden eenzelfde resultaat kan worden bereikt. In de jurisprudentie wordt aan deze subsidiariteitstoets geen verdergaande eis gesteld dan dat redelijkerwijs, naar ervaringsregels, aangenomen mocht worden dat andere methoden, die de uitoefening van fundamentele rechten in mindere mate zouden aantasten, ontoereikend zouden zijn (Hoge Raad, 11 oktober 2005, *LJN* AT4351).

3.5 Geheimhouders

In het strafrecht is bepaald dat voor een aantal beroepsgroepen het verschoningsrecht geldt. Artikel 218 Sv zegt hierover:

> Van het geven van getuigenis of van het beantwoorden van bepaalde vragen kunnen zich ook verschoonen zij die uit hoofde van hun stand, hun beroep of hun ambt tot geheimhouding verplicht zijn, doch alleen omtrent hetgeen waarvan de wetenschap aan hen als zoodanig is toevertrouwd.

In de praktijk betekent dit dat bij gebruik van de telefoontap gesprekken met verschoningsgerechtigden, ook wel geheimhouders genoemd, niet mogen worden afgeluisterd en opgenomen. Daarnaast moeten al opgenomen gesprekken worden vernietigd. Artikel 126aa lid 2 Sv zegt hierover:

> Voor zover de processen-verbaal of andere voorwerpen mededelingen behelzen gedaan door of aan een persoon die zich op grond van artikel 218 zou kunnen verschonen indien hem als getuige naar de inhoud van die mededelingen zou worden gevraagd, worden deze processen-verbaal en andere voorwerpen vernietigd. Bij algemene maatregel van bestuur worden hieromtrent voorschriften gegeven. Voor zover de processen-verbaal of andere voorwerpen andere mededelingen dan bedoeld in de eerste volzin behelzen gedaan door of aan een in die volzin bedoelde persoon, worden zij niet bij de processtukken gevoegd dan na voorafgaande machtiging door de rechter-commissaris.

De beroepen die als geheimhouder worden aangemerkt zijn onder andere advocaat, huisarts, tandarts, medisch specialist, verpleegkundige, verloskundige, geestelijke, notaris, reclasseringsmedewerker (behalve wanneer deze als voorlichter werkt voor de rechter), juridisch medewerker van het Juridisch Loket en journalist. Afgeleide geheimhouders zijn de medewerkers van de geheimhouder, zoals de secretaresse en assistent(e) (OM, 2011). Wanneer een geheimhouder zelf (mede)verdachte is van een strafbaar feit waarvoor een tap kan worden ingezet, kan deze zich niet beroepen op zijn verschoningsrecht. Echter, wanneer deze verdachte contact heeft met een niet-verdachte geheimhouder, dan valt het gesprek onder het verschoningsrecht van de niet-verdachte geheimhouder.

In het verleden is het voorgekomen dat uitgewerkte gesprekken tussen verdachten en geheimhouders in het procesdossier terecht zijn gekomen. Een bekend voorbeeld hiervan is de strafzaak tegen leden van de Hells Angels. In deze zaak werd het OM op grond hiervan niet ontvankelijk verklaard in de strafvervolging van alle 22 verdachten (Rechtbank Amsterdam, 20 december 2007, *LJN* BC0685). Om dit in de toekomst te voorkomen zijn sindsdien maatregelen getroffen. Hieronder zullen we de achtergronden en de inhoud van de nieuwe maatregelen beschrijven. In 2003 heeft Het College Bescherming Persoonsgegevens (CBP) voor het eerst een onderzoek verricht naar de uitvoering van de vernietigingsplicht. Op grond van dit onderzoek, concludeerde het CBP dat de werkwijze met betrekking tot het opnemen en registreren van vertrouwelijke communicatie onrechtmatig was (CBP, 2003). Een eerste versie van een *Instructie voor vernietiging van geïntercepteerde gesprekken met geheimhouders* was toen wel al ingevoerd door het College van procureurs-generaal (CvPG). Op grond van de onderzoeksresultaten van het CBP werd deze instructie aangepast en trad ze in 2007 vernieuwd in werking. In deze instructie is de procedure beschreven die doorlopen moest worden wanneer een geheimhoudergesprek, in de zin van artikel 218 Sv, door een opsporingsambtenaar werd ontdekt bij het uitluisteren van de telefoontap. Het gesprek diende uitgewerkt te worden en vervolgens aan de OvJ te worden doorgegeven. Aan de hand van de uitwerking diende de OvJ te beoordelen of het daadwerkelijk een gesprek betrof dat onder het verschoningsrecht viel. Wanneer dit het geval was diende de OvJ een bevel ter vernietiging aan de teamleider van de politie te geven. Deze moest er vervolgens voor zorgen dat alle stukken vernietigd zouden worden, waarna het bevel doorgestuurd diende te worden naar de beheerder van het interceptiecentrum. Wanneer alle stukken bij de recherche en het interceptiecentrum waren vernietigd, diende de OvJ hiervan een bewijs te krijgen in de vorm van een proces-verbaal van vernietiging. In 2007 is een nieuw onderzoek uitgevoerd door het CBP, dat uitwees dat de vernietigingsplicht met betrekking tot opgenomen gesprekken met advocaten nog steeds niet voldoende werd nageleefd. Zowel de termijnen voor de vernietiging, als het daadwerkelijk vernietigen van gegevens bleek gebrekkig te worden uitgevoerd (CBP, 2007). Naar aanleiding van deze situatie heeft het CvPG ervoor gezorgd dat strafdossiers over de periode 2009-2010 zijn gecontroleerd op het voorkomen van geheimhouders. Daarnaast is in opdracht van het College een systeem van nummerherkenning ontwikkeld dat wordt ondersteund door het OM en de advocatuur. Dit systeem, dat samen met de NOvA is ontwikkeld, is op 1 september 2011 officieel in werking getreden. [9] In dit systeem staan opgegeven telefoon- en faxnummers van advocaten en daarvan afgeleide personen met het verschoningsrecht, in een filter geregistreerd bij het ULI. Wanneer een telefoonnummer wordt getapt, worden de verkeersgegevens (telefoonnummers, tijdstip, etc.) langs een filter geleid. Wordt een telefoonnummer door het systeem herkend, dan wordt de opname automatisch gestopt. Mocht er vertraging zitten in het doorkomen van de verkeersgegevens, dan wordt de reeds opgenomen communicatie vernietigd.[10] In dit nieuwe systeem, kan het opsporingsteam alleen de verkeersgegevens van de in het systeem geregistreerde geheimhoudergesprekken inzien. Deelname aan het nieuwe systeem is voor alle advocaten verplicht gesteld (zie artikel 2, Verordening op de nummerherkenning). Wanneer het systeem volledig in gebruik zal zijn genomen, zullen problemen met opgenomen gesprekken met geheimhouders opgenomen in het nummer herkenningsysteem worden ondervangen. Echter, gesprekken met andere geheimhouders zoals artsen of geestelijken worden niet automatisch gefilterd.

Op 19 augustus 2011 is de nieuwste Instructie vernietiging geïntercepteerde gesprekken met geheimhouders in werking getreden, onder andere met het oog op de ontwikkeling van het nummerherkenningsysteem. Bij het aftappen van gesprekken fungeert het systeem van nummerherkenning als een eerste filter. Gesprekken met nummers geregistreerd in dit systeem worden geblokkeerd en komen niet bij de politie terecht. Daarnaast is er een early warning tool waarmee geïmporteerde gespreksdata wordt vergeleken met een bestand van telefoonnummers van mogelijke geheimhouders. Voor de gesprekken die vervolgens terecht

[9] Het systeem werkt nog niet optimaal in de praktijk. In hoofdstuk 6.17 zal dit nader worden besproken.

[10] Zie de Algemene toelichting op de Verordening op de Nummerherkenning, 3.

komen bij de politie is het mogelijk de BVO (Basis Voorziening Opsporing) scantool te gebruiken. Deze scantool maakt het mogelijk om alle gesprekken te scannen aan de hand van een telefoonnummerbestand van mogelijke geheimhouders en een woordenlijst met woorden die kunnen wijzen op een geheimhoudersgesprek. Wanneer een geheimhoudersgesprek wordt geconstateerd moet als volgt worden gehandeld: zodra een opsporingsambtenaar, belast met het uitwerken van tapgesprekken, een geheimhouder detecteert, blokkeert hij/zij dit gesprek en meldt dit bij de tapcoördinator/teamleider. Deze controleert vervolgens of er daadwerkelijk een geheimhouder bij het gesprek betrokken is. Bij voorkeur gebeurt dit controleren niet door de tapcoördinator of teamleider zelf maar door een speciaal aangestelde medewerker geheimhouder die niet bij het opsporingsonderzoek is betrokken (in een aantal regio's is een dergelijke medewerker geheimhouder al aangesteld). Te allen tijde geldt dat als uitgangspunt moet worden genomen dat het geheimhoudersgesprek niet wordt uitgewerkt. Wanneer het gesprek inderdaad een geheimhouder betreft, meldt de teamleider dit zelf aan de OvJ. De OvJ laat zich vervolgens door de politie informeren over de aard van het gesprek waarna de OvJ binnen 3 werkdagen met een inhoudelijke beoordeling van het mogelijke geheimhoudersgesprek komt. Wanneer de OvJ over het gesprek twijfelt, kan het gesprek worden afgeluisterd door een andere (dan de zaaks-) OvJ. Bij vaststelling van een geheimhoudersgesprek door de OvJ, stuurt de teamleider ter bevestiging hiervan binnen 5 werkdagen een proces-verbaal aan de OvJ. Na ontvangst van het proces-verbaal geeft de OvJ binnen 3 werkdagen schriftelijk bevel ter vernietiging van het geheimhoudersgesprek. De teamleiding is verantwoordelijk voor de uitvoering van dit bevel bij de recherche, en stuurt het bevel naar het interceptiecentrum waar vervolgens alle geheimhouderbestanden worden vernietigd.

De Hoge Raad heeft bepaald dat wanneer geheimhoudergesprekken niet tijdig zijn vernietigd, dit niet meer kan worden hersteld en de rechtsgevolgen hiervan niet uit de wet blijken, dit een vormverzuim[11] oplevert. Volgens artikel 359a lid 1 Sv, kan de rechter in deze situatie een sanctie opleggen, waarvan die van niet-ontvankelijkheid van het OM in de strafvervolging de zwaarste is. Bij de toepassing van dit eerste lid dient de rechter volgens het tweede lid rekening te houden met het belang dat het geschonden voorschrift dient, de ernst van het verzuim en het nadeel dat daardoor wordt veroorzaakt. De heersende jurisprudentie van de Hoge Raad is dat in slechts zeer uitzonderlijke gevallen de niet-ontvankelijkverklaring van het OM in de vervolging, in aanmerking komt. [12]

3.6 Notificatie, vernietigen en gebruik voor ander doel

Omdat de bijzondere opsporingsbevoegdheden een inbreuk kunnen maken op de persoonlijke levenssfeer, heeft de wetgever het noodzakelijk gevonden om personen tegen wie een dergelijke bevoegdheid is ingezet daarover in te lichten (Koops, 2002, p. 50). Dit wordt notificeren genoemd. Artikel 126bb lid 1 Sv zegt hierover:

> De officier van justitie doet aan betrokkene schriftelijk mededeling van de uitoefening van de bevoegdheden, genoemd in de titels IVa tot en met Vc, zodra het belang van het onderzoek dat toelaat. De mededeling blijft achterwege, indien uitreiking van de mededeling redelijkerwijs niet mogelijk is.

Uit de wettekst blijkt dat enkel betrokkenen tegen wie een bijzondere opsporingsbevoegdheid is ingezet genotificeerd dienen te worden. Artikel 126bb lid 2 Sv geeft aan wie als betrokkenen gezien kunnen worden:

[11] Wanneer op grond van artikel 359a Sv sprake blijkt te zijn van vormverzuimen tijdens het voorbereidend onderzoek, deze niet meer kunnen worden hersteld en de rechtsgevolgen hiervan niet uit de wet blijken[11], moet de situatie worden beoordeeld aan de hand van de door de Hoge Raad vastgestelde regels (Hoge Raad, 30 maart 2004, *LJN* AM2533).

[12] Hoge Raad, 16 juni 2009, *LJN* BH2678; Hoge Raad, 1 februari 2005, *LJN* AP4584

a de persoon ten aanzien van wie een van de bevoegdheden van titel IVa, V, Va, Vb of Vc is uitgeoefend;
b de gebruiker van telecommunicatie of de technische hulpmiddelen waarmee de telecommunicatie plaatsvindt, bedoeld in artikel 126m, derde lid, onderdeel c, artikel 126t, derde lid, onderdeel c, en artikel 126zg, tweede lid, onderdeel a.

Verdachten hoeven niet genotificeerd te worden, als zij inzage hebben gehad in hun dossier. Lid 3 zegt daarover:

> Indien de betrokkene de verdachte is, kan mededeling achterwege blijven, indien hij op grond van artikel 126aa, eerste of vierde lid, met de bevoegdheidstoepassing op de hoogte komt.

De mededeling kan eveneens achterwege blijven indien deze redelijkerwijze niet mogelijk is, bijvoorbeeld omdat de woon- of verblijfplaats van de betrokkene niet kan worden achterhaald. Inhoudelijke redenen voor het niet mededelen kunnen alleen liggen in het criterium 'belang van het onderzoek' (Cleiren & Nijboer, 2009, p. 627). Dit belang kan zijn het veiligheidsrisico dat verbonden is met het notificeren, bijvoorbeeld veiligheid van een betrokkene (Staatscourant, 2011).
De mededeling vindt plaats zodra het belang van het onderzoek dat toelaat. Vaak is dat enige tijd nadat het onderzoek is beëindigd (een onherroepelijke einduitspraak van een rechter of een buitenvervolgingstelling). Voor uitstel van notificatie gelden bepaalde termijnen: indien er sprake is van een verdenking van een misdrijf waarop een gevangenisstraf van 8 jaar of meer staat, dan zal een termijn van 6 maanden worden vastgesteld. Indien er sprake is van een misdrijf waarop een maximale gevangenisstraf van minder dan 8 jaar staat, dan zal een termijn van 3 maanden worden vastgesteld. Nadat deze termijn is verstreken, moet opnieuw worden beoordeeld of er inmiddels genotificeerd kan worden. Indien dit niet het geval is, wordt dezelfde procedure gevolgd. Deze procedure wordt herhaald totdat daadwerkelijk kan worden genotificeerd. Echter in het geval er 5 jaar zijn verstreken na de eerste beoordeling kan de notificatie achterwege blijven indien nog steeds sprake is van onderzoeksbelang en/of veiligheidsrisico's (Staatscourant, 2011).
Het moment van notificeren bepaalt mede het moment van de vernietiging van de gegevens zoals beschreven in artikel 126cc lid 2 Sv. Twee maanden na het beëindigen van het onderzoek en dus twee maanden na notificatie van de betrokkenen, wordt door de OvJ een bevel tot vernietiging afgegeven voor de informatie verkregen met bijzondere opsporingsbevoegdheden. Een proces-verbaal van vernietiging wordt naar de OvJ toegezonden als deze handelingen zijn afgerond.
Deze periode van twee maanden lijkt te zijn bedoeld om de betrokkene de tijd te geven inzage in zijn stukken te krijgen, maar daar laat de wet een gat in de rechtsbescherming open: van het recht om inzage in stukken te krijgen is namelijk bewust afgezien (Cleiren & Nijboer, 2009, p. 628; *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 85).[13]
Soms kan vernietiging worden uitgesteld omdat de OvJ de gegevens die met behulp van onder andere de telefoontap zijn verkregen wil gebruiken in een ander onderzoek (artikel 126dd lid 1 sub a Sv) of omdat de OvJ de gegevens wil opslaan in een zogenaamd register zware criminaliteit (artikel 126dd lid 1 sub b Sv). In dat register worden gegevens opgeslagen met betrekking tot personen die betrokken zijn bij zware criminaliteit.[14] In dat geval worden de gegevens pas vernietigd wanneer de Wet Politiegegevens dat vereist.[15]

[13] De mogelijkheid inzage te krijgen in stukken is wellicht wel af te dwingen door een beroep te doen op de Wet openbaarheid van bestuur (WOB) of door een klacht in te dienen bij de Nationale Ombudsman.

[14] Onder zware criminaliteit wordt verstaan (art 10 lid 1 sub a en b Wet Politiegegevens): misdrijven als omschreven in art 67 lid 1 Sv, die in georganiseerd verband worden beraamd of gepleegd en die gezien hun aard of de samenhang met andere misdrijven die in het georganiseerde verband worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde kunnen opleveren; misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld; misdrijven als omschreven in artikel 67, eerste lid, van het Wetboek van Strafvordering, die bij algemene maatregel van bestuur zijn aangewezen en die gezien hun aard of samenhang met

3.7 Hoofdstuk 13 van de Telecommunicatiewet

Om te kunnen tappen, moet de telecommunicatie wel aftapbaar zijn. Aanbieders van openbare telecommunicatienetwerken en –diensten zijn, op grond van Hoofdstuk 13 van de Telecommunicatiewet, dan ook verplicht hun netwerken en diensten aftapbaar te maken (artikel 13.1 lid 1 Tw). Niet alleen moeten de aanbieders zorgen dat hun netwerken en diensten technisch aftapbaar zijn, ook zijn ze verplicht actief medewerking te verlenen aan een bevel tot aftappen (artikel 13.2 lid 1 Tw).
Aanbieders hebben ook een bewaarplicht van verkeersgegevens: gegevens met betrekking tot telefonie dienen 12 maanden bewaard te worden (artikel 13.2a lid 3 sub a Tw) en gegevens met betrekking tot internettoegang, e-mail en internettelefonie 6 maanden (artikel 13.2a lid 3 sub b Tw).

andere door de betrokkene begane misdrijven een ernstige inbreuk op de rechtsorde opleveren; handelingen die kunnen wijzen op het beramen of plegen van bij algemene maatregel van bestuur aan te wijzen categorieën van misdrijven die door hun omvang of ernst of hun samenhang met andere misdrijven een ernstig gevaar voor de rechtsorde opleveren

15 Art 10 lid 6 Wet Politiegegevens stelt dat de politiegegevens worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking. Daartoe worden de gegevens periodiek gecontroleerd. De gegevens worden verwijderd uiterlijk vijf jaar na de datum van de laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van de politiegegevens van betrokkene op grond van het doel als omschreven in het eerste lid van artikel 10 Wet Politiegegevens.

4 Wat is een tap en hoe komt deze tot stand?

Hoofdstuk 13 van de Telecommunicatiewet (Tw) legt aanbieders van openbare telecommunicatie de verplichting op om de aftapbaarheid van telecommunicatie te waarborgen. Aftapbaarheid duidt op de mogelijkheid om telecommunicatiegegevens te onderzoeken, dus om de communicatie af te tappen en gebruikers- en verkeersgegevens te achterhalen. De wet spreekt van 'onderzoek van communicatie', maar in de dagelijkse praktijk heeft men het over tappen. In dit hoofdstuk beschrijven we hoe een tap in de praktijk tot stand komt en welke gegevens er kunnen worden afgevangen bij een telefoon- en internettap. Het Wetboek van Strafvordering geeft de volgende beschrijving van het opnemen van communicatie (artikel 126m Sv):

> In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, aan een opsporingsambtenaar bevelen dat met een technisch hulpmiddel niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst, wordt opgenomen.

Deze wettekst geldt zowel voor het tappen van telefoonverkeer als voor het tappen van internetverkeer. Zoals in het voorgaande hoofdstuk is beschreven wordt een tap aangesloten op bevel van een OvJ, na machtiging van de RC. Hieronder wordt ingegaan op wat het aansluiten van een telefoon- en internettap praktisch inhoudt en wat (historische) verkeersgegevens zijn. Ook wordt de procedure beschreven die in Nederland wordt gevolgd om een tap aan te kunnen sluiten.

4.1 Wat is een telefoontap?

In de uitvoering houdt een telefoontap in dat de gespreksinhoud en verkeersgegevens van gesprekken en sms-berichten, gevoerd via een bepaalde telefoon[16] of met een bepaald telefoonnummer, worden doorgegeven door de aanbieder aan de Unit Landelijke Interceptie (ULI) van het Korps Landelijke Politiediensten (KLPD). Hier worden de gesprekken en gegevens in een beveiligde omgeving opgeslagen en bewaard. Om te kunnen tappen vindt gelijktijdige uitvoering van een tapbevel (artikel 126m Sv) en een bevel tot het verstrekken van toekomstige verkeersgegevens (artikel 126n lid 1 sub b Sv) plaats, aangezien de verkeersgegevens nodig zijn om objectief vast te kunnen stellen wat het tegennummer[17] is en wie daarvan de tenaamgestelde is.

4.2 Verkeersgegevens van communicatie

Naast het tappen van gespreksinhoud en verkeersgegevens, is het ook mogelijk alleen verkeersgegevens op te vragen.[18] In dat geval krijgt men enkel de nummerinformatie van beller en gebelde, de datum, het tijdstip, de lengte van het gesprek en de zendmastinformatie binnen, zonder de gespreksinhoud. Het Wetboek van Strafvordering geeft de volgende beschrijving van het opvragen van verkeersgegevens (artikel 126n Sv):

[16] Naast het aftappen van een telefoonnummer, dat verbonden is aan een SIM-kaart, kan ook een telefoon worden getapt. Een telefoon heeft een uniek nummer, het zogenaamde IMEI-nummer. Dit nummer kan worden getapt. Dit heeft als voordeel dat als een persoon van SIM-kaart wisselt, de gevoerde gesprekken op die telefoon toch kunnen worden afgeluisterd.

[17] Een tegennummer is het telefoonnummer van degene waarmee wordt gebeld door de getapte persoon.

[18] Zie voor meer informatie over verkeersgegevens: Asscher & Ekker, 2003 en Smits, 2006, p. 97-102.

> In geval van verdenking van een misdrijf als omschreven in art 67, eerste lid, kan de officier van justitie in het belang van het onderzoek een vordering doen gegevens te verstrekken over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker.

Dit kunnen zijn *historische verkeersgegevens*, gegevens over communicatiestromen die ten tijde van het doen van de vordering zijn verwerkt (artikel 126n lid 1 onder a Sv) en *toekomstige verkeersgegevens,* gegevens die betrekking hebben op communicatie die na het doen van de vordering nog niet zijn verwerkt (artikel 126n lid 1 onder b Sv).[19]
Historische verkeersgegevens kunnen voor de opsporing tot een jaar vóór de vordering beschikbaar worden gemaakt (*Kamerstukken II* 2009/10, 32 185, nr. 2, p. 1). Deze gegevens bieden inzicht in het belgedrag van de getapte persoon in de periode voorafgaand aan de vordering. Door de historische verkeersgegevens van een verdachte op te vragen, kan bijvoorbeeld worden onderzocht of deze in een bepaalde periode in contact heeft gestaan met andere verdachten of met een slachtoffer. Door historische verkeersgegevens op te vragen van een slachtoffer, kan worden achterhaald met wie het slachtoffer voor het misdrijf telefonisch in contact heeft gestaan. Historische verkeersgegevens maken het mogelijk om sociale netwerken in kaart te brengen en kunnen een rol spelen bij de overwegingen om bepaalde nummers wel of niet te gaan tappen.
Toekomstige verkeersgegevens bieden inzicht in het belgedrag van de persoon van wie deze gegevens worden opgevraagd ten tijde van het onderzoek. Een voordeel van het opvragen van toekomstige verkeersgegevens ten opzichte van het tappen van gespreksinhoud is dat men op de hoogte kan blijven van de nummers waarmee de getapte persoon contact heeft, terwijl er geen gesprekken hoeven te worden uitgeluisterd en uitgewerkt.
Het opvragen van (historische) verkeersgegevens is een lichtere bijzondere opsporingsbevoegdheid dan de telefoontap en kan door de OvJ worden gevorderd zonder machtiging van de RC. Er moet sprake zijn van een misdrijf als omschreven in artikel 67 lid 1 Sv en de opsporingshandeling moet in het belang zijn van het onderzoek. Dit zijn lichtere vereisten dan voor de inzet van de tap. Later in dit rapport (in paragraaf 6.8) wordt uitgebreider stilgestaan bij de rol van (historische) verkeersgegevens bij de overwegingen om te gaan tappen.

4.3 Historische verkeersgegevens van e-mail- en internetverkeer

Ook van internetverkeer kunnen verkeersgegevens worden opgevraagd. De Telecommunicatiewet schrijft voor dat ook gegevens over internetgebruik bewaard moeten blijven (artikel 13.2a, lid 3, sub b Tw). Vanaf 16 juli 2011 is de bewaartermijn van deze gegevens gesteld op 6 maanden (*Kamerstukken II* 2009/10, 32 185, nr. 2, p. 1). Het opvragen van verkeersgegevens aangaande internetcommunicatie levert onder ander inzicht op in: tijdstip van aanmelden, IP-adres, informatie over e-mailcontacten van zender en ontvanger, het gebruikte protocol en IP-adressen van de opgevraagde internetpagina's. Zoektermen ingetypt in een zoekmachine en de inhoud van communicatie over het internet worden niet bij de verkeersgegevens geleverd.

4.4 Wat is een internettap?

In de opsporing is het sinds een aantal jaar mogelijk om een internettap in te zetten als opsporingsmiddel. Een internettap houdt in dat al het internetverkeer of, indien er enkel een

[19] Opsporingsambtenaren spreken in het geval van toekomstige verkeersgegevens over de printertap. De benaming printertap is gebaseerd op de vroegere situatie waarbij toekomstige verkeersgegevens alleen te verkrijgen waren via een technische functionaliteit van een tap, maar nu kan dat gewoon op grond van een vordering 126n lid 1 sub a Sv.

e-mailtap wordt geplaatst, alleen het e-mailverkeer over een bepaalde internetlijn door de aanbieder wordt doorgegeven aan de ULI waar de gegevens worden bewaard en opgeslagen in een beveiligde omgeving. Een internettap wordt geplaatst op een IP (Internet Protocol)-adres, wat het identificatienummer van een computer op internet is. Deze hoeft echter niet altijd hetzelfde te zijn en kan per internetbezoek wisselen, de zogenaamd dynamische IP-adressen. De aanbieder van de internetdiensten weet wie de gebruiker achter een dynamisch IP-adres is. Sommige aanbieders kunnen een internettap aansluiten op basis van de zogenaamde NAW-gegevens (Naam, Adres en Woonplaats). Bij een internettap wordt het dataverkeer afgetapt dat van en naar een huisadres of IP-adres gaat, dus ook het dataverkeer van huisgenoten of anderen die de betreffende aansluiting gebruiken. Tenzij gekozen is voor het tappen van alleen e-mailverkeer, wordt alles wat over de lijn komt bij het ULI binnengehaald en opgeslagen (dus ook de films en muziek die gedownload worden en de bezoekjes aan een online warenhuis). Hierdoor kan de hoeveelheid data die met een internettap wordt onderschept enorm zijn.

4.5 De procedurele weg van een tap

Wanneer de OvJ, in samenspraak met een opsporingsteam, besluit tot de inzet van een tap, wordt een tapaanvraag opgemaakt waarin de redenen en doelstellingen staan om te willen tappen. De OvJ controleert of hierbij is voldaan aan de wettelijke vereisten zoals; is er een verdenking, is er sprake van een ernstige inbreuk op de rechtsorde en in hoeverre vordert het onderzoek de inzet van de tap dringend? Hierbij dient de OvJ rekening te houden met de eisen van proportionaliteit en subsidiariteit. Om een tap te kunnen inzetten, heeft de OvJ een machtiging van de RC nodig. De RC toetst of de OvJ in redelijkheid had kunnen komen tot een vordering machtiging tap en toetst of uiteindelijk is voldaan aan de gestelde eisen.[20] Wanneer de RC positief beslist geeft deze een tapmachtiging af. Bij een negatief oordeel houdt het hierbij op. Een tapmachtiging wordt voor maximaal vier weken afgegeven, maar de RC kan ook besluiten de tap voor een kortere periode toe te staan.
Als het oordeel van de RC positief is, wordt het tapbevel met originele handtekening van de OvJ opgemaakt.[21] Naast het tapbevel wordt een uittreksel (zonder naam van de getapte persoon en de verdenking) van het bevel gemaakt. Dit wordt naar de ULI gestuurd. De ULI maakt aan de hand van het uittreksel een werkformulier op, dat wordt gefaxt naar de aanbieder. De aanbieder zorgt ervoor dat de gesprekken of het dataverkeer worden afgeleverd in het systeem van de ULI. Deze procedure hoeft niet veel langer dan een dag in beslag te nemen. Als de uiteindelijke tapvordering voor 14.00 uur bij de ULI binnen is, kan deze nog dezelfde dag worden verwerkt en 'lopen'. De aanbieders garanderen namelijk dat elke tap die voor 15.00 uur bij een aanbieder binnen is, nog dezelfde dag wordt aangesloten. Dit is vastgelegd in een *service level agreement*.

4.5.1 Spoedtap

In urgente situaties is het mogelijk een zogenaamde 'spoedtap' aan te vragen. In dat geval vindt er telefonisch overleg plaats tussen de OvJ en RC. De OvJ motiveert de tapaanvraag mondeling en de RC geeft op dat moment wel of geen machtiging voor het plaatsen van de spoedtap. Wanneer de RC akkoord gaat, wordt er een tapbevel naar de ULI gefaxt en kan een tap in zeer korte tijd worden aangesloten. De mondelinge tapaanvraag dient schriftelijk bevestigd te worden. Het mondelinge bevel van de OvJ moet binnen drie dagen op schrift worden gesteld en worden verstrekt aan de aanbieder. Als de bevestiging niet tijdig door de aanbieder is ontvangen, wordt de tap afgesloten.

[20] Zie Hoge Raad, 11 oktober 2005, *LJN* AT4351 voor meer informatie over het beoordelingskader bij de toetsing van tapmachtigingen van de RC en tapbevelen van de OvJ.

[21] Sinds januari 2011 (Staatsblad, 2011, nr. 1533) kan een tapmachtiging met een elektronische handtekening worden ondertekend. Ten tijde van de interviews was dit nog niet operationeel, vandaar dat we de ervaringen met het gebruik van de elektronische handtekening niet hebben kunnen optekenen in dit rapport.

Indien het opsporingsteam in overleg met de OvJ een tap voortijdig wil afsluiten kan dat altijd, maar in het geval men het noodzakelijk vindt de tap voort te zetten dient de OvJ een aanvraag voor verlenging aan de RC voor te leggen. Opnieuw dient de inzet van de tap gemotiveerd te worden. De RC zal vervolgens oordelen of de noodzaak van de tap nog aanwezig is en of de subsidiariteits- en proportionaliteitseis bij verlenging niet in het geding zijn. Indien het besluit voor verlenging door de RC negatief wordt beoordeeld, wordt de tap afgesloten. Bij een positief besluit blijft de tap aangesloten.

4.5.2 Het uitwerken van tapgesprekken

Wanneer een telefoontap is aangesloten heeft de politie de wettelijke verplichting om de gesprekken uit te luisteren en uit te werken (artikel 152 Sv). De opgenomen gesprekken kunnen door geautoriseerde personen op locatie worden uitgeluisterd om uitgewerkt te worden. De onderzochte regio's hebben hiervoor afsluitbare ruimtes ingericht, de zogenaamde tapkamers. Indien nodig is het ook mogelijk om gesprekken live uit te luisteren. Om te kunnen inloggen op het systeem van de ULI dient iemand geautoriseerd te zijn.
De verwerking van de internettap verschilt van die van de telefoontap in die zin dat gegevens die over het internet komen vaak bekeken moeten worden in plaats van beluisterd. De programmatuur voor uitluisteren van een telefoontap is ook anders dan die van de internettap. Ook verschilt de verwerking van de informatie in een proces-verbaal. Hierop komen we later in het rapport terug (paragraaf 7.2).
Ter zake doende telefoongesprekken dienen letterlijk te worden uitgewerkt om vervolgens in het proces verbaal te worden opgenomen. Gesprekken die niet relevant zijn dienen zodanig kort samengevat te worden dat duidelijk wordt dat het gevoerde gesprek niet van belang is voor de zaak. Indien er een andere taal wordt gesproken dan het Nederlands worden er beëdigde tolken ingeschakeld voor het uitwerken van de gesprekken. Deze speciaal opgeleide tolken gaan op eenzelfde manier te werk als de politiemedewerkers en zorgen ervoor dat belangrijke gesprekken, uitgewerkt in een proces-verbaal, kunnen worden opgenomen. Op de rol van tolken wordt in paragraaf 6.10 verder ingegaan.

4.5.3 Notificeren en vernietigen

Nadat een zaak onder de rechter is geweest en is beëindigd, of wanneer een zaak wordt geseponeerd of wordt stopgezet en 'het belang van het onderzoek' het toestaat, moet er volgens artikel 126bb Sv door de OvJ worden genotificeerd. In de praktijk is het 'de BOB-kamer' (personen bij het OM die zorgen voor die administratieve afhandeling van de aanvragen en verlengingen van bijzondere opsporingsbevoegdheden, voor notificatie en voor vernietiging van gegevens) die hiervoor zorg draagt. Zij administreren de namen en adressen, verzamelen de handtekeningen bij de OvJ en versturen uiteindelijk de notificatiebrieven.
Processen-verbaal dienen twee maanden na notificatie te worden vernietigd. Dat wil in het geval van de tap zeggen dat uitgewerkte gesprekken, verkeersgegevens en alle informatie die verkregen is met behulp van een tap dienen te worden vernietigd. Ook de bestanden bij de ULI worden op bevel van de OvJ vernietigd.

4.6 Het CIOT

Bij het opstellen van een tapaanvraag wordt een digitaal formulier met vereiste informatie ingevuld. Eén van de vereisten is dat wordt nagegaan of het betreffende telefoonnummer of IP-adres nog steeds in gebruik is. Dit kan worden achterhaald door middel van een bevraging van het CIOT-systeem (Staatscourant, 2011). Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is de schakel tussen opsporingsdiensten en telecombedrijven. Dagelijks stellen de telecom- en internetbedrijven een kopie van hun klantenbestand met de wettelijk vastgelegde identificerende gegevens ter beschikking aan het CIOT in een beveiligde omgeving. Identificerende gegevens zijn naam, adresgegevens en woonplaats behorende bij telefoonnummers, e-mailadressen en IP-adressen. Deze kopie van

het klantenbestand wordt 24 uur bewaard door de telecom- en internetbedrijven in de beveiligde omgeving en wordt automatisch ingelezen in de blackbox-omgeving van het CIOT-informatiesysteem. Het opvragen van de identificeerbare gegevens via het CIOT-informatiesysteem door opsporingsdiensten vindt plaatst in een specifieke beveiligde locatie van de desbetreffende dienst. De vragen worden vervolgens automatisch verwerkt via de centrale omgeving van het CIOT-informatiesysteem. Na verwerking worden de vragen gesteld aan het bestand met de aanbiedergegevens in de blackbox-omgeving en de antwoorden zichtbaar in het CIOT-informatiesysteem.
In de regeling *Besluit verstrekking gegevens telecommunicatie* is omschreven welke gegevens vastgelegd moeten worden (artikel 4 lid 1 en 2). Aanbieders van telefonie- en internetdiensten dienen dagelijks de volgende gegevens van hun gebruikers aan te leveren bij het CIOT:

Aanbieders van telefoniediensten:
1 naam, adres, postcode en woonplaats
2 afgenomen telecommunicatiedienst (vast, prepaid, mobiel etc.)
3 toegewezen telefoonnummer
4 naam aanbieder van de dienst

Internetaanbieders:
1 naam, adres, postcode en woonplaats;
2 afgenomen telecommunicatiedienst (soort verbinding)
3 toegewezen gebruikersnaam en/of inlognaam
4 toegewezen e-mailadressen
5 toegewezen identificatienummers van randapparaten (MAC adres etc.)
6 toegewezen IPv4 en/of IPv6 adressen
7 naam aanbieder van de dienst

De (bijzondere) opsporings- en inlichtingendiensten kunnen twee soorten bevragingen doen via het CIOT. Ten eerste een vraag om identificerende gegevens behorende bij een bepaald telefoonnummer of IP-adres met als mogelijke antwoord een naam, adres, woonplaats en netwerk- en dienstaanbieder. Ten tweede kan bevraagd worden met een postcode en huisnummer waarop in het systeem gezocht wordt naar een bijbehorende naam, adres, woonplaats en netwerk- en dienstaanbieder.
Identificerende gegevens van vaste klanten van aanbieders van telefonie- en internetdiensten zijn bekend omdat deze personen zich bij het afsluiten van het abonnement hebben moeten legitimeren. Echter, bij prepaid telefoonnummers is dat anders. De telefoonnummers staan in de database van het CIOT omdat de nummers zijn uitgegeven door de aanbieder. Maar omdat men zich bij het aanschaffen van een prepaid toestel of telefoonkaart niet hoeft te registreren zijn er doorgaans geen identificerende gegevens van de gebruiker bekend.
Bevragingen bij het CIOT mogen enkel plaatsvinden op grond van artikel 126n, 126na, 126u, 126ua, 126zh, 126zi, 126ii Sv, artikel 29 Wiv (Wet op de inlichtingen- en veiligheidsdiensten 2002) en artikel 10.10 TW in het kader van een concreet opsporingsonderzoek. Dus wanneer men een tap wil aanvragen of verkeersgegevens wil opvragen, wordt er vaak eerst een CIOT-bevraging gedaan. Hiermee kunnen de opsporingsdiensten niet alleen identificerende gegevens van personen ophalen, maar daarmee kunnen ze ook voorkomen dat een verkeerde persoon wordt getapt of dat er een tap wordt aangesloten op een nummer dat niet meer in gebruik is. Een bij een tapaanvraag gevoegde CIOT-uitdraai mag dan ook niet ouder zijn dan 48 uur.
Meer dan 35 (bijzondere) opsporings- en inlichtingendiensten mogen telecommunicatiegegevens opvragen bij het CIOT, dit zijn o.a. de 25 politieregio's, het Korps Landelijke Politiediensten (KLPD), Landelijk Parket (LP), Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Militaire Inlichtingen- en Veiligheidsdienst (MIVD), de 4 bijzondere opsporingsdiensten (Fiscale Inlichtingen- en Opsporingsdienst (FIOD), Sociale Inlichtingen- en Opsporingsdienst (SIOD), Algemene Inspectiedienst (AID), Inlichtingen- Opsporingsdienst (IOD)), Inspectie voor de Gezondheidszorg (IGZ), Rijksrecherche en 112. Een CIOT-

bevraging mag alleen gedaan worden door geautoriseerde opsporingsambtenaren (artikel 5 lid 1 Besluit verstrekking gegevens telecommunicatie). Inlogcertificaten die hiervoor nodig zijn worden enkel uitgegeven aan door de opsporings- en inlichtingendiensten aangewezen personen.

4.6.1 Hoe verloopt een aanvraag?

Als een geautoriseerde opsporingsambtenaar een CIOT-bevraging wil doen, moet worden ingelogd op de webserver van het CIOT. Dan opent er een sessie waarin verzoekgegevens kunnen worden ingevuld: de identificerende gegevens, het kenmerk van het onderzoek waarvoor de ambtenaar deze gegevens wil opvragen, de rechtsgrond en de bevoegde autoriteit die heeft gevorderd. In een sessie kunnen één of meer vragen worden gesteld. Zoals hierboven beschreven kunnen dat telefoonnummers zijn, IP-adressen en NAW-gegevens van een persoon. Naast de bevraging van gegevens van individuele personen, kunnen ook bijvoorbeeld telefoonnummers die door middel van mastgegevens zijn binnengehaald in het systeem worden bevraagd.

5 De tapstatistieken in Nederland

Op verzoek van de Tweede Kamer heeft de minister van Veiligheid en Justitie de afgelopen jaren herhaaldelijk inzicht gegeven in het aantal ingezette telefoontaps door de Nederlandse opsporingsdiensten. Het aantal telefoontaps wordt geregistreerd bij de ULI van de Dienst Specialistische Recherche Toepassingen (DSRT) van het KLPD. De statistieken komen tot stand door het aantal tapbevelen te tellen. Op een tapbevel wordt de aanvraag voor de tap op één telefoonnummer of IMEI-nummer geregeld. De tapbevelen worden, na goedkeuring door de RC, met handtekening van de OvJ naar de ULI gefaxt. Hierna wordt door de ULI de telefoontap aangesloten. Als een telefoontap, na het verstrijken van de door de RC afgegeven eerste periode wordt verlengd, dan wordt deze niet nog eens meegeteld in de tapstatistieken. Wel kan het zijn dat eenzelfde telefoonnummer meerdere malen wordt getapt. Deze losse op zichzelf staande tapaanvragen op hetzelfde nummer worden in dat geval wel meerdere keren in de tapstatistieken meegeteld. Wanneer iemand zijn telefoon of telefoonnummer wijzigt, dient de OvJ een nieuw tapbevel af te geven. Dit nieuwe tapbevel telt vervolgens weer mee in de tapstatistieken. Wanneer iemand meerdere telefoons gebruikt, is het mogelijk meerdere taps aan te vragen op één verdachte. In dat geval moet voor elk van de nummers een nieuw tapbevel worden afgegeven, en wordt elk tapbevel meegeteld in de tapstatistieken.

5.1 Telefoontaps

De gepubliceerde tapstatistieken tot en met 2009 zijn in tabel 1 weergegeven, samen met het aantal vaste en mobiele telefoonaansluitingen in Nederland. Het percentage getapte vaste en mobiele nummers van de totale aantallen is berekend en weergegeven in de laatste twee kolommen. De percentages laten zien dat het aantal taps slechts een klein percentage betreft van het totaal aantal telefoonaansluitingen in Nederland. De toename van het aantal telefoontaps vanaf 1998, is toe te schrijven aan de opkomst van de mobiele telefonie. Het aantal taps op vaste lijnen is ongeveer gelijk gebleven. Hieruit kan worden opgemaakt dat het aantal telefoontaps het stijgende aantal mobiele telefoons op de voet is gevolgd.

Tabel 1 Tapstatistieken ten opzichte van het aantal mobiele en vaste telefoonaansluitingen in Nederland

	Aantal telefoon aansluitingen		Aantal telefoontaps		Percentage getapte telefoons	
	Vast	Mobiel	Vast	Mobiel	Vast	Mobiel
1993	7.634.000	216.000	3.610	0	0,05%	0%
1994	7.859.000	321.000	3.284	0	0,04%	0%
1998	9.337.000	3.351.000	3.000	7000	0,03%	0,21%
2007	7.404.300	19.285.000	3.997*	20.985*	0,05%	0,11%
2008	7.317.200	20.627.000	2.642	23.783	0,04%	0,12%
2009	7.320.000	21.182.000	3.461	21.263	0,05%	0,10%

* Geschatte cijfers, gebaseerd op twee maal de gepubliceerde halfjaarcijfers van 2007.

Bron: telecomgegevens aansluitingen: ITU, World Telecommunication/ ICT indicators database, 15Th edition 2011

De tapstatistieken voor het jaar 2010 zijn bewust buiten tabel 1 gelaten. Dit omdat het onderscheid tussen vaste telefoonaansluitingen en mobiele telefonie bij de tellingen van de ULI in 2010 is komen te vervallen. Door ontwikkelingen in de markt waardoor vaste

aansluitingen steeds vaker gekoppeld zijn aan mobiele nummers, is dat onderscheid onbetrouwbaar geworden.
Het aantal telefoontaps is in 2010 uitgekomen op 22.006. Ten opzichte van 2009, toen het totaal uitkwam op 24.724, is het absolute aantal telefoontaps met bijna 11 procent gedaald. Om de procentuele verschillen tussen de jaren te kunnen bekijken zijn vanaf het jaar 2007 de vaste en mobiele aansluitingen en taps bij elkaar opgeteld. De totalen en procenten worden gepresenteerd in tabel 2. Uit de tabel blijkt dat niet alleen het aantal telefoontaps in absolute zin afneemt, bijna 17% in 2010 ten opzichte van 2008, maar ook het aantal telefoontaps ten opzichte van het totaal aantal telefoonaansluitingen neemt af.

Tabel 2 Tapstatistieken ten opzicht van het totaal aantal telefoonsluitingen in Nederland

	Aantal telefoon aansluitingen	Aantal telefoontaps	Percentage getapte telefoons
2007	26.689.300	24.982*	0,09%
2008	27.944.200	26.425	0,10%
2009	28.502.000	24.724	0,09%
2010	26.479.000	22.006	0,08%

* Geschatte cijfers, gebaseerd op tweemaal de gepubliceerde halfjaarcijfers van 2007.

Bron: telecom gegevens aansluitingen: ITU, World Telecommunication/ ICT indicators database, 15Th edition 2011

5.2 Historische verkeersgegevens

Sinds de tweede helft van 2010 is het aanvragen van historische (verkeers)gegevens centraal geregeld via het ULI. Hiervoor was dit niet het geval waardoor er niet eerder cijfers zijn gepubliceerd over het aantal aanvragen van historische (verkeers)gegevens. In de tweede helft van 2010 zijn 24.012 aanvragen gedaan van historische gegevens, die zowel betrekking hadden op verkeersgegevens als op identificerende gegevens.

5.3 Statistieken internettap

Over het jaar 2010 zijn door de minister voor het eerst het aantal IP-taps openbaar gemaakt. Totaal heeft het ULI in 2010 1.704 maal een bevel ontvangen voor het plaatsen van een IP-tap. Dit aantal betreft zowel internettaps als e-mailtaps. In de voorgaande jaren zijn niet eerder officiële cijfers door het ministerie van Veiligheid en Justitie bekend gemaakt.

5.4 Voorbeeld casus

Het overzicht van het aantal telefoontaps dat de minister jaarlijks publiceert biedt slechts kale cijfers die zonder context moeilijk te interpreteren zijn. Hierboven zijn deze jaarlijkse cijfers naast het totale aantal telefoons geplaatst en is uitgelegd hoe de tapstatistieken tot stand komen. Om de cijfers nog meer kleur te geven hebben we één zaak uitgebreid bestudeerd. Dit is geen 'typische of doorsnee' casus en de zaak is niet representatief voor opsporing van vergelijkbare misdaden. De zaak wordt hier beschreven omdat het een illustratie biedt van de wijze waarop de telefoontap bij een moordzaak voor heel veel verschillende doelen kan worden ingezet. De zaak biedt tevens inzicht in het feit dat het aantal telefoontaps soms flink kan oplopen als het gaat om een ernstige zaak waarbij het opsporingsteam probeert zoveel mogelijk kansen en mogelijkheden te benutten om tot een oplossing te kunnen komen.

Begin 2009 vindt de politie een dode man in een woning. Er is op de plaats delict vrijwel geen forensisch bewijs voorhanden en er zijn geen getuigen die iets van het misdrijf hebben gezien. Om toch enige informatie te kunnen krijgen over de leefwereld van het slachtoffer en over mogelijke onderzoeksrichtingen is de politie niet alleen veel mensen gaan horen in de sociale kring van het slachtoffer, maar is ze in deze kring ook vrij breed gaan tappen. Zo zijn er (soms voor een korte periode) familieleden en goede bekenden van het slachtoffer getapt om erachter te komen of iemand meer informatie heeft over het misdrijf. Omdat het team meerdere scenario's open hield over wat er gebeurd zou kunnen zijn (ligt het in de relationele sfeer? Heeft het met drugs te maken?), bleef het onderzoek in het begin vrij breed en leidde informatie die via de telefoontap of via getuigenverklaringen binnenkwam ook weer tot het plaatsen van nieuwe telefoontaps bij personen die bij een bepaald verdachten-scenario zouden kunnen passen. Herhaaldelijk heeft de zaak vastgezeten, maar door toevalligheden en doordat het team tactisch 'ruis op de lijnen' veroorzaakte[22], worden er met name door de afgeluisterde gesprekken toch steeds nieuwe aanknopingspunten gevonden waarop verder kan worden gerechercheerd. Uiteindelijk leidt een tip, die overigens niet wordt verkregen via de telefoontap, ertoe dat duidelijk wordt welke personen het slachtoffer als laatste hebben gezien. Deze personen worden ook getapt en de informatie die uit de telefoontaps op deze personen en op enkele andere personen die al eerder werden getapt naar voren komt, leidt uiteindelijk tot de hoofdverdachten.
De opsporingsinspanningen van de politie hebben uiteindelijk na 2 jaar geleid tot de aanhouding van 6 verdachten. In deze zaak is de telefoontap het belangrijkste opsporingsmiddel geweest omdat elk ander bewijs ontbrak en er ook verder door getuigen weinig tactische informatie over de zaak werd verschaft. In totaal zijn er in deze zaak 205 telefoontaps aangesloten. Van dit aantal is de helft, 104 taps, aangesloten geweest op 9 personen die in beginsel als verdachten zijn aangemerkt. Dit grote aantal taps op deze 9 verdachten is ontstaan doordat deze verdachten regelmatig van telefoon en/of telefoonnummer wisselde en doordat de taps niet doorlopend aangesloten zijn geweest. Daarnaast zijn er 27 telefoontaps geplaatst op 8 familieleden en/of de partners van de verdachten; 39 taps op andere betrokkenen, 9 taps op NN (onbekende) personen. Er werden in deze zaak 3 keer verkeersgegevens opgevraagd en 1 keer werd een IP-tap geplaatst. Bij 2 taps bleek het getapte nummer niet in gebruik te zijn door de persoon die men had willen tappen.

In deze casus werd de telefoontap in eerste instantie ingezet om te onderzoeken in welke richting de oplossing van de zaak moest worden gezocht. De taps werden dus ingezet om de beschikbare informatie tactisch te kunnen duiden, en richting te kunnen geven aan het onderzoek. In deze zaak heeft de telefoontap hiervoor bruikbare informatie opgeleverd. In de tweede fase van het onderzoek – toen er mogelijke verdachten in beeld kwamen – dienden de taps vooral om bewijs over de zaak te vergaren. Hiertoe werden niet alleen de verdachten zelf, maar ook enkele van hun familieleden getapt. Dit gebeurt vaak omdat opsporingsteams verwachten dat familieleden loslippiger zullen zijn via de telefoon dan de verdachten zelf. De ervaring leert dat deze veronderstelling vaak ook wel klopt (zie hierover Bokhorst, Van der Steeg & De Poot, 2011, Bokhorst, 2004 en De Poot et al., 2004). Overigens is er in de bewijsfase van het opsporingsproces altijd sprake van de inzet van verschillende opsporingsmethoden die elkaar aanvullen (bijvoorbeeld tappen naast observatie en verhoor). In de laatste fase van het onderzoek, toen men wilde overgaan tot de aanhouding van verdachten, werden de taps ingezet om te bepalen waar de verdachten zich bevonden. In de aanhoudingsfase van een onderzoek wordt de telefoontap doorgaans gebruikt om de gangen van de verdachten na te gaan en om het observatieteam en het arrestatieteam te kunnen begeleiden of te kunnen sturen.

[22] Dit is jargon voor tactische handelingen van de politie die ervoor zorgen dat mensen loslippig kunnen worden over de telefoon. Dit gebeurt bijvoorbeeld door media-aandacht te schenken aan de zaak (in de vorm van opsporingsberichtgeving). Zie hierover ook paragraaf 6.14.

6 De telefoontap in de praktijk

Dit uitgebreide hoofdstuk handelt over de wijze waarop de telefoontap in de praktijk wordt ingezet. De informatie die in dit hoofdstuk wordt weergegeven is afkomstig van de sleutelpersonen (zie paragraaf 1.2.4) die over het gebruik van de tap in de praktijk zijn bevraagd. In dit hoofdstuk geven we allereerst een beeld van de wijze waarop de tap wordt ingezet bij verschillende soorten misdrijven (6.1) en van de doelen waarmee dit opsporingsinstrument wordt ingezet (6.2). Voorts gaan we in op de overwegingen die een rol spelen bij de inzet van de tap (6.3) de personen die aan dit opsporingsinstrument kunnen worden onderworpen (6.4), het aantal taps dat per opsporingsonderzoek kan lopen (6.5) en de wijze waarop de spoedtap wordt ingezet (6.6). Voorts beschrijven we de wijze waarop identificerende gegevens kunnen worden opgevraagd van telefoonnummers die tijdens een opsporingsonderzoek in beeld komen (6.7). Ook gaan we in op de mogelijkheden om in de opsporing – zonder daarbij gebruik te maken van de tap – informatie op te vragen over belcontacten van verdachten, slachtoffers en betrokkenen (6.8). Voorts beschrijven we de wijze waarop telefoontaps worden uitgewerkt en uitgeluisterd (6.9), de manier waarop hierbij tolken worden ingezet (6.10), en de overwegingen die spelen bij vragen rond het verlengen of afsluiten van een lopende tap (6.11). Vervolgens wordt ingegaan op de opbrengsten van de tap (6.12), op de wijze waarop opsporingsteams tegen de tap aankijken (6.13) en op factoren die de opbrengsten kunnen beïnvloeden (6.14). In de daarop volgende paragrafen gaan we kort in op het gebruik van de stealth-sms, die tijdens het tappen kan worden ingezet om de locatie van een telefoon die onder de tap staat te bepalen (6.15) op de IMSI-catcher die kan worden ingezet om in gebruik zijnde onbekende telefoonnummers te achterhalen (6.16) op de wijze waarop in de praktijk wordt omgegaan met geheimhoudersgesprekken (6.17) en op enkele andere privacy-kwesties (6.18). In dit verband staan we uitgebreider stil bij het notificeren van personen wier privacy is geschonden omdat hun telecommunicatie is afgetapt en op de wijze waarop deze privacy-gevoelige opsporingsinformatie weer wordt vernietigd (6.19) Tot slot van dit hoofdstuk staan we stil bij de administratieve lasten (6.20) en bij enkele andere knelpunten van de tap (6.21).

6.1 Schets van de inzet bij verschillende misdrijven

In deze paragraaf beschrijven we de inzet en het gebruik van de telefoontap bij verschillende soorten misdrijven. Wat we hierover optekenen is gebaseerd op de ideeën van de geïnterviewden hierover. Het is niet de bedoeling om hier uitputtend te beschrijven op welke verschillende wijzen de tap in de opsporing kan worden ingezet. Ongetwijfeld zijn er meer toepassingen te verzinnen dan we hier beschrijven. Het doel van deze paragraaf is vooral de verscheidenheid van situaties te illustreren waarmee de telefoontap als opsporingsmiddel kan worden ingezet.

Soorten misdrijven en gebruik van de telefoontap

Bij calamiteiten, zoals een gijzeling, ontvoering of een moord, moet er snel worden gehandeld, terwijl er bij de start van het onderzoek vaak weinig informatie voorhanden is over de gebeurtenis die moet worden onderzocht. Bij deze zaken speelt tijdsdruk – zeker bij aanvang van het onderzoek – altijd een grote rol. Er moet in deze zaken snel worden gehandeld, enerzijds om nog dreigend gevaar af te kunnen wenden wanneer er bijvoorbeeld nog levende slachtoffers zijn (zoals bij een gijzeling of ontvoering), anderzijds om sneller en beter tot een oplossing van de zaak te kunnen komen. Hoe sneller er informatie over de gebeurtenis kan worden vergaard, hoe groter de kans dat de zaak kan worden opgelost, zo blijkt uit diverse onderzoeken (De Poot et al., 2004; Baardewijk, Van den Brink & Van Os, 2007; Kruyer, 2010).

De keuze om bij een dergelijk onderzoek wel of niet te gaan tappen is vooral sterk afhankelijk van de sporen en aanwijzingen die bij aanvang van de zaak voorhanden zijn. Als er direct voldoende forensische sporen en getuigen zijn, of als de verdachte direct in de

omgeving van de plaats delict kan worden aangehouden, biedt een telefoontap geen of weinig meerwaarde (Bokhorst, 2004). Maar als er slechts weinig informatie voorhanden is, kan een telefoontap een onmisbaar opsporingsmiddel zijn, zeker bij aanvang van het onderzoek. Daarom worden er bij TGO's[23] relatief veel spoedtaps aangevraagd die vaak binnen een paar uur 'lopen'.

> "Een TGO gaat vaak om leven of dood. Dan lopen er vaak gelijk een stuk of 20 lijnen en de officier zit dan naast je in de beginfase, de hectische fase. Dan wordt er gelijk besproken, tap wel of niet doen. Zo gaat het dan, want er is snelheid geboden". - politie

> "Op zich heb ik er in de wat zwaardere onderzoeken nul komma nul moeite mee dat er veel taps ingezet worden. (..) Als er iemand dood is of gegijzeld wordt, dan mag je vol gas proberen alles in te zetten wat je ongeveer hebt." – OvJ

Respondenten geven aan dat ze de tap bij urgente zaken het liefst breed inzetten in de beginfase van het onderzoek en dat ze later, als er meer duidelijk is over de richting waarin naar informatie moet worden gezocht het aantal taps weer terugschroeven. Wanneer een TGO wordt samengesteld gaat het altijd om een ernstig misdrijf. De proportionaliteitseis is dan geen discussiepunt omdat het overduidelijk is dat de zaak ernstig genoeg is om de tap in te kunnen zetten. In zo'n situatie wil het opsporingsteam zo snel mogelijk beginnen met het verzamelen van informatie om gericht te kunnen handelen.

> "…vergeet ook niet dat je op uitslagen van forensisch onderzoek een tijd moet wachten. Zeker in het begin van een TGO zijn dat dingen die je eigenlijk liever niet hebt, want je wilt zo snel mogelijk je onderzoeksrichting gaan bepalen. Als je daarop moet wachten wat ga je dan in de tussentijd doen? Getuigen horen en taps aansluiten." - politie

Door opsporingsteams, ook bij TGO's, worden bij aanvang van een onderzoek scenario's opgesteld over de werkwijze (modus operandi) en de motieven van de dader, en over mogelijke verdachten. Vooral wanneer het team eigenlijk niet goed weet waar ze moet beginnen, bieden deze scenario's inzicht in de mogelijke onderzoeksrichtingen. Deze scenario's geven houvast en vormen een leidraad voor het onderzoek. Met de inzet van een of meerdere telefoontaps kan het opsporingsteam mogelijke scenario's gaan 'toetsen' en informatie verzamelen waaruit afgeleid kan worden of ze in de goede richting naar informatie zoeken.
Door de tap zo breed in te zetten, krijgt het team meer inzicht in de leefwereld van het slachtoffer, hetgeen kan leiden tot nieuwe mogelijkheden voor het verdere opsporingsonderzoek.
Later, als er duidelijker voor een bepaalde richting gekozen wordt in het onderzoek en er verdachten in beeld komen, blijft de tap in deze zaken een belangrijk opsporingsmiddel. Maar als het gaat om bijvoorbeeld een moordzaak of een grote overval, is het de kunst om verdachten hierover te laten spreken. Anders dan bij georganiseerde misdaad, waarbij verdachten met elkaar communiceren om lopende zaken te regelen met betrekking tot de illegale handel waarbij ze betrokken zijn, is er bij misdrijven die in het verleden plaatsvonden veel minder reden om over deze zaken te praten via de telefoon. Rechercheteams proberen daarom soms te bevorderen dat men loslippig wordt. Zo wacht de politie bijvoorbeeld met het horen van een verdachte of getuige totdat ze deze persoon 'onder de knop' of 'onder controle' heeft, zoals dat wordt genoemd. Ze hopen dat de verdachte of getuige, na het contact met de politie, hier met anderen over zal praten. Ook maken opsporingsteams soms

[23] Een TGO is een groot ad-hoc onderzoek waarvoor een Team Grootschalig Onderzoek wordt samengesteld. In een TGO wordt volgens een vaste structuur gewerkt om in een korte tijd veel informatie te kunnen vergaren over een ernstige gebeurtenis.

gebruik van de media om 'ruis op de lijnen' te veroorzaken. Hier komen we nog op terug in paragraaf 6.14.

Een heel andere wijze waarop de telefoontap kan worden ingezet is bij minder ernstige misdrijven zoals een gewelddadige straatroof. Wanneer bij een gewelddadige straatroof een mobiele telefoon is buitgemaakt, kan het team in samenspraak met de OvJ besluiten een tap aan te sluiten op de gestolen mobiele telefoon. Snel handelen is ook dan een vereiste, omdat een telefoon doorgaans snel weer is doorverkocht. Het betreft dan ook vaak een spoedtap, aangesloten op het identificatienummer, de IMEI code, van de telefoon. De kans dat een dader het toestel toch even gebruikt blijkt heel reëel te zijn.

> "Op grond van ervaring doen we op dat moment altijd standaard een spoedtap. Weliswaar maar voor een of twee dagen maar we doen het wel." – politie, straatroofteam

Wanneer de telefoon wordt gebruikt, is uit de aangesloten tap bekend met welk ander toestel contact is geweest. Met deze informatie kan men, indien de beller onbekend is of indien men een groep van daders in beeld wil krijgen, verder rechercheren en bijvoorbeeld besluiten een tap aan te sluiten op het tegennummer. Door middel van de informatie uit de tap kan er tevens een inschatting worden gemaakt van de locatie van waaruit met de gestolen telefoon is gebeld. Ook deze informatie kan mogelijk bijdragen aan het vinden van de verdachte. In dit soort zaken wordt de tap slechts kort – meestal niet langer dan een week - ingezet.

Bij onderzoek naar zware criminaliteit (zwacri) wordt er daarentegen volgens de respondenten langdurig en veelvuldig gebruik gemaakt van de telefoontap (zie hierover ook Bokhorst et al., 2011; Van de Bunt & Kleemans, 2007; Bokhorst, 2004; De Poot et al., 2004). In dit soort zaken gaat het vaak om voortdurende criminaliteit, zoals drugshandel of mensenhandel, waarover verdachten met elkaar moeten communiceren. Er moeten afspraken gemaakt worden over allerlei logistieke zaken, en de kans dat daarbij af en toe gebruik wordt gemaakt van de telefoon is vrij groot (Bokhorst, 2004; De Poot et al., 2004; Van de Bunt & Kleemans, 2007; Kleemans, et al., 2002).
Het gaat in deze gevallen om projectmatige onderzoeken die zorgvuldig worden voorbereid. Bij de start van het onderzoek ligt er al een plan van aanpak klaar en zijn er al verdachten in beeld waarop men zich in het onderzoek zal gaan richten.
In de voorbereidingsfase van het onderzoek wordt de doelstelling van het opsporingsonderzoek geformuleerd, en wordt gekeken welke opsporingsmiddelen er kunnen worden ingezet om deze doelen te bereiken (zie hierover ook Bokhorst et al., 2011). De tap wordt daarbij, naast eventuele andere middelen, gezien als een zeer belangrijk opsporingsmiddel.

> "Ik denk dat in zwacri onderzoeken standaard getapt wordt. Ik kan er geen bedenken waarin we niet hebben getapt." - OvJ

De geïnterviewden geven aan dat ze de telefoontap bijvoorbeeld gebruiken om informatie van de Criminele Inlichtingen Eenheid (CIE) te controleren op geldigheid. Maar de belangrijkste motivatie voor de inzet van de telefoontap bij zwacri-zaken is het feit dat de onderlinge communicatie tussen verdachten kan worden gemonitord om zodoende de handel en wandel van een organisatie in kaart te kunnen brengen. Bij projectmatige opsporing wordt het moment waarop wordt getapt vaak zorgvuldig bepaald.
Daarbij blijken vooral ook de locatiegegevens interessante informatie op te leveren. Vanaf welke geografische locatie wordt er met wie contact gelegd en waar bevindt deze tweede persoon zich? Locatiebepaling is mogelijk doordat in de verkeersgegevens die bij de tap worden meegeleverd staat aangegeven welke zendmast bij het contact is gebruikt. En hoewel dit een grove indicatie is van de locatie, levert het vaak bruikbare informatie op. Echter, verkeersgegevens worden alleen verkregen wanneer er met een telefoon wordt gebeld of wanneer deze gebeld wordt. Soms is het nodig om de locatie van een persoon te

achterhalen wanneer er geen communicatie plaatsvindt. In dat geval wordt gebruik gemaakt van een stealth-sms. Daarop komen we in paragraaf 6.15 nog terug.
De inhoudelijke opbrengst van de afgetapte gesprekken is in dit soort onderzoeken vooral ondersteunend. Zelden wordt er in dit soort zaken direct bewijs vergaard door middel van de tap. De meeste criminelen die zich met zware criminaliteit bezighouden zijn zich goed bewust van het feit dat ze worden getapt en hebben de wijze waarop ze via de telefoon communiceren daarop aangepast. Een kwaliteit die door opsporingsteams wordt aangeduid als 'communicatiediscipline' of 'telefoondiscipline'.

> "Die gasten doen bijna niets meer over de telefoon." - politie

Hoewel er in georganiseerde misdaadzaken dus zelden direct bewijs wordt verkregen door middel van een telefoontap, levert de tap wel vaak 'sturingsinformatie' op. Door middel van de informatie die via de tap wordt vergaard kan het opsporingsteam worden aangestuurd en kan met behulp van andere opsporingsmiddelen naar nieuwe informatie worden gezocht (zie hierover ook De Poot et al., 2004, p. 161-182; Bokhorst, 2004).

Of het nou gaat om georganiseerde misdaadzaken, of om een moordzaak, een algemene constatering is dat aan het tappen veel opsporingscapaciteit wordt gespendeerd. Het kost veel tijd om alle opgenomen telefoongesprekken uit te luisteren en te verwerken. Bovendien is het uitluisteren van telefoongesprekken vaak intensief, omdat de aandacht niet moet verslappen. Respondenten geven aan tijdens het uitluisteren van gesprekken te hopen en te wachten op net die ene kleine aanwijzing of verspreking. In de meeste onderzoeken zijn daar wel voorbeelden van te geven. Ondanks de soms zware lasten die de inzet van de tap meebrengt voor het opsporingsteam, geven de respondenten aan veel waarde te hechten aan de inzet van dit opsporingsmiddel. Respondenten vinden dat de opbrengst van de tap nog altijd opweegt tegen de kosten die ermee gemoeid zijn en de lasten die het met zich meebrengt voor het opsporingsteam.

> "Er zitten zoveel nevenvangsten op een tap, denk aan plaatsbepaling, denk aan al zijn nietszeggende contacten, maar misschien zegt het heel veel over het milieu waarin iemand iets zegt. Het is altijd wel heel prettig als je een tap hebt." – politie

Ook op wijkteamniveau wordt gebruik gemaakt van de tap. In sommige regio's wordt het lichtere recherchewerk op wijkteamniveau aangepakt door de wijkrecherche. In dat geval worden straatroven waarbij mobiele telefoons worden gestolen door wijkteams onderzocht. In het algemeen geldt dat wijkteams belast zijn met het opsporen van criminaliteit in de wijk. Het gaat dan vaak om het leefbaar houden van een wijk door bijvoorbeeld drugspanden te ontruimen of drugoverlast door dealers en gebruikers te beperken. De telefoontap was lang voorbehouden aan de gespecialiseerde rechercheteams, maar door enerzijds het toenemende aantal ernstige delicten dat in de wijken wordt gepleegd, en anderzijds overbelasting van de rechercheafdelingen, wordt de tap tegenwoordig ook ingezet door 'blauwe' wijkteams. Dit zijn teams die niet specifiek met recherchetaken zijn belast, maar de basis politiezorg uitvoeren. In regio A wordt het recherchewerk op wijkteamniveau uitgevoerd door de wijkrecherche, die door de aard van hun taken altijd al gebruik maakten van de tap. In Regio B is het een recente ontwikkeling dat een blauw wijkteam de telefoontap inzet bij haar activiteiten. Door het blauwe wijkteam wordt heel nauw samengewerkt met een rechercheclusterdat zich sterker op de drugshandel richt, terwijl het wijkteam vooral in de wijk opereert. Als het gaat om het tegengaan van overlast door bijvoorbeeld drugspanden, kan dat strafrechtelijk of bestuurlijk worden aangepakt. Vaak is van tevoren niet helemaal duidelijk of een onderzoek zal uitmonden in een strafrechtelijk onderzoek. In regio B werkt het wijkteam bij dit soort activiteiten daarom nauw en gericht samen met de gemeente en de belastingdienst om panden te kunnen sluiten en mensen financieel af te kunnen romen. Het blauwe wijkteam had op het moment dat dit onderzoek plaatsvond inmiddels twee zaken waarbij de tap was ingezet, met succes afgerond. Bij de

wijkteams komt in het algemeen een breed scala aan misdrijven binnen. Uiteraard wordt de tap alleen ingezet bij onderzoek naar ernstigere misdrijven en bij geplande acties.

> "Gemiddeld wordt er één tap per zaak aangesloten. Soms is het wel eens zo dat het nummer verandert. Wat we vooral niet willen op ons niveau is dat wij langdurig lijnen hebben en ook veel lijnen hebben. (…) We vragen de tap ook maar voor twee weken aan. Als we nu een tap aanvragen staat er al een actiedag gepland." - politie, wijkteam

Bovenstaande illustraties laten zien dat de telefoontap een opsporingsmiddel is dat door verschillende teams op verschillende wijzen wordt gebruikt en ingezet. Later in dit rapport zullen we meer voorbeelden laten zien van de wijze waarop de tap gericht of als aanvulling wordt ingezet bij acties zoals ontruimingen of aanhoudingen, bij het opsporen van verdachten en bij het vergaren van bewijs. Uit de gesprekken met respondenten is een aantal factoren te identificeren die een rol spelen bij de overwegingen om al of niet te gaan tappen en bij overwegingen over de wijze waarop en de mate waarin de tap wordt ingezet. Hierop gaan we in de volgende paragraaf nader in.

6.2 Doelen

Wanneer een opsporingsteam een tap wil plaatsen, dient dit gemotiveerd te worden in het aanvraagproces-verbaal. In die motivatie dient te worden beschreven wat de doelstelling(gen) van de inzet van de telefoontap zijn. Uit de gesprekken met respondenten komt naar voren dat de doelstelling om te gaan tappen drieledig is, namelijk *traceren van verdachten of gezochte personen, sturing* en *bewijs* of een combinatie van deze drie.

6.2.1 Traceren

Informatie verkregen met een telefoontap kan inzichtelijk maken waar een verdachte zich ongeveer bevindt. Dit kan inhoudelijk uit de gesprekken worden gehaald, maar ook door zendmastgegevens te bekijken. De locatie van een verdachte, is in het bijzonder van belang op de dag van aanhouding en doorzoeking. Een respondent zegt hierover:

> "Op de dag van aanhouding wil je dolgraag dat iedereen onder de tap ligt, want stel je voor dat je er eentje mist of [iemand] vlucht." - RC

In het geval van een calamiteit, zoals een ontvoering, kan het voorkomen dat een opsporingsteam wil weten waar een bepaalde persoon of een slachtoffer zich bevindt. Als er niet wordt gecommuniceerd met de telefoon die getapt wordt, kan men een *stealth-sms* naar die desbetreffende telefoon sturen. Dit 'stille' sms-bericht zorgt ervoor dat de telefoon, zonder dat dit zichtbaar is, bij ontvangst van het bericht contact maakt met het netwerk. De gebruikte zendmast kan dan als indicatie dienen voor een grove locatiebepaling. Voordat een aanhouding gaat plaatsvinden, wordt ook regelmatig gebruik gemaakt van stealth-sms. Hierdoor wordt van tevoren nog enige zekerheid verkregen over de locatie van een persoon (zie over de stealth-sms verder paragraaf 6.15).
Naast het opsporen van personen bij calamiteiten, noemt een respondent ook het onder controle houden van slachtoffers. Een respondent noemt het voorbeeld van mensenhandelonderzoek waarbij men via de telefoontap in de gaten kan houden of het doorlaatverbod met betrekking tot slachtoffers niet wordt overtreden.[24]
Uit de gesprekken komt naar voren dat er door straatroofteams regelmatig taps worden aangesloten op gestolen mobiele telefoons. Zo kan een team de informatie die de tap

[24] Zie voor meer over de rol van de tap in mensenhandelonderzoeken: Verhoeven, Van Gestel & De Jong, 2011.

mogelijk oplevert over het gebruik en de locatie van de mobiele telefoon gebruiken om de telefoon en degene die de telefoon in bezit heeft te traceren.
De respondent van de FIOD geeft aan de telefoontap bijvoorbeeld in te zetten om de locatie van een boekhouding van een verdacht bedrijf of van een verdachte persoon te achterhalen. Een respondent van een wijkteam in regio A, geeft aan dat het team gebruik maakt van zogenaamde gecontroleerde afleveringen. Hierbij heeft het team een pakketje met een duistere inhoud onderschept, doorgaans drugs afkomstig vanuit het buitenland. Verkleed als postbezorger levert een politiefunctionaris het pakje af bij de geadresseerde, om deze vervolgens aan te kunnen houden. Tijdens een dergelijke actie staan de geadresseerde en mogelijk andere betrokkenen onder de tap met als doel controle te houden over het pakketje en het netwerk van personen, zodat snel tot inbeslagname en aanhoudingen kan worden overgegaan.

6.2.2 Sturing

Een telefoontap kan veel informatie opleveren over iemands leefwijze; bijvoorbeeld wie hij is, wat hij doet, met welke mensen hij relaties onderhoudt en wat de aard is van die relaties, waar hij zich bevindt, zijn dagindeling, zijn dagbesteding, etc. (zie ook Bloem & Aarts, 2000, p. 132).
Zoals gezegd (zie paragraaf 6.1) kan deze informatie worden gebruikt om richting te geven aan een onderzoek. Bij aanvang van een opsporingsonderzoek naar een ernstig misdrijf, zoals een moord, worden er zoals gezegd scenario's opgesteld over wat er mogelijk gebeurd kan zijn. Bij het maken van keuzen over de richting van het onderzoek is de informatie uit de tap volgens respondenten een belangrijk sturingsmiddel.

> "Dan heb je zo'n man daar liggen en denk je wie is dat, wat is zijn wereldje (…)? Kan het een vergelding zijn? Je moet rekening houden met verschillende scenario's. Is het een liefdesprobleem, ging hij vreemd, verzin het maar. Dus we zijn de familie rondom gaan tappen. Zijn vrouw, schoonzussen, aangetrouwde neefjes, aangetrouwde nichtjes, noem maar op. Dat hebben we langdurig gedaan. Dan krijg je een behoorlijk idee van hem."- politie

Daarnaast kan informatie uit de telefoontap sturing geven aan de inzet van andere opsporingsmiddelen. Zo kan, indien uit de tap blijkt dat verdachten X en Y op een bepaald adres afspreken om 15 uur, het observatieteam worden aangestuurd om op dat tijdstip op die locatie te zijn en daar vast te leggen dat die afspraak heeft plaatsgevonden. Ook bij het plaatsen van apparatuur voor het opnemen van vertrouwelijke communicatie is het noodzakelijk inzicht te hebben in iemands leven om tijdstip en locatie voor plaatsing te kunnen bepalen. De tap dient dan om de veiligheid van degene die de apparatuur plaatst te waarborgen en om te zorgen dat deze heimelijke apparatuur – zonder gevaar voor voortijdige ontdekking – kan worden geplaatst Overigens vraagt één van de respondenten zich af of de veiligheid van degene die de apparatuur moet plaatsen valt onder het opsporingsbelang dat de wetgever voor ogen had. In ieder geval is het duidelijk dat als deze politiefunctionaris gevaar loopt, het opsporingsonderzoek ook gevaar loopt, omdat er dan een grote kans is dat het onderzoek 'stuk gaat'. In de praktijk zijn deze doelen – het belang van de opsporing en de veiligheid van de opsporingsambtenaar – niet van elkaar te scheiden.
De tap wordt ook ingezet met als doel contacten en netwerken in kaart te brengen. Soms kan met een aantal taps een heel netwerk in kaart worden gebracht, waarna het opsporingsteam kan besluiten wie de kopstukken zijn en wie niet, en op welke personen en activiteiten het opsporingsteam zich in het verdere onderzoek het beste kan concentreren.

6.2.3 Bewijs

Kleemans et al. (2002, p. 88) constateren in hun onderzoek naar georganiseerde criminaliteit in Nederland dat de telefoontap, vaak ook in combinatie met andere methoden,

een belangrijke bijdrage levert aan de bewijsvoering van de door hen geanalyseerde opsporingsonderzoeken. Het beeld dat de tap een belangrijke bijdrage kan leveren aan het bewijs wordt in ons onderzoek bevestigd. Veelal gaat het daarbij om aanvullend en indirect bewijs. Veel respondenten geven aan dat direct bewijs, een bekentenis als 'ik heb die overval gepleegd', niet meer uit een tap wordt verkregen. Een respondent zegt hierover dat tappen om bewijs een kwestie is van 'naar adem happen', niets hebben maar hopen dat er iets over de tap wordt gezegd. Toch wordt de telefoontap regelmatig ingezet met als doel bewijs te vergaren. Veel respondenten geven aan dat ze veel indirect en aanvullend bewijs krijgen door het tappen van telefoongesprekken. Respondenten geven aan dat ze bij onderzoeken naar georganiseerde criminaliteit regelmatig gebruik maken van de tap om informatie te kunnen achterhalen over de verhoudingen tussen de verschillende verdachten die in het onderzoek in beeld zijn gekomen: wie heeft de touwtjes in handen, wie is de geldschieter en wie voert er slechts uit? Ook de motieven voor een misdaad worden regelmatig duidelijk tijdens het tappen.
Een mooi voorbeeld van de wijze waarop de tap aanvullend bewijs kan opleveren, gaf een respondent van een wijkteam uit regio A. Dit wijkteam houdt zich voornamelijk bezig met drugsoverlast en gebruikt de tap om dealers onder controle te krijgen. In dit soort zaken biedt de tap volgens hem regelmatig zicht op de plekken waar afspraken tussen dealers en kopers plaatsvinden. Als men dergelijke plekken in beeld heeft, worden deze met behulp van het observatieteam geobserveerd, en kunnen de deals worden vastgelegd en de kopers worden aangehouden. Waar drugshandel in het verleden op de hoek van de straat plaatsvond, wordt tegenwoordig gebruik gemaakt van panden omdat de openbare ruimte steeds beter in de gaten wordt gehouden met camerasystemen. Met behulp van de tap kan men nu toch zicht krijgen op transacties waar het opsporingsteam zonder de tap niet meer bij kan komen. Door met behulp van de tap meerdere transacties in beeld te krijgen en te registreren en vervolgens de kopers met het observatieteam te volgen en na de koop aan het houden, kan de dealer voor handel worden opgepakt in plaats van enkel voor het bezit van drugs.

6.3 Overwegingen om te tappen

Het besluit om te gaan tappen komt tot stand in overleg tussen de teamleider en de OvJ. Bij deze besluitvorming speelt een aantal factoren een rol die bepalen of er een tap kan worden ingezet en zo ja, om hoeveel taps het zal gaan en welke personen of nummers er getapt zullen gaan worden. In de vorige paragraaf is beschreven dat de wijze waarop de tap wordt ingezet sterk afhankelijk is van de aard van het misdrijf. Dit is niet alleen het geval omdat de tap bij verschillende soorten misdrijven verschillende doelen kan dienen, maar ook omdat voldaan moet worden aan de eisen van proportionaliteit en subsidiariteit die bij wet aan het gebruik van de tap zijn gesteld. Zo moet het onderzoek de inzet van de tap dringend vorderen. Dat houdt in dat geen ander, lichter opsporingsmiddel voorhanden moet zijn. Daarnaast speelt de capaciteit van het team een grote rol bij de besluitvorming hieromtrent. Het opsporingsteam moet na het verkrijgen van toestemming om te gaan tappen mankracht beschikbaar hebben om de gesprekken uit te kunnen werken, wat niet ten koste mag gaan van het andere recherchewerk dat in die zaak of in andere zaken moet worden verricht. Verder spelen de persoonlijke smaak van de teamleider en het gemak waarmee een tap kan worden gerealiseerd een rol in de besluitvorming over de inzet van de tap. Hoewel het gemak waarmee een tap kan worden gerealiseerd wel een rol speelt bij de overwegingen om te gaan tappen, is het niet zo dat alles wat kan ook daadwerkelijk gebeurt. Van een eventuele tapcultuur - waarbij standaard gebruik zou worden gemaakt van de tap als de aard van de zaak dat toelaat - is volgens de respondenten allerminst sprake. Er wordt altijd bewust nagedacht over de meerwaarde die een tap kan opleveren (ofwel over de mate waarin het onderzoek dit dringend vordert), vooral ook omdat er veel politiecapaciteit is gemoeid met het uitluisteren en uitwerken ervan.

> "Het is zeker niet zo dat we als een jekko die stekkers erin rossen aan het begin van het onderzoek. Daar wordt echt wel over nagedacht." – OvJ

6.3.1 Proportionaliteit en subsidiariteit

Bij de overwegingen om een tap in te zetten moet rekening worden gehouden met de eisen van proportionaliteit en subsidiariteit. Het *proportionaliteitsbeginsel* schrijft voor dat er een zekere evenredigheid moet zijn tussen de ingrijpendheid van een opsporingsmiddel enerzijds en de ernst van het op te lossen misdrijf anderzijds. Het proportionaliteitsbeginsel zie je onder andere terug in de wettelijke eisen omtrent de zwaarte van het misdrijf. Zo kan een tap volgens de wet alleen worden ingezet als het een misdrijf betreft als omschreven in artikel 67 lid 1 Sv (een misdrijf waarop minstens 4 jaar gevangenisstraf staat), dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert (artikel 126m Sv).
Of de inzet van een opsporingsmiddel, in dit geval de tap, proportioneel is, wordt twee keer beoordeeld. In eerste instantie komt het opsporingsteam in samenspraak met de OvJ tot het besluit om te gaan tappen. Het is de OvJ die in deze fase beoordeelt of de inzet van een tap proportioneel is. Vervolgens is het de RC die een machtiging moet afgeven aan de OvJ om te kunnen tappen. De RC beoordeelt of de OvJ in alle redelijkheid tot een tapaanvraag had kunnen komen en bekijkt daarbij ook of is voldaan aan het proportionaliteitsbeginsel.
Alle RC's die we in het kader van dit onderzoek spraken, zeggen een tapaanvraag zonder enige twijfel af te wijzen wanneer zij vinden dat de verdenking niet zwaar genoeg is. Tegelijkertijd geven ze aan dat deze grenzen moeilijker te trekken zijn als het gaat om de vraag of de ernst van het misdrijf de inzet van dit middel rechtvaardigt. De vraag of het middel al of niet proportioneel is, is bij minder ernstige delicten een terugkerend punt van discussie.

> "Voor wat betreft de ernst van het misdrijf, daar wordt verschillend over gedacht door verschillende RC's en daar hebben we het ook vaak over. Bijvoorbeeld een beroving waarbij een mes of pistool wordt gebruikt op straat wel, maar een diefstal van je handtas in een café niet. Stapje verder is een woninginbraak. Wordt de rechtsorde daardoor ernstig geschokt? In het algemeen zeg ik nee, dat is ontzettend vervelend maar niet iets waar mensen (in het algemeen) van wakker liggen. Maar wat nou als de bewoners thuis zijn op dat moment? Wat als de dief wordt overlopen door een bewoner en er wordt geweld gebruikt? Het is dus de hele tijd een glijdende schaal waar je op zit." – RC

Vanuit het Kabinet RC worden beleidslijnen opgesteld en probeert men op een lijn te komen om te voorkomen dat OvJ's gaan 'shoppen' en een RC zoeken waarbij ze "het meeste voor elkaar krijgen". Er zijn hierover ook afspraken gemaakt tussen de politie en het OM:

> "In overleg met het OM is een aantal criteria (mes/ vuurwapen; seriematig; excessief geweld) opgesteld op basis waarvan het (straatroof)team zonder meer een tap mag aansluiten. Dus dan is het alleen een kwestie van de OvJ bellen en vertellen dat je zaak aan de criteria voldoet en dan mag er getapt worden. Meestal gaat het dan om spoedtaps." – politie

Toch is er binnen deze beleidslijnen ruimte voor persoonlijke overwegingen. Een aantal RC's geeft aan dat er zich onder de RC's 'rekkelijken en preciezen' bevinden. De rekkelijke RC zoekt de grenzen op van wat is toegestaan en de precieze RC gaat uit van de letter van de wet. Eén van de respondenten zegt hierover:

> "Het wel of niet machtigen tot het geven van een bevel voor een telefoontap is een persoonlijke overweging, waarbij het grensgebied altijd wordt opgezocht. Bij sommige zaken staat het vast, bestaat geen twijfel, en teken je er bijna blind voor. Maar de grens wordt wel steeds verder opgerekt. De politie wil het liefst elke telefoon aftappen. De OvJ misschien ook wel, maar als RC moet je op een gegeven moment wel een grens stellen." – RC

Zo wordt door meerdere respondenten de discussie aangehaald betreffende de mate van geweld waarmee diefstal van een mobiele telefoon gepaard moet gaan voordat er in de opsporing een tap kan worden ingezet. Een mobiele telefoon die uit een tas wordt gestolen is voor geen van de respondenten, zowel RC als OvJ, voldoende. Diefstal van een mobiele telefoon waarbij een duw wordt uitgedeeld, wordt wel gezien als een vorm van geweld, hoewel dit als veel minder ernstig wordt beoordeeld dan wanneer er een wapen wordt gebruikt.
Een RC die zichzelf als rekkelijk beschouwt, geeft aan dat de opsporing in zo'n geval zo snel mogelijk moet worden gestart. Als iemand op straat van zijn telefoon wordt beroofd, moet je er heel snel bij zijn. Een ander voorbeeld dat in dit verband wordt genoemd is de woninginbraak. De RC geeft aan dit persoonlijk heftig te vinden. Hij heeft veel met slachtoffers van woninginbraak te maken gehad in zijn vorige baan als OvJ. Hij stelt dat het in sommige gevallen zinnig kan zijn om bij woninginbraak een tap aan te sluiten (wanneer bij de inbraak een telefoon is gestolen), omdat inbraken zowel vrij ernstig zijn als moeilijk oplosbaar.

> "En als je op een makkelijke manier toch de daders kunt achterhalen doe ik niet moeilijk over het aansluiten van een tap." - RC

Bovenstaande redenering laat zien dat de vraag of een opsporingsmiddel al of niet kan worden ingezet in een specifieke situatie niet alleen afhangt van de aard van het misdrijf en dus van de proportionaliteit. Ook de vraag of er in het specifieke geval een ander minder ingrijpend opsporingsmiddel kan worden ingezet waarmee hetzelfde resultaat kan worden bereikt speelt daarbij een rol. Dit is het *subsidiariteitsbeginsel.* De woninginbraak uit het bovengenoemde voorbeeld bevindt zich, gezien de zwaarte van de zaak, op de grens als het gaat om de mate waarin het middel proportioneel is. In het geval een telefoon is weggenomen bij een woninginbraak is de tap een voor de hand liggend opsporingsmiddel. Het doel van de inzet is in dat geval het vinden van aanknopingspunten over de richting waarin naar een verdachte kan worden gezocht. Het gaat daarom in het genoemde voorbeeld om een tap die slechts zeer kort, hoogstens enkele dagen, zal lopen. Ook wat betreft de mate waarin de tap inbreuk maakt op de privacy van specifieke personen kan dus worden gesteld dat de ene tap de andere niet is. In overwegingen omtrent de vraag of het middel in een bepaalde situatie al of niet moet worden ingezet en voldoet aan de subsidiariteitseisen, worden al deze factoren meegewogen.

In eerste instantie is het aan de OvJ om te beoordelen in hoeverre het subsidiair is om de tap in te zetten. Voorts is de RC die ook toetst of voldaan is aan de eisen van het subsidiariteitsbeginsel en daarmee beoordeelt of de gestelde doelen niet met andere opsporingsmiddelen – die minder inbreuk zouden maken op de privacy - zouden kunnen worden bereikt. Eén van de RC's geeft aan altijd actief in het dossier op zoek te gaan naar informatie die aanknopingspunten biedt voor de opsporing, om deze vraag te kunnen beantwoorden. Meerdere RC's geven aan wel eens contact met de OvJ op te nemen met de vraag of er wel getapt moet worden en of er niet eerst op een andere manier informatie kan worden vergaard. Ook geven RC's aan behoefte te hebben aan meer informatie in de tapaanvraag over de mogelijke zoekwegen die nog bewandeld kunnen worden. Volgens de respondenten worden er in deze nota's vaak standaardformuleringen gebruikt en mist men een beschrijving van de zoekwegen en activiteiten die reeds zijn uitgevoerd door de politie. Op deze manier is het vormen van een mening over de subsidiariteit lang niet altijd mogelijk. Meerdere RC's geven aan contact te zoeken met de OvJ wanneer er onduidelijkheden of vragen zijn over de aanvraag. Een OvJ omschrijft de subsidiariteitseis als juridisch krom:

> "De tap wordt gezien als een privacy inbreukmakend middel maar minder inbreukmakende middelen, zoals het stelselmatig inwinnen van informatie, kosten meer tijd en capaciteit om resultaat mee te behalen." – OvJ

De capaciteitsafweging (efficiëntie in de opsporing) wordt vaak genoemd als een belangrijk punt:

> "Ga je vier man wekenlang zetten op stelselmatige informatie-inwinning of ga je een week tappen en is er dan waarschijnlijk ook genoeg informatie?" - OvJ

Een OvJ vindt dat er, naast de tap, niet veel andere mogelijkheden zijn om zo dicht bij iemand te komen. Een respondent die gespecialiseerd is in de aanpak van zware criminaliteit geeft aan het belangrijk te vinden dat er alternatieven zijn bekeken voordat de tap ingezet wordt. Maar op grond van voorkennis en ervaring met bepaalde verdachten en zaken weet men vaak dat sommige opsporingsmiddelen niet werken en dat er dus wel direct getapt moet gaan worden.

> "Met zo'n container is het natuurlijk al heel snel dat je dat nummer gaat tappen omdat je anders niet weet hoe je bij zo'n verdachte moet komen; je hebt niet zo veel mogelijkheden om zo dicht bij iemand te komen als met tappen. Er zijn vaak niet zoveel andere opsporingsmiddelen inzetbaar." – OvJ

De subsidiariteitseis lijkt vooral een juridische eis waaraan in de praktijk moeilijk of niet altijd kan worden getoetst. De RC's geven aan wel eens een tapaanvraag af te wijzen, maar dit gebeurt niet vaak omdat er niet wordt voldaan aan de subsidiariteitseis. Wel worden er soms tapaanvragen afgewezen omdat de inzet van het middel niet noodzakelijk wordt geacht voor het opsporingsproces. Dat betekent niet dat er niet aan de subsidiariteitseis wordt voldaan – in de zin dat de informatie met een ander opsporingsmiddel kan worden achterhaald. Veeleer is het in die gevallen zo dat de RC van een specifieke tap weinig meerwaarde verwacht voor het opsporingsproces.

> "Meestal als ik afwijs, zet ik erbij dat je deze tap niet nodig hebt voor je opsporing. Maar goed je blijft die afweging maken: welke belangen zijn er in het spel." - RC

Uit de gesprekken blijkt dat maar weinig eerste tapaanvragen door de RC worden afgewezen. Exacte aantallen zijn niet te geven omdat toe- of afwijzingen niet worden geregistreerd. Geen van de RC's is in staat het aantal toe- en afwijzingen uit te drukken in percentages. Vaak wordt bij de beantwoording van de vraag hoe vaak er percentueel wordt afgewezen en om welke redenen dat vooral gebeurt, teruggedacht aan de laatste keer dat een tapaanvraag werd afgewezen. Een onvoldoende gemotiveerde aanvraag was de meest genoemde reden om een tapaanvraag af te wijzen. Een reden waarom de meeste tapaanvragen worden goedgekeurd en slechts een heel klein deel wordt afgewezen, ligt vermoedelijk in het feit dat er twee toetsingen plaatsvinden: één door de OvJ en één door de RC.

> "De toets van subsidiariteit en proportionaliteit vindt tweemaal plaats volgens mij. Ik vind het wel of niet goed en als ik het niet goed vind gaat het niet gebeuren." – OvJ.

> "Ik zeg een stuk vaker ja dan nee. Omdat je ook al de eerste schifting hebt gehad door de OvJ, die mogelijk zegt 'geen sprake van, dat gaan we niet doen." - RC

Wanneer de inzet van een tap wordt overwogen geven de OvJ's aan hierbij rekening te houden met de eisen van proportionaliteit en subsidiariteit. Als de OvJ niet achter een tapaanvraag staat, zal deze niet snel aan de RC worden voorgelegd. Meerdere OvJ's geven

aan bij grensgevallen of in moeilijke zaken wel eens contact op te nemen met een RC voor informeel overleg of om juridische grenzen af te tasten.

> "Het gebeurt wel eens dat de politie met een verzoek komt om te gaan tappen en dat ik denk dat doen we niet. Soms denk je dan als officier, nou ja het kan en het kan ook niet en dan ga je overleggen met de rechter-commissaris. Kijk, zo kijk ik er tegen aan, je zou het wel of niet kunnen doen, wat vind jij? Dan weet je eigenlijk wel dat die RC wellicht zegt; nee." - OvJ

Een OvJ van een straatroofteam geeft aan dat hij niet alleen rekening houdt met de mate van het geweld, maar dat hij ook kijkt naar de gevolgen voor het slachtoffer. Hij geeft als voorbeeld dat boven een bepaalde leeftijd het breken van een heup bijna dodelijk geweld is. Hiermee houdt hij rekening bij zijn overwegingen omtrent het aanvragen van een tap op een gestolen mobiele telefoon. Een andere OvJ geeft aan dat wanneer er geen sprake is van geweld er volgens haar toch mogelijkheden zijn voor de inzet van een tap. Zij gaf als voorbeeld een zaak waarin een jongen van 12 ingesloten wordt door een groep van meerdere personen en onder bedreiging zijn telefoon moet afstaan. Dit wordt door de OvJ bestempeld als een ernstig feit, de RC was het in dat geval met haar eens en heeft een tapmachtiging afgegeven.

> "Het algemene gevoel is dat er wel heel makkelijk getapt wordt in Nederland, maar er moet altijd sprake zijn van een ernstig misdrijf. Je moet bij de afweging van toepassing van een dwangmiddel altijd de proportionaliteit en de subsidiariteit afwegen. Proportionaliteit is of het feit ernstig genoeg is om dit middel in te zetten bij deze betrokkene, subsidiariteit is gewoon is er ook een ander middel mogelijk, een minder vergaand middel om dit te bereiken. Dat weeg je altijd af." - RC

De respondenten uit de advocatuur denken hier heel anders over en zien de afwegingen op grond van de proportionaliteits- en subsidiariteitstoets in het geheel niet terug in de aanvraag. Volgens deze respondenten stelt de toets niks voor.

> "Of er nou een proportionaliteitseis of subsidiariteitstoets heeft plaatsgevonden blijkt nergens uit. Ook blijkt nergens uit of de aanvraag inhoudelijk is getoetst. Het is niet voor niets dat advocaten al jaren roepen dat die rechter-commissaris gewoon stempelmachines zijn. Op het kabinet RC komen stapels aanvragen binnen die worden gewoon afgetikt." - advocaat

> "Ik vind dat er wel heel snel wordt getapt op basis van soms flinterdunne pv-tjes [*processen-verbaal*]. Ik denk dat gewoon heel snel een machtiging en een bevel wordt gegeven. Soms heb ik wel eens de neiging om te denken dat het eerste dat men doet is een telefoontap aansluiten. Terwijl ik denk probeer eerst eens wat andere mogelijkheden." - advocaat

Een respondent vertelt dat het zijn ervaring is dat in elke substantiële opsporingszaak getapt wordt. In zijn jarenlange ervaring als advocaat heeft hij zich altijd verbaasd over het gemak waarmee een tap kan worden ingezet. Na de wetswijziging dat niet meer vast hoeft te staan dat de verdachte gespreksdeelnemer is, breidt het tappen volgens hem helemaal uit als een olievlek:

> "…om te kijken of mensen met familieleden of medeverdachten communiceren over het misdrijf waar onderzoek naar wordt gedaan. Maar ik heb nooit de indruk uit dossiers dat serieus stil gestaan wordt bij de vraag: voldoet dit aan de proportionaliteits- en subsidiariteitseis? Integendeel." - advocaat

Volgens een respondent van Bits of Freedom wordt er in Nederland achteloos omgegaan met de inzet van de telefoontap:

> "...het zegt natuurlijk wel heel erg veel dat we in Nederland evenveel taps hebben lopen op een dag als de VS in een heel jaar. Puur als maatstaf. Het gebeurt gewoon heel erg vaak hier. [..] We denken niet dat opsporingsdiensten expres de nieuwe vriendjes van hun dochter gaan zitten afluisteren, tuurlijk niet. Maar er is wel een bepaalde achteloosheid in geslopen die met behulp van wat strengere wet- en regelgeving ondervangen zou moeten worden." - BoF

6.3.2 Capaciteit

Het verwerken van getapte telefoonlijnen is arbeidsintensief werk. De telefoongesprekken, die snel kunnen oplopen tot vele uren gesprekken per dag, moeten worden uitgeluisterd en worden verwerkt voor het strafdossier (zie ook Bloem & Aarts, 2000, p. 133). Informatie die interessant is voor het opsporingsteam moet, zeker in grote zaken, worden gecodeerd om het mogelijk te maken om later nog iets terug te vinden. Bij de beslissing of er in een onderzoek getapt gaat worden en zo ja, hoeveel lijnen dit dan zullen zijn, speelt de beschikbare capaciteit van een opsporingsteam een belangrijke rol. Hierbij houden de teamleider en de OvJ zoveel mogelijk rekening met de werkdruk om het aantal taps niet verlammend te laten zijn voor de rest van het onderzoek. Een respondent van de politie die belast is met de aanpak van zware criminaliteit zegt hierover:

> "In de strategiebepaling kies ik standaard voor de tap, omdat het altijd een extra bijdrage levert. Maar niet zomaar 20 lijnen vanuit de gedachte baat het niet dan schaadt het niet, want het kost heel veel capaciteit." - politie

Problemen in de personele bezetting worden regelmatig opgelost door te schuiven met mensen, daarnaast worden onderzoeken continu afgebouwd en opgeschaald. Wanneer naar een climax wordt toegewerkt – de aanhouding van verdachten - worden er vaak weer extra mensen ingezet voor het *live* uitluisteren van de taplijnen. Een aantal respondenten geeft aan dat er minder taps worden aangesloten wanneer het team aan het plafond zit van hun capaciteit. Behalve als het taps betreft die door tolken moeten worden uitgeluisterd en uitgewerkt:

> "….daar hebben we geen capaciteit te verliezen. Daar ben ik makkelijker in. Nederlandse taps moet ik in de gaten houden, want die moeten allemaal uitgewerkt worden." – politie

Opvallend is dat alle respondenten uit regio B capaciteit als eerste noemen bij het beantwoorden van de vraag welke overwegingen een rol spelen bij de inzet van de telefoontap. Voor de respondenten in regio A speelt capaciteit een minder grote rol. De respondenten uit regio B vertellen dat ze kampen met personeelstekort, terwijl de misdaad in die regio steeds professioneler is en beter wordt georganiseerd. Vooral de aantallen wietplantages en de georganiseerde misdaad uit het Oostblok vormen daar een groeiende 'uitdaging'.

> "Er is een schrijnend tekort aan rechercheurs. Vraag me niet hoe dat komt. Zoals ik al zei, als je eigenlijk vijf of zes nummers wilt tappen, dan ga je kijken welke we persé moeten tappen. Er komen er dan drie of twee uit en die andere schuiven we even terzijde. We kunnen niet meteen met zes beginnen, dat kan gewoon niet." - politie

Het tekort aan personeel dwingt de teamleiders de overwegingen om te gaan tappen nog eens extra kritisch af te wegen. De verwachte opbrengst moet opwegen tegen de capaciteit die nodig is voor het uitluisteren en uitwerken. In regio A is capaciteit ook een overweging bij de inzet van de tap, maar het lijkt erop alsof capaciteit minder dwingend is in de besluitvorming. Het moment waarop capaciteit in beide regio's geen discussiepunt lijkt, is bij calamiteiten, omdat het daarbij gaat om grote onderzoeken naar ernstige misdrijven die van tevoren niet kunnen worden gepland.

> "Zo'n TGO wordt gelijk opgeschaald naar 30 man, dezelfde dag nog. Als er getapt moet worden dan wordt er getapt. Als er 10 of 20 lijnen moeten lopen, dan gaan die alle 20 lopen." - politie

Verschillende respondenten geven aan lijnen af te sluiten als het aantal taps een te grote druk legt op het team. Hierbij stoot men eerst de minst relevante lijnen af. Maar een respondent geeft toe dat het aansluiten van een tap makkelijker gaat dan het beslissen dat er een lijn afgesloten moet worden door capaciteitstekort. Een andere respondent vertelt dat door capaciteitsproblemen de tap niet altijd op tijd uitgeluisterd kan worden.

> "Je zit op overvallers te tappen (..) en het is belangrijk dat je live tapt. Maar dat vergt wel capaciteit want dan moet je bijna 16 uur per dag die tapkamer bezetten en dat kan ik niet ophoesten. Dan zeggen we echt, in overleg met de officier, dat we om 6 uur stoppen met luisteren. Want we kunnen het niet. Dat zijn momenten dat ik ook afstem met mijn districtschef, dat hij weet om die en die redenen gaan wij nu niet luisteren. Wat tot gevolg kan hebben dat er vanavond een overval gepleegd gaat worden die we eigenlijk mee hadden kunnen krijgen, maar we gaan het niet doen." - politie

Dit zijn situaties die volgens respondenten voorkomen dienen te worden door vooraf de inzet van het aantal taps kritisch af te wegen. Het opvragen en bestuderen van historische verkeersgegevens kan hierin een belangrijke rol spelen. Het geeft inzicht in hoe vaak en hoe lang er gebeld wordt met een bepaald nummer, hetgeen gebruikt kan worden om vooraf de capaciteit voor de verwerking van een tap in te schatten. Wanneer uit de verkeersgegevens blijkt dat een nummer heel veel gebruikt wordt, kan dit een overweging zijn dat nummer wel te gaan tappen vanwege de grote kans dat een tap op dat nummer informatie oplevert, maar het kan ook een overweging zijn om het nummer juist niet te gaan tappen vanwege de capaciteit die ermee gemoeid zal zijn. Op het gebruik van historische verkeersgegevens komen we nog uitgebreid terug in paragraaf 6.8. Er komen ook situaties voor waarin een team meer moet tappen dan het eigenlijk zou willen om bepaalde communicatiestromen in beeld te kunnen krijgen, en om te voorkómen dat er - door bepaalde nummers te selecteren - een vertekend beeld ontstaat van de situatie.

> "…je zegt we willen deze persoon tappen, en wanneer je erachter komt dat hij nog drie andere nummers heeft, dan wil ik die drie ook tappen. Voor mijn informatievergaring en dat de verdediging straks niet kan zeggen dat er allerlei dingen zijn gemist. Als je A zegt moet je ook B zeggen, als iemand drie telefoonnummers heeft, moet je ze alle drie doen." - OvJ

6.3.3 Gemak

Naast capaciteit en de eisen van subsidiariteit en proportionaliteit speelt het gemak waarmee een tap vanachter het bureau kan worden gerealiseerd een rol bij de overweging om te gaan tappen. Zeker in vergelijking met het realiseren van de inzet van bepaalde andere bijzondere opsporingsbevoegdheden, is een tap snel en eenvoudig te regelen. Bovendien levert een tap ook vaak snel relevante opsporingsinformatie op.

> "Afgezien wat je van tappen vindt, het is natuurlijk een middel dat heel veel rendement geeft. Als je 25 lijnen zet weet je precies hoe het zit. Het gaat makkelijk, er zijn maar weinig RC's die zeggen ik geef hem niet, OvJ is akkoord. Als het een buitenlandse tap is doet de tolk het werk voor je. Geld wordt niet omgeslagen naar onderzoeksniveau dus daar heb je geen last van." - politie

> "De tap is gemak, bekendheid met het systeem en het middel. Het is verdomd lastig om buiten dat kader te stappen, want het kan wel eens minder snel het gewenste resultaat opleveren." - politie

Het gemak waarmee de tap te realiseren valt, is voor velen dan ook een reden om voor de tap te kiezen en niet voor een opsporingsmiddel waarvoor minder bekende administratieve, tactische en juridische drempels moeten worden genomen.

6.3.4 Persoonlijke voorkeur van de teamleider

Uit de gesprekken blijkt dat de persoonlijke voorkeur van de teamleider en/of OvJ een rol speelt bij de overwegingen om te gaan tappen. Uit onderzoek van Kruisbergen & De Jong (2010, p. 152-153) komt naar voren dat de inzet van bijzondere opsporingsbevoegdheden afhangt van kennis en ervaring ermee. Ook speelt houding ten opzichte van een opsporingsmiddel, dus de wijze waarop men tegen het opsporingsmiddel aankijkt, een rol bij overweging omtrent de inzet ervan.
Een aantal respondenten blijkt geen liefhebber te zijn van de tap en geeft aan de tap pas in te willen zetten als het echt niet anders kan. Zij vinden dat de tap te veel capaciteit opslokt en de flexibiliteit uit het team haalt. Een respondent geeft aan dat hij zijn team liever de straat op stuurt om buurtbewoners te spreken en dat het aanwezig zijn in de wijk ook veel resultaat oplevert.

> "Het tappen is een hele traditionele ouderwetse opsporingsmethode. Het is vooral een heel duur middel en kost gewoon heel veel capaciteit. (…) Ik heb de rechercheurs liever anders." - politie

Toch zeggen respondenten die geen voorstander zijn van de telefoontap dat ze niet zonder de tap kunnen. Wel proberen ze de inzet ervan zo kort mogelijk te houden.
Andere respondenten vinden het een geweldig opsporingsmiddel. Deze respondenten zetten, volgens eigen zeggen, daar waar mogelijk de tap eigenlijk standaard in.

> "Als door bewijs één verdachte bekend is en die loopt nog op straat. Die ga je dan vooral tappen. Waarom? Omdat je wilt weten wie de overige daders zijn. Dan ga je naar Opsporing Verzocht, je plaatst het in de krant, je gooit het item er lekker in en dan heb je de stille hoop dat ze elkaar gaan bellen van 'jeetje, we waren op televisie die zaak'. Taps zijn zinnig, echt." - politie

Resultaten uit het verleden bepalen de inzet van opsporingsmiddelen in het heden. Indien men voorheen positieve resultaten heeft behaald met een bepaald opsporingsmiddel, is men eerder geneigd wederom dat opsporingsmiddel in te zetten (zie hierover ook De Poot et al., 2004, p. 256-257). Opsporingsmiddelen waarmee negatieve ervaringen zijn opgedaan worden het liefst vermeden. Sommige opsporingsteams komen er niet toe bepaalde opsporingsmiddelen in te zetten, vanwege onbekendheid met het middel, waardoor ze niet de kans krijgen ervaring met deze opsporingsmiddelen op te doen en de specifieke (on)mogelijkheden ervan leren kennen.
Zoals gezegd speelt houding die men ten aanzien van bepaalde opsporingsmiddelen heeft ontwikkeld ook een rol bij de overwegingen om die middelen in te zetten. Meerdere respondenten maken de vergelijking met Amerika waar men veel gebruik maakt van

undercoverbevoegdheden. Deze opsporingsmiddelen worden hier als 'zwaar' ervaren. Deze perceptie zorgt er mede voor dat deze middelen minder vaak worden ingezet dan bijvoorbeeld de tap, wat als een minder zwaar opsporingsmiddel wordt ervaren.

6.3.5 Tapcultuur

Respondenten herkennen zich in de uitspraak dat het tappen is verankerd in de Nederlandse opsporingspraktijk en een lange geschiedenis kent met vele succesverhalen. Maar tegelijkertijd vinden ze dat dit niet leidt tot buitensporig veel tappen. De algemene opinie van de respondenten is dat de tap veelvuldig wordt ingezet maar dit weloverwogen gebeurt.

> "Wij tappen veel en dat kan in Nederland omdat we heel transparant zijn" - ULI
> "Ja, er wordt veel getapt, maar niet omdat dat de cultuur is" – politie
> "We kijken er kritisch naar en weten wat de beperkingen en nadelen zijn. Maar het is wel een standaardmiddel geworden." - politie

Uit de gesprekken komt naar voren dat er binnen de onderzochte regio's initiatieven en ideeën bestaan over het terugdringen van het aantal taps door bijvoorbeeld het opsporingsonderzoek anders in te richten.

> "Wij [in regio B] krijgen van stuurgroepen vaak de opdracht mee: je gaat dit onderzoek doen maar er wordt niet getapt. Probeer het maar op een andere manier. Probeer het financieel in te vliegen, of op een andere manier. Maar niet tappen. Dat is puur en alleen om van dat traditionele af te willen, van die cultuur af te willen." - politie

> "We zijn [in regio A] nu meer dadergericht dan dat we zaaksgericht aan het opsporen zijn. Dus het heeft geen nut meer om links en rechts maar stekkers erin te stoppen bij mensen die zijdelings betrokken zijn bij een zaak want die gaan we toch nooit meer aanpakken." – politie

Dezelfde respondent uit regio A geeft ook aan dat men is afgestapt van veel langlopende onderzoeken naar zware criminaliteit. De sterkere focus op de hoofdverdachten hangt daarmee samen. Na drie maanden opsporen worden de resultaten van het opsporingsonderzoek geëvalueerd en wordt besloten of er nog een verlenging van maximaal twee maanden volgt, of dat het onderzoek moet worden stopgezet. Omdat er in een korte periode veel informatie moet worden vergaard grijpt men volgens deze respondent sneller naar de tap. Dit omdat het een opsporingsmiddel is dat snel veel informatie oplevert:

> "In die drie maanden voel je je als opsporing wel betrokken bij die zaak en wil je gewoon die zaak rond hebben of je verlenging krijgen. Dat betekent dat je snel door moet pakken (…) om het voor elkaar krijgen om zo'n zaak rond te hebben binnen de gestelde termijn. En dat maakt dat het verzoek naar de artikel 126 bevoegdheden [onder andere de tap] explosief stijgt. (…) Logisch dat men dan wat sneller naar de wat hardere middelen grijpt." – politie

De korte termijn die hen gesteld wordt voor het uitvoeren van een onderzoek leidt er dus toe dat de opsporingsteams hoog inzetten om een zo goed mogelijk resultaat te behalen. Het hoog inzetten lijkt echter niet aan te sluiten bij de doelstelling om het aantal taps terug te dringen.

6.4 Wie wordt er getapt

Als besloten wordt een tap aan te sluiten kan deze zowel op een verdachte als op een betrokkene worden ingezet. Wanneer het nummer van de verdachte niet bekend is kan dit vaak achterhaald worden door een tap op naaste familie of de partner van deze persoon in te zetten. Dit geldt voor zaken waarin gericht op bepaalde verdachten wordt gerechercheerd. Er zijn ook zaken waarin de verdachte nog moet worden opgespoord. In dat geval gaat men anders te werk. Als het misdrijf ernstig genoeg is – zoals bij een moordzaak – kunnen er taps worden aangesloten op de nummers waarmee het slachtoffer als laatste heeft gebeld. Wie er in contact stond met het slachtoffer en of deze personen iets met het misdrijf te maken hebben, kan dan later tijdens het onderzoek worden achterhaald. Ook wordt er in dergelijke situaties in de sociale kring van het slachtoffer getapt om op die manier informatie te krijgen over de leefwereld van het slachtoffer en over mogelijke motieven voor de moord. Op die manier probeert men aanknopingspunten te vinden waarmee verder richting kan worden gegeven aan het onderzoek.

> "Je zet de telefoontap eerder op een verdachte in, maar soms moet je ook op een betrokkene inzetten om bij een verdachte te komen. Soms is dat zelfs gewoon de reden waarom je iemand anders gaat tappen." - politie

> "Eigenlijk is de belangrijkste reden dat je alles wilt weten van de mogelijke verdachte. En als het niet de mogelijke verdachte is, zelfs van het slachtoffer. Dat is van belang: in welke wereld leeft hij en noem maar op. Dan ga je rondom het slachtoffer tappen." - politie

RC's, OvJ's maar ook een aantal politiefunctionarissen geven aan voorzichtiger te zijn met het plaatsen van een tap op een betrokkene dan op een verdachte. Men vindt een tap op een betrokkene vaak ingrijpender. Sommige respondenten geven aan op grond hiervan de termijn waarvoor een tap wordt aangevraagd te verkorten naar bijvoorbeeld twee weken in plaats van de standaard vier weken. Een tap op een betrokkene moet in de aanvraag ook beter worden gemotiveerd. In het algemeen vinden respondenten het gemakkelijker om een verdachte te tappen, dan een betrokkene.

> "Op moment dat uit feiten en omstandigheden een redelijk vermoeden van schuld komt dat jij iets gedaan hebt, dan vind ik het voor mijn eigen gemoedstoestand makkelijker om te zeggen nou wij gaan jou tappen, dan dat wij jouw broertjes, zusjes, moeder die er helemaal niks mee te maken hebben gaan tappen. (..) Bij betrokkenen leg ik de lat hoger." - RC

6.5 Aantal taps per onderzoek

Het aantal telefoontaps per onderzoek is zeer verschillend en onder meer afhankelijk van het delict, de omstandigheden, de capaciteit van het team en de persoonlijke voorkeur van de teamleider. Zo kan in een zaak waarbij een mobiele telefoon is gestolen worden besloten om voor een korte periode een tap aan te sluiten op de telefoon (IMEI tap) én op het telefoonnummer. Deze twee taps kunnen voldoende zijn om de zaak af te ronden. In een grotere zaak kan het aantal taps daarentegen behoorlijk oplopen. Wanneer men geen verdachten in beeld heeft begint het zoeken naar aanknopingspunten. In dat geval kunnen de scenario's die zijn opgesteld een leidraad vormen voor de personen die onder de tap komen te staan.

> "Dan ga je de kring steeds breder maken en dan heb je op een gegeven moment in die eerste twee en een halve maand al 40 a 50 taps aangesloten die nergens toe hebben geleid maar die wel noodzakelijk waren om überhaupt een richting te krijgen.- politie

> "Hoeveel taps er lopen in een zaak is afhankelijk van de groepering waarop je werkt, hoeveel telefoons ze hebben, hoe vaak ze van telefoon wisselen. Vaak moet je de telefoon (IMEI) en het sim-kaartje tappen in onze zaken. We proberen zo min mogelijk te tappen, maar aan het eind van het onderzoek blijken het er altijd veel te zijn." - politie

Het komt vaak voor dat verdachten meerdere telefoons in gebruik hebben die dan ook allemaal onder de tap staan. Op de vraag hoeveel taps gemiddeld per onderzoek worden aangesloten kunnen respondenten geen antwoord geven. Dit blijkt zeer wisselend te zijn, uiteenlopend van geen tot in totaal soms wel 200 taps. De teamleiders en OvJ's kunnen in hun beleving een onbegrensd aantal taps inzetten bij hun onderzoeken. Er zijn geen quota vastgesteld of afspraken gemaakt over het aantal in te zetten taps per jaar.

6.6 Spoedtap

Voor de inzet van een spoedtap moet er aan de eisen van een 'normale' tap zijn voldaan. Daarnaast moet de noodzaak tot onmiddellijk tappen aanwezig zijn om te voorkomen dat belangrijke informatie verloren gaat of om snel ingrijpen mogelijk te maken. Dit is zoals gezegd bijvoorbeeld het geval bij een straatroof waarbij de mobiele telefoon van het slachtoffer is afgenomen. In de eerste uren na de roof is de kans het grootst dat de dader de telefoon gebruikt. Daarna is de telefoon meestal al doorverkocht en is de dader (bijna) niet meer te traceren.[25]
De inzet van een spoedtap is soms ook noodzakelijk als er op de dag dat er een belangrijke actie gepland staat een nieuw telefoonnummer over een getapte lijn komt. In dat geval wil men het nieuwe nummer ook onder de tap hebben om controle te kunnen houden over het telefoonverkeer.

> "Normaal is het geen spoedtap als we meekrijgen dat hij weer een ander nummer heeft. Dan doen we een gewone aanvraag. Vorige week krijg je mee dat er 'vanavond een deal gaat plaatsvinden' en dat hoor je dan om 14 uur 's middags. Dan maken we daar een spoedtap van omdat je die avond een deal krijgt."- OvJ

Een normale tapaanvraag wordt gemiddeld binnen 2 uur uitgevoerd. Ten aanzien van tapbevel dat na 14.00 uur bij de ULI binnenkomt, kan niet worden gegarandeerd dat die dezelfde dag wordt uitgevoerd. Het is dan mogelijk dat het tapbevel pas de volgende dag wordt uitgevoerd. Wanneer er een goede reden is om niet langer te wachten met tappen kan gekozen worden voor een spoedtap. Deze is binnen een half uur te realiseren. Over het algemeen zijn de respondenten van mening dat als er geen echte spoed is, er dan geen spoedtap moet worden aangevraagd.

> "Als het vandaag niet lukt voor tweeën dan komt het gewoon morgen toch. Spoed is spoed." – OvJ

Bij de aanvraag van een spoedtap kan de RC na telefonisch overleg met de OvJ een machtiging tot tappen afgeven. Een OvJ geeft aan nog nooit te hebben meegemaakt dat de RC een spoedaanvraag afwijst.

> "De RC mag ervan uitgaan dat de officier die hem om 3 uur 's nachts belt, niet zomaar een tapje gaat aanvragen." – OvJ

[25] Er wordt bij een roof alleen gebruik gemaakt van een spoedtap wanneer de gestolen mobiele telefoon enige waarde heeft en/of als er geweld is toegepast.

Een spoedtap wordt meestal voor een periode van 1 tot 2 weken aangevraagd. Dit is korter dan de maximale looptijd van een tap. De geïnterviewde RC's geven als reden hiervoor dat de informatie waarop de spoedtap wordt aangevraagd vaak beperkter is. De verhouding tussen normale taps en spoedtaps verschilt per type onderzoeksteam. Over het algemeen zijn er veel minder spoedtaps dan gewone taps. Uitzondering hierop zijn de straatroofteams die zoals gezegd vaak gebruik maken van (korte) spoedtaps wanneer er sprake is van gewelddadige berovingen waarbij een mobiele telefoon is buitgemaakt.

> "We besluiten meteen over te gaan tot een spoedtap. Want de kans dat de dader het ding toch even snel gebruikt die is gewoon heel reëel gebleken. En op grond van ervaring doen we op dat moment altijd standaard een spoedtap. Weliswaar maar voor één of twee dagen maar we doen het wel. Bij elke straatroof, standaard." – politie

6.7 CIOT

6.7.1 Hoeveelheid bevragingen

Voordat een tapaanvraag tot stand komt, zal moeten worden nagegaan of het betreffende nummer nog steeds in gebruik is. Dit kan door middel van een bevraging bij het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Daarmee kunnen tenaamstellingen van telefoonnummers en IP-adressen worden achterhaald. Aan vaste en mobiele telefoonverbindingen op basis van een abonnement hangen vaak deze identificerende gegevens vast. Bij prepaid telefoonnummers is dat anders. Deze staan wel in het CIOT, maar er hangen vaak geen identificerende gegevens aan. Wel staat in het CIOT bij welke aanbieder het telefoonnummer is uitgegeven. Verdachten maken vaak gebruik van prepaid telefoonnummers, hetgeen de identificatie van deze personen bemoeilijkt. Een respondent zegt hierover:

> "Het zijn allemaal prepaids. Negentig procent van wat wij tappen is prepaid. De laatste keer dat ik een vast nummer heb getapt is ook al jaren terug ofzo." - OvJ

Naast de bevraging van gegevens van individuele personen, kunnen ook gegevens behorende bij telefoonnummers die door middel van mastgegevens zijn binnengehaald bij het CIOT worden verkregen. Een respondent van het CIOT zegt dat het grootste aantal aanvragen dat ze in één keer hebben gehad 30.000 is geweest. Hij legt uit:

> "Als er op een bepaalde plek een moord is gepleegd en je loopt een beetje vast, dan ga je een aantal masten in de buurt leeghalen op dat tijdstip van die dag. En dan kunnen er zo zo'n 30.000 telefoonnummers actief zijn geweest. Op die plaats delict in die buurt. En die 30.000 dat duurt ongeveer een paar uur, dan hebben ze ze allemaal." – CIOT

Het aantal CIOT-bevragingen is in de loop der jaren sterk toegenomen. In 2007 is het CIOT 1,7 miljoen keer bevraagd, in 2008 2,8 miljoen keer en in 2009 ruim 2,9 miljoen keer (CIOT, 2008; CIOT, 2009). Als we uitgaan van het jaar 2009 zijn van de 2,9 miljoen CIOT-bevragingen er minimaal 24.724 gesteld in het kader van het aansluiten van een telefoontap. De overige vragen zijn onder andere op basis van het opvragen van verkeersgegevens, gevonden telefoonnummers in een agenda, het binnenhalen van zendmastgegevens, en zogenaamde contranummers of tegennummers uit een tap die worden bevraagd, om identificerende gegevens van die nummers te kunnen achterhalen. Het door het CIOT halen van tegennummers, telefoonnummers die over een getapte telefoonlijn komen, levert al snel een groot aantal bevragingen op. Tegennummers die in een tap naar voren komen mogen automatisch door het CIOT gehaald worden om te kijken of ze op naam staan. De toestemming voor die bevraging is geïncorporeerd in het model voor het vorderen van verkeersgegevens, hiervoor hoeft dus geen apart bevel worden afgegeven. Het bevragen

van tegennummers doet men om te bezien met wie gebeld wordt door de getapte persoon. Wanneer het getapte nummer een drukke lijn blijkt te zijn, levert dit al gauw aardig wat tegennummers op.

> "Dat levert op dat er heel veel bevragingen zijn en dat is iets om over na te denken. Waar worden die gegevens weggeschreven? En er zullen tig keer dezelfde bevragingen worden gedaan. Daar valt best in te bezuinigen, als je je bijvoorbeeld beperkt tot de gegevens van de belangrijke gesprekken." – politie

Er is veel kritiek gekomen op de hoeveelheid CIOT-bevragingen, omdat het een schending van de privacy met zich brengt. Immers, van allerlei personen worden NAW-gegevens behorend bij een telefoonnummer of IP-adres opgevraagd. Een respondent probeert uit te leggen waarom er zoveel bevraagd wordt:

> "Ja, dan kun je zeggen, hoe kan dat nou? Je kunt er beelden bij hebben. Als we een aantal onderzoeken bekijken waarvan politie en justitie zeggen jullie hebben tunnelvisie gehad, dat betekent dat je kennelijk maar heel beperkt hebt gekeken. Je kunt ook zeggen, je gaat heel breed kijken. Dan zijn dit wel één van die dingen die er mogelijk bij zitten. Ik weet niet of dat zo is, maar dat gevoel heb ik ook. Hoe breder je kijkt, hoe meer je gaat bevragen. Alleen je moet wel zodanig bevragen dat je later de stukken die je niet nodig hebt voor de rechtszitting dat je die weer kunt vernietigen." – politie

De regio's verschillen in de hoeveelheid bevragingen. Volgens een respondent heeft dat te maken met de onderzoeken die er lopen en hoe breed deze zijn.

6.7.2 In control statement

Het bevragen van het CIOT is met wettelijke waarborgen omkleed. In het verleden heeft de politie zich bij het bevragen van het CIOT niet altijd aan de (administratieve) regels gehouden. Dat heeft aanbieders bewogen om te zeggen dat zij, voordat zij de identificerende gegevens van hun klanten dagelijks aan het CIOT leveren, zeker willen weten dat de politie haar proces op orde heeft. Korpsen, alsook andere (bijzondere) opsporingsdiensten dienen jaarlijks een *in control statement* af te geven om het CIOT te kunnen bevragen. Het niet 'in control' zijn, wil overigens niet zeggen dat ze onrechtmatige bevragingen doen, aldus één van de respondenten.

> "Grasduinen zit er dus niet bij. Alle bevragingen van het systeem zijn uitwerkingen van vorderingen." – OvJ

Opsporingsdiensten dienen zich aan het Besluit CIOT te houden, waarin de procedures beschreven staan. Wanneer een opsporingsdienst administratief niet in control is, kan het de rechtmatigheid niet borgen. Zo moet een opsporingsambtenaar door de korpsbeheerder gemachtigd zijn om CIOT-bevragingen te kunnen doen.
Alle opsporingsdiensten zijn op dit moment 'in control'. Eén van de respondenten die we hebben gesproken geeft cursussen aan korpsen om uit te leggen hoe men moet omgaan met het Besluit CIOT. De korpsen worden vervolgens geaudit om te bezien of ze in control zijn. Niet in control zijn betekent dat het korps niet langer geautoriseerd is om CIOT-bevragingen te doen. Om deze nog wel te kunnen doen moet men naar een ander korps gaan, dat wel in control is, om CIOT-bevragingen te kunnen doen. Dat men hier zo streng op toeziet heeft te maken met privacybescherming. Een respondent zegt:

> "Ik vind de privacy en de wetgeving ontzettend belangrijk. En de gevolgen die aan de privacy zitten. Met name voor de burgers, want jullie zijn ook burgers. Daar probeer ik altijd op te hameren, van wees zorgvuldig met wat je doet." – politie

6.8 Opvragen verkeersgegevens

Verkeersgegevens geven inzicht in het belgedrag van de gebruiker van een telefoonnummer. Door het opvragen van deze gegevens kan inzichtelijk worden gemaakt met wie, hoe vaak, hoe lang en vanaf welke locatie ongeveer er gebeld is met een bepaald telefoonnummer. Dit is tot 12 maanden terug in de tijd opvraagbaar. Dit is de bewaartermijn die voor deze gegevens gesteld is in de Telecommunicatiewet (artikel 13.2a, lid 3, sub a Tw). Verkeersgegevens kunnen door een OvJ, zonder tussenkomst van een RC, worden opgevraagd op basis van artikel 126n Sv. Deze verkeersgegevens komen in de praktijk binnen met een vertraging van maximaal 48 uur.

6.8.1 Historische verkeersgegevens

Als het gaat om onderzoek naar georganiseerde misdrijven, lijken historische verkeersgegevens met name in de voorbereidende fase van een onderzoek van belang. Volgens een zwacri-respondent zijn verdachten vaak alert op het piekmoment van een zaak, wanneer de politie dicht op de zaak zit, en is de communicatiediscipline op die momenten vaak hoog. Maar tijdens de voorbereiding van een onderzoek kunnen verdachten denken dat ze uit de wind zijn. Juist dan kunnen historische verkeersgegevens volgens deze respondent nog wel eens mooie bevindingen opleveren.
Voor TGO-onderzoeken, bijvoorbeeld naar een moordzaak, geldt dat de historische verkeersgegevens veel informatie kunnen opleveren over personen waar het slachtoffer mee in contact stond. In het algemeen probeert men alle contacten in kaart te brengen en te onderzoeken wat de aard was van de relatie en van het contact. Ook worden de gegevens in dat geval gebruikt om verklaringen van getuigen over hun contacten met het slachtoffer te toetsen.
Daarnaast kunnen historische verkeersgegevens een grote rol spelen bij de overweging een bepaald telefoonnummer te gaan tappen. Op basis van het historische belgedrag kan een inschatting worden gemaakt van de capaciteit die nodig is om een eventuele tap uit te luisteren en te verwerken. Wanneer blijkt dat een bepaald nummer zeer intensief wordt gebruikt, kan dit enerzijds voor meerdere respondenten een reden zijn om op dat nummer geen tap aan te sluiten. Anderzijds kan een intensief gebruikt nummer een reden zijn om dat nummer juist wel te tappen, aangezien intensief contact kan duiden op voor de opsporing mogelijk interessante informatie. Ook kan uit de verkeersgegevens blijken dat een telefoonnummer niet meer wordt gebruikt en dat het dus zinloos is om een tap op dat nummer aan te vragen.
De motivatie om historische verkeersgegevens op te vragen is voor een respondent uit een zwacri-team de mogelijkheid om contacten en netwerken binnen een criminele organisatie in alle rust in kaart te brengen zonder de bijkomende werkzaamheden van het uitwerken.
Ook kan het in opsporingsonderzoeken voorkomen dat een getuige vertelt dat hij "gister rond een uur of drie" gebeld is door een bepaalde persoon die wordt gezocht, maar dat hij het nummer niet heeft. In zo'n geval kan een OvJ bijvoorbeeld een beroep doen op artikel 126n Sv en daarmee het nummer eenvoudig achterhalen. Voorts worden de bevragingen gebruikt om verklaringen over wie wanneer voor het laatst contact heeft gehad met bijvoorbeeld een slachtoffer of een vermiste persoon te kunnen toetsen. Als het alleen gaat om het achterhalen van één nummer, zoals in het bovengenoemde voorbeeld, kan worden volstaan met het opvragen van een bestandsanalyse (126nb Sv). Hiermee wordt een minder grote inbreuk gemaakt op de privacy van de getuige, omdat in dat geval niet alle overige, niet relevante, belcontacten van de getuige worden verkregen. Als het opsporingsteam echter verwacht dat ze uitgebreidere informatie nodig heeft over de belcontacten van de getuige met deze gezochte persoon, bijvoorbeeld om verklaringen van de getuige over deze

belcontacten te kunnen toetsen, dan kunnen voor dat doel beter de historische verkeersgegevens van de getuige worden opgevraagd.
Historische verkeersgegevens kunnen ook zicht bieden op personen die mogelijk interessant zijn voor het onderzoek, bijvoorbeeld doordat ze veelvuldig telefonisch contact hebben met een verdachte.
Daarnaast worden historische verkeersgegevens aangevraagd als een OvJ het misdrijf niet zwaar genoeg vindt voor het inzetten van een tap. Aan de hand van de verkeersgegevens kan men dan toch zicht krijgen op de communicatiestromen:

> "Als de officier zegt het [misdrijf] is te licht, dan vragen we of we een histo mogen. Dat kan leiden tot herkenning van nummers en dan gaan we kijken of we daarmee verder kunnen. Dat kan dan net dat stukje informatie geven die een RC of officier overtuigt om wel een tap te krijgen." - politie

Uit de gesprekken die zijn gevoerd in regio B blijkt dat daar, in ieder geval als het gaat om zwacri-zaken en TGO's, nagenoeg geen telefoontap wordt aangesloten voordat de historische verkeersgegevens zijn opgevraagd en geanalyseerd. Door het opvragen van historische verkeersgegevens kan de telefoontap gerichter worden ingezet omdat vooraf een analyse heeft plaatsgevonden van het gebruik van het telefoonnummer waarvan de historische verkeersgegevens zijn opgevraagd. Hierdoor is vooraf al inzicht in het belpatroon van het te tappen telefoonnummer.
Vanuit de ULI wordt dit ook aanbevolen "om te voorkomen dat je een heel zwaar middel toepast wat heel weinig rendement oplevert". Het frequente gebruik van historische verkeersgegevens in regio B is voor een deel toe te schrijven aan het feit dat het een relatief klein korps is dat kampt met een capaciteitsgebrek. Deze omstandigheid dwingt tot een kritische afweging van de in te zetten opsporingsmethoden. Het opvragen van historische verkeersgegevens blijkt in regio B een vaste plek te hebben gekregen bij de overwegingen die een rol spelen bij de inzet van de telefoontap. Deze manier van werken hebben we niet terug kunnen vinden in regio A. Hoewel in regio A ook vaak en veelvuldig gebruik wordt gemaakt van historische verkeersgegevens, lijkt het vooraf bestuderen van verkeersgegevens daar niet zo'n prominente rol te spelen bij de overwegingen om te gaan tappen en bij de vraag welke lijnen getapt zouden moeten worden als in regio B.

Vanuit de ULI wordt het opvragen van historische verkeersgegevens aangemoedigd, maar naar hun mening gebeurt dit nog te weinig. Uit cijfers van de ULI blijkt dat de onderzochte regio B, samen met nog een klein aantal andere regio's, hierop een uitzondering vormen. De respondent van de FIOD blijkt eveneens altijd historische verkeersgegevens op te vragen alvorens te gaan tappen. Vooral het inschatten van de capaciteit die nodig is voor het verwerken van de telefoontap wordt hiervoor als achterliggende reden genoemd. De opsporing zou ongewenste vertraging kunnen oplopen als er in een onderzoek opeens veel meer capaciteit nodig is om te kunnen tappen dan vooraf was gepland. Ook voor de FIOD geldt dat de capaciteit beperkt is, en dat langdurig en veel tappen daarom wordt vermeden.

> "Historische verkeersgegevens daar begin je mee. Vooral om te kijken welke telefoon je wilt hebben. Tegenwoordig is een verdachte met 10 gsm's geen uitzondering meer. Ze hebben een tas vol met genummerde telefoons, die telefoon gebruiken voor die en die telefoon voor die. Het grote probleem van dit moment voor de telefoontaps: Hoe krijg je het goede nummer?" - FIOD

Voor een RC is het opvragen van verkeersgegevens geen voorwaarde voor het toe- of afwijzen van een tap. Dit wordt gezien als taak en verantwoordelijkheid van de OvJ en het speelt geen rol in de besluitvorming. Wel merken de RC's uit regio B op dat het opvragen van historische verkeersgegevens vaker voorkomt. Dit wordt door de RC's gezien als een positieve ontwikkeling.

> "In het verleden kwam dat nauwelijks voor. Dat is duidelijk een tactiekverandering die heeft plaatsgevonden." - RC

Het opvragen van historische verkeersgegevens heeft volgens de respondenten niet altijd zin. Vooral bij kortdurende taps in kleine zaken heeft het volgens hen geen meerwaarde. Men heeft dan het nummer van een verdachte en er is noodzaak voor een tap.
Een respondent geeft aan dat bij TGO's vaak geen tijd is voor het opvragen van historische verkeersgegevens. Er zou kostbare tijd verloren gaan en men wil liever direct over inhoudelijke informatie beschikken. Ook het feit dat het informatie betreft uit het verleden wordt genoemd als nadeel.

> "Je kunt ervoor kiezen eerst verkeersgegevens op te vragen, dan weet je waar iemand is geweest. Maar het zegt niets over met wie de overvaller daar was en waar hij de buit heeft verstopt. Dat is informatie die je over een tap wel kunt krijgen." - OvJ

6.8.2 Toekomstige verkeersgegevens

Het nadeel van historische verkeersgegevens dat zojuist is aangestipt, het feit dat het informatie uit het verleden betreft, is niet aan de orde als men toekomstige verkeersgegevens aanvraagt. Daarmee komen verkeersgegevens binnen van de gesprekken die op dat moment worden gevoerd. Een overweging om enkel toekomstige verkeersgegevens aan te vragen in plaats van een 'gewone' tap, is capaciteit. Met een aanvraag toekomstige verkeersgegevens hoeven de gesprekken niet uitgeluisterd en uitgewerkt te worden.
Een respondent uit een zwacri-team geeft aan dat wanneer van bepaalde verdachten bekend is dat ze inhoudelijk niet over de telefoon communiceren, ook wel eens wordt besloten om te kiezen voor het opvragen van toekomstige verkeersgegevens. Maar wanneer het opsporingsteam vervolgens deze verdachten wil gaan observeren wordt de aanvraag toekomstige verkeersgegevens, na machtiging van de RC, omgezet naar een 'gewone' tap. Toekomstige verkeersgegevens blijken dan ontoereikend omdat het opsporingsteam op zo'n moment over inhoudelijke informatie wil beschikken.
Het opvragen van toekomstige verkeersgegevens wordt door een aantal respondenten genoemd als een minder privacyschendend middel dan de telefoontap, omdat de inhoud van de gesprekken niet wordt opgenomen. Dit volgt ook uit het systeem van de wet: het opvragen van toekomstige verkeersgegevens is een officiersbevoegdheid en voor inzet van de tap is een machtiging van de RC vereist. Het lijkt erop dat toekomstige verkeersgegevens niet vaak worden aangevraagd. Door de respondenten wordt veelal gesproken over de inzet van historische verkeersgegevens en slechts in een enkel geval over toekomstige verkeersgegevens. Harde cijfers hierover ontbreken helaas doordat de aanvragen voor toekomstige verkeersgegevens, in tegenstelling tot de aanvragen voor historische gegevens, niet worden geregistreerd.

6.9 Uitluisteren en uitwerken

De gesprekken die zijn opgenomen met een telefoontap worden opgeslagen in de computersystemen van de ULI. Hierop kunnen geautoriseerde personen inloggen om de gesprekken uit te werken. Niet alles hoeft letterlijk uitgetypt te worden. Voor gesprekken die voor de opsporing niet van belang zijn, volstaat het deze te omschrijven als 'niet ter zake doende'. Er dient een korte beschrijving te worden gegeven van de inhoud van het gesprek. Wel moet het gesprek volledig worden uitgeluisterd.[26]

[26] Zie Aanwijzing opsporingsbevoegdheden, Stcrt, 2011, 3240 (2011A002), in werking getreden op 1 maart 2011.

> “Stel je hebt een gesprek van een uur. Dan kan drie kwartier gaan over een feestje en een kwartier over een zaak. En dat hele uur moet je uitluisteren. Of je wilt of niet, je moet luisteren.” - politie

Het uitwerken van tapgesprekken is arbeidsintensief. Het vraagt capaciteit waar volgens de respondenten altijd een tekort aan is. Een respondent vertelt dat een telefoongesprek van een uur, ongeveer anderhalf uur duurt om uit te werken. Het zijn doorgaans rechercheurs zelf die de taps uitwerken. Eén respondent geeft aan dat de taps in zijn team zoveel mogelijk door de rechercheassistent worden uitgewerkt. De uitgewerkte gesprekken worden dan wel nagelezen door een rechercheur. Wanneer er een interessant gesprek tussen zit wordt dit gesprek opnieuw, dus een derde keer, beoordeeld door bijvoorbeeld een tapcoördinator. Ervaring in het uitwerken van telefoontaps speelt een grote rol bij de kwaliteit:

> “Je zou bijna specialisten moeten hebben” – politie.

Respondenten vertellen dat sommige collega’s beter en vaardiger zijn in het interpreteren van tapgesprekken dan anderen. Zo geeft een respondent het volgende voorbeeld van een fout gemaakt door een onervaren collega:

> “In een gesprek zegt één van die knakkers ‘morgen een ov’. Die collega denkt ‘morgen een ov-jaarkaart halen’. Wat bleek nou, hij ging morgen een overval plegen.” - politie

Er worden bij de politie cursussen georganiseerd waarin het uitwerken en interpreteren van tapgesprekken aan de orde komt en ook tijdens de rechercheopleiding wordt er aandacht aan het tappen besteed. Toch is het, volgens een respondent, een vaardigheid die voornamelijk ‘on the job’ geleerd wordt. De kennisoverdracht tijdens de rechercheopleiding wordt magertjes genoemd. Een andere respondent geeft aan regelmatig moeite te hebben met het vinden van personeel dat de gesprekken op een kwalitatief hoog niveau uit kan werken.

> “Daar blijken we steeds weer tegenaan te lopen. Dan ga je zelf wat gesprekken nalopen en dan denk je: waarom hebben we dat gemist, of waarom hebben ze dat zo opgeschreven. We hebben al een paar keer geroepen dat er een tappool moet worden samengesteld met daarin mensen die alleen maar tappen en die daarvoor goed zijn opgeleid.” - politie

Naast ervaring is continuïteit van de personele bezetting ook van belang. Wanneer er vaak wordt geschoven met personeel krijgt men niet de gelegenheid bekend te raken met de stemmen die over de lijnen komen. Wanneer er geen stemherkenning aanwezig is bij de personen die de taps uitwerken kan het voorkomen dat een stem over een telefoonlijn niet wordt herkend en vervolgens als NN (e.g. een onbekend persoon) gecodeerd wordt, terwijl het een verdachte kan betreffen. Het team kan hierdoor tactisch op het verkeerde been gezet worden.

> “Bij wisselingen van personeel krijg je allemaal van die gesprekken die uitgewerkt zijn welke ik later, omdat het een interessant gesprek is, moet gaan naluisteren, en vervolgens een apart verbaal moet gaan maken waarin staat dat die NN man die daar bedoeld wordt onze verdachte is.” - politie

Het coderen van gesprekken wordt gedaan om het mogelijk te maken later in het onderzoek iets terug te kunnen vinden in de uitgewerkte tapgesprekken. Dit is zeker in grote zaken met veel taps een belangrijke klus die volgens een respondent niet gelijktijdig met het uitwerken gedaan kan worden. In het team worden codes afgesproken en nadat de gesprekken zijn uitgewerkt, tijdens het nalezen, pas toegevoegd. Zo krijgen gesprekken die 'niet ter zake doen' de code 99 mee.
Het moment van uitluisteren en uitwerken van tapgesprekken kan nog wel eens verschillen. Een respondent uit een TGO vertelt dat in zijn team twee à drie vaste 'tappers' zitten die de gesprekken live uitluisteren en daarbij aantekeningen maken. De informatie wordt vervolgens gedeeld met de teamleider om te bepalen of de inhoud van de gesprekken interessant is en of erop geacteerd moet worden. Als het niet interessant is, wordt het gesprek weggeschreven als niet ter zake doende en gaat men verder. Een andere respondent vertelde:

> "Als je tegen het plafond van je capaciteit zit, dan moet je gaan schrappen. Dan schrap je het uitluisteren. Ik ga dan wel verder met opbouwen, maar lijn 1 t/m 3 laat ik links liggen, daar doe ik niks meer mee. Als er gesprekken op die lijnen zijn dan laat ik die gewoon lopen. Maar dan moet het wel heel spannend zijn, want in principe laten we niks lopen anders had ik de tap niet aangevraagd. Maar als het gaat opstapelen en je komt in een soort finale terecht, dan pakken we alleen de hoofdlijnen. Die worden uitgeluisterd, het uitwerken komt later. Dan weet je pas de relevantie van de gesprekken." - politie

Het uitluisteren van de lijnen die men in verband met het capaciteitstekort niet kan bijbenen, wordt dan op een later tijdstip gedaan.
Drie respondenten vertellen weleens een achterstand te hebben bij het uitwerken. Eén daarvan vertelde dat zijn vorige team nog bezig is met het verwerken van vele en langdurige taplijnen die gezet zijn na participatie in een groot onderzoek.

> "Ze zijn nu nog bezig die duizenden tapgesprekken uit te werken. Daar hebben we hier angst voor. Dat gebeurt ons niet. Als we nu een tap aanvragen dan is er al een actiedag gepland. Op de actiedag luistert er één de tap uit en geeft aanwijzingen aan de rest." - politie

Wanneer een TGO wordt samengesteld heeft dat alle voorrang en wordt daarvoor capaciteit bij andere opsporingsteams weggehaald. Dit heeft als gevolg dat het werk bij andere teams stil kan komen te liggen of met minder mensen gewerkt moet worden. Een respondent geeft aan dat in zo'n geval taps wel doordraaien maar dat het uitwerken en uitluisteren niet altijd meer bijgehouden kan worden. Meerdere respondenten zeggen dat ze in principe elke dag naar de taps moeten kijken, maar ze dit wel eens overslaan als het druk is.

> "Soms zit je een hele week de taps uit te werken met het team. Dat hoort erbij. (…) We hebben een hoera-stemming als we de daders hebben, maar het moet wel achteraf allemaal op papier komen." - politie

De respondenten uit de advocatuur vinden de kwaliteit van de uitgewerkte gesprekken wisselend. Wanneer de manier waarop een gesprek is uitgewerkt een bepaalde kleuring heeft die volgens de verdachte niet juist is, kan een advocaat vragen het bewuste gesprek zelf te mogen beluisteren. Parketten blijken verschillend om te gaan met het verzoek van advocaten om gesprekken te mogen beluisteren. Volgens een advocaat is niet ieder parket welwillend in het ter beschikking stellen van de gesprekken. Een respondent vertelt dat hij standaard bekijkt of de taps op de juiste wijze in het dossier terecht zijn gekomen.

> "Wat ik af en toe doe en moet doen vind ik, is de taps zelf beluisteren. Kijken of het op een juiste wijze is neergedaald in het proces-verbaal. En vervolgens ga ik ook kijken of er nog

meer taps zijn, niet alle gesprekken zitten in het dossier, waardoor ik gesprekken mogelijk in een ander perspectief kan plaatsen dan politie en openbaar ministerie doet. Ik vind het echt de moeite waard om dat te controleren" – advocaat

6.10 Tolken

Bij het tappen van telefoongesprekken komt het geregeld voor dat de gesproken taal een andere is dan de Nederlandse. In dat geval schakelen teamleiders een tolk in om de gesprekken te vertalen. Dit zijn doorgaans vaste tolken die zijn gecertificeerd, gescreend en een interne opleiding hebben gehad bij de politie. Echter, de procedures betreffende de omgang en het werken met tolken wordt door de onderzochte regio's en parketten zelf ingevuld en verschillen dan ook op meerdere punten.
Uit de gesprekken met de respondenten van de politie blijkt dat men zeer zorgvuldig is bij het aanstellen of selecteren van een tolk. Bij eerdere slechte ervaringen wordt een tolk niet meer gevraagd om te komen tolken. Wanneer een tapcoördinator of teamleider een tolk binnenkrijgt die hij of zij niet kent, wordt navraag gedaan naar eerdere tolkwerkzaamheden. Bij enige twijfel geven meerdere respondenten aan telefonisch navraag te doen. De reacties op de vraag of men het prettig vindt om met tolken te werken zijn uiteenlopend. Het extra paar handen om tapgesprekken uit te werken wordt door een aantal respondenten genoemd als groot voordeel.

"De tolk zit als het ware op de plek waar normaal de rechercheur zit met z'n koptelefoon. De tolken die ingezet worden, zeker in wat langer lopende onderzoeken, kunnen redelijk goed inschatten wat wel of niet van betekenis is voor het onderzoek." - OvJ

"Wat niet ten koste gaat van de capaciteit is lijnen waarover in een andere taal wordt gesproken. Dan gaat de tolk de tap uitwerken en heb je een reden om door te tappen. Daar heb je geen omkijken meer naar." - politie

Een respondent werkzaam bij de FIOD geeft daarentegen aan, dat werken met een tolk geen rechercheur vrijspeelt:

"Je kunt de tolk niet alleen op de tapkamer laten." - politie

Een respondent van de politie vertelt dat een tolk eigenlijk aan een rechercheur zou moeten vertellen wat er gezegd wordt waarna de rechercheur dit intypt. Dit gebeurt volgens deze respondent zelden omdat het onbegonnen werk is.
In regio B heeft men het werken met tolken, volgens eigen zeggen, met strakke procedures omkleed. Alle tolken werkzaam in deze regio, hebben daar een interne opleiding gekregen. Voordat een tolk de tapkamer ingaat, dient hij/zij telefoons, usb-sticks, fototoestellen en andere elektronische apparatuur op te bergen in hiervoor bedoelde kluisjes die naast de ingang van de tapkamer staan. De tolken zijn geautoriseerd voor de tapsystemen en werken geheel zelfstandig de tapgesprekken uit. De autorisatie werkt alleen voor de zaak waar de tolk op werkt en verloopt zodra de tolk klaar is met zijn werkzaamheden.
Het nadeel dat wordt genoemd van het werken met tolken is de afhankelijkheid. De respondenten vertellen dat, zeker wanneer het een taal is die men zelf niet machtig is, men volledig overgeleverd is aan een tolk.

"Het heeft geen zin om het gesprek na te gaan luisteren, want je verstaat het niet". - FIOD

Op de vraag of het uitwerken van telefoontaps door tolken goed gaat, antwoordt het merendeel positief. Men vraagt tolken die goed werk leveren regelmatig terug. Deze tolken raken zo ingewerkt en thuis in de systemen dat ze deel uitmaken van het opsporingsteam.

Maar ondanks de zorgvuldigheid waarmee de politie te werk gaat bij het selecteren van tolken, gaat er wel eens wat mis.

> "Het is wel voorgekomen dat je een tap naleest en je denkt dat er iets anders wordt bedoeld dan de tolk heeft vertaald. Dit is toen nog eens geverifieerd bij een Surinaamse collega. Deze beaamde dat het gesprek wel over vuurwapens ging, die tolk hoefde niet meer terug te komen." - politie

Bij het vertalen van tapgesprekken gaat het niet enkel om het letterlijk vertalen en uitwerken van een tekst. Er wordt veel meer gevraagd van een tolk. Gesprekken zijn niet altijd woordelijk te vertalen en in een taal kan een woord meerdere betekenissen hebben die afhankelijk zijn van de context van het gesprek. De nuance kan in de opsporing een groot verschil maken. Ook bij het gebruik van versluierde taal is ervaring van een tolk onontbeerlijk om de juiste interpretatie of strekking van een gesprek te kunnen geven. Voor de opsporing kunnen niet relevante gesprekken afgedaan worden als 'niet ter zake doende'. Echter, het is niet zo eenvoudig als het lijkt om deze gesprekken te herkennen als wel ter zake doende. Ook dit moet een tolk kunnen.
Het vinden van een tolk blijkt niet altijd eenvoudig te zijn. Voor bepaalde talen bestaat een schaarste waardoor een opsporingsteam soms moet wachten tot een tolk beschikbaar is. De opsporing kan hierdoor vertraging oplopen. Het ondervangen van de tekorten is niet eenvoudig. Een knelpunt dat door de respondenten wordt aangegeven is, dat een tolk van onbesproken gedrag dient te zijn en dit vaak moeilijk of niet te achterhalen is in het land van herkomst. Een ander probleem is het vaststellen in hoeverre de tolken gelieerd zijn aan de groeperingen waarop wordt gewerkt. Dat kan natuurlijk in zekere zin ook gelden voor Nederlanders maar in dat geval zijn de tapgesprekken bij twijfel makkelijker te controleren.

> "In sommige talen ben je afhankelijk van iemand waarvan je twijfelt over de betrouwbaarheid, maar je hebt geen keuze." - politie

Om vertaalfouten of verschillende vertaalinterpretaties te ondervangen zijn waarborgen ingebouwd. Een gesprek kan altijd opnieuw door een andere vertaler worden uitgewerkt. Een respondent vertelt dat de nuance, vooral bij meer ingewikkelde talen, dan net even anders kan zijn. Meerdere respondenten vertellen dat ze cruciale gesprekken een tweede keer laten vertalen. Niet uit wantrouwen richting hun tolk maar vanwege het belang van het gesprek voor de bewijsvoering.

> "De manier van tappen en de kwaliteit van uitwerken is wel belangrijk voor de keuzes die je maakt, maar ik geloof niet dat er hele grote onzorgvuldigheden zijn, omdat belangrijke passages altijd opnieuw worden beoordeeld als het gesprek gebruikt wordt als bewijs." – politie

Respondenten uit de advocatuur geven aan dat wanneer hun cliënt aangeeft dat een tapgesprek niet goed is vertaald, dat een reden is om te gaan toetsen.

> "Soms is dit gegrond, maar lang niet altijd. Over het algemeen beheersen die tolken hun werk goed, ze doen gewoon hun best." - advocaat

Een opvallende rol van de tolk werd genoemd door een teamleider. Deze vertelde dat zijn team een tolk wel eens om culturele achtergrondinformatie vraagt, bijvoorbeeld over man/vrouw-verschillen binnen een cultuur. Sommige tolken werken lange tijd, soms jaren, aan het vertalen van tapgesprekken die zijn opgenomen in meerdere opsporingsonderzoeken maar zich allemaal afspelen binnen hetzelfde milieu. Volgens deze respondent hebben de betreffende tolken hierdoor een helikopterview gekregen die het opsporingsteam niet heeft en waar de respondent graag gebruik van maakt binnen zijn opsporingsteam.

6.11 Verlengen of afsluiten

Een tap kan in eerste instantie voor een periode van ten hoogste vier weken worden aangevraagd en toegekend. Na deze periode kan de tap steeds opnieuw met een termijn van ten hoogste vier weken worden verlengd. Het afsluiten van een tap kan op elk willekeurig moment worden gedaan, ook voordat de afgegeven termijn is verstreken. Bij het niet aanvragen van een verlenging, wordt de tap automatisch afgesloten na het verstrijken van de afgegeven periode. Wat zijn de overwegingen om te verlengen dan wel af te sluiten? En op welk moment gebeurt dat?
De overweging om een tap te verlengen is met name of de tap iets oplevert in verhouding tot de capaciteit die het kost. Wanneer een tap relevante informatie heeft opgeleverd, kan dit een reden zijn om verlenging aan te vragen. Een verlenging wordt door de RC in principe hetzelfde beoordeeld als een nieuwe tapaanvraag. Is de verdenking er (nog)? Is de tap (nog) dringend noodzakelijk voor het onderzoek? Bij de beoordeling van een verlenging van een tap door de RC, weegt de opbrengst van de tap op de betreffende lijn zwaar mee. Een verlenging moet immers zinvol zijn. Aan de hand van tapgesprekken die in de eerste periode zijn onderschept, moet in een proces-verbaal worden onderbouwd waarom een verlenging noodzakelijk is voor het onderzoek.
Als een lijn geen relevante informatie oplevert, geven de respondenten aan de tap voortijdig af te sluiten. Maar ook een tekort aan capaciteit om de lijnen uit te luisteren en uit te werken kan een reden zijn om een tap voortijdig te beëindigen. Ook komt het voor dat een getapte lijn 'dood' blijkt te zijn en wanneer een zaak ten einde is sluit men de lijnen ook af.
Soms zitten het rechercheteam en de OvJ niet op één lijn. Het komt voor dat het rechercheteam een tap wil laten doorlopen maar de OvJ het daar niet mee eens is. Maar omdat het rechercheteam de beste inschatting kan maken van de opbrengst van een tap, is het vaker het rechercheteam dat voorstelt om een lijn af te sluiten. De OvJ neemt de uiteindelijke beslissing, waarbij doorgaans het advies van het rechercheteam wordt opgevolgd.
De RC's geven aan dat hoe langer een tap loopt, hoe kritischer men wordt voor het toekennen van een verlenging. Zo zegt een RC:

> "Op een gegeven moment zeg je ook: 'nou jongens, er is nou wel lang genoeg getapt. Er komt helemaal niks uit, we stoppen ermee'. Hoe lang die termijn is, hangt van het onderzoek en de ernst van het feit af." - RC

Sommige taps lopen maar een week, maar er zijn ook taps die een half jaar lopen of soms nog wel langer. Aan de respondenten is gevraagd of het moeilijk is om een tap die al een tijdje loopt af te sluiten, gezien de investering die gedaan is door het team. Een aantal respondenten geeft aan dat dat best moeilijk kan zijn. De ervaring is dat de politie vaak door wil gaan, want "je weet maar nooit" en "hebben is hebben", aldus een politiefunctionaris. Een OvJ geeft aan dat het dan de rol van de OvJ is om betrokken distantie te bewaren en in te grijpen waar nodig. Deze respondent is van mening dat soms sneller een beslissing genomen moet worden om een tap te stoppen als blijkt dat een lijn na een dag of vier niets lijkt op te leveren. Een andere OvJ geeft aan het afsluiten van een tap ook niet zo moeilijk te vinden. De afwegingen of een tap wat oplevert tegenover de inbreuk die de tap maakt op de privacy, spelen continu een rol. Een OvJ zegt:

> "Het is niet zo dat ik denk: het maakt me allemaal geen biet uit. Ik bedoel je bent wel met mensen bezig. Je moet proportioneel zijn natuurlijk." - OvJ

Een RC merkt op dat er ook OvJ's zijn die soms langer willen doorgaan met tappen dan nodig is. Dit bemerkt deze respondent zeker in grote onderzoeken waarvoor genoeg geld en 'poppetjes' beschikbaar zijn. In zo'n situatie wordt de rol als RC en de positie van de OvJ in het opsporingsonderzoek nog eens extra benadrukt voor deze respondent.

"Ik heb ook wel eens een onderzoek gehad waarbij er drie maanden lang getapt is op basis van een CIE-tip dat bepaalde jongens zich bezig zouden houden met de handel van precursoren. Op een gegeven moment hadden we 5 mensen onder de tap, 2 maanden lang. Dan krijg je steeds weer die verlengingen. Er wordt wel gesproken over "ik zie je zo, kun je nog even bij me langskomen", en op een gegeven moment vroeg ik aan de OvJ hoe staan jullie ervoor in de rest van dit onderzoek, wordt er bijvoorbeeld ook geobserveerd, hoe lang willen jullie dit nog laten doorlopen want volgens mij gebeurt er niet zoveel. Toen was het ook ineens zo dat door personeelsgebrek zijn er op dit moment maar twee rechercheurs die eigenlijk alleen maar de taps uitluisteren. Toen heb ik gezegd binnen twee dagen laat je me weten of dit nog een serieus onderzoek gaat worden en of we hiermee nog wat gaan bereiken, want twee rechercheurs in een tapkamer daar los je geen leveringen mee op. Toen ik na twee dagen niks had gehoord heb ik gezegd dan ga ik de boel niet meer verlengen." - RC

6.12 Opbrengsten

De doelstellingen om te gaan tappen zijn *sturing* en *bewijs.* Maar ook het *traceren* van personen kan een reden zijn om een tap aan te sluiten. Maar worden deze doelstellingen ook behaald? Met andere woorden: wat zijn de opbrengsten van de tap?
Uit eerder onderzoek (Reijne et al., 1996) blijkt dat de telefoontap het meeste bijdraagt aan het opsporen van nieuwe informatie door sturing van het team. Met informatie die voortkomt uit de telefoontap wordt bijvoorbeeld het observatieteam aangestuurd. Bewijsgaring is hiervan meestal een indirect gevolg. Ook wordt informatie uit de tap gebruikt om netwerken in kaart te brengen. Wel zagen zij dat de bijdrage, dus de opbrengst, van de tap verschilt per delictsoort. Tappen bij voortdurende criminaliteit zoals drugshandel, heling en milieudelicten levert met name opsporingsinformatie op, terwijl tappen bij ernstige tegen personen gerichte delicten vaker bewijs oplevert omdat het hier vaker om gelegenheidscriminelen zou gaan. De vraag is of er in de loop der tijd veranderingen zijn opgetreden in de opbrengsten van de tap. Daar gaan we hieronder op in.

6.12.1 Bewijs

Veel respondenten geven aan dat de telefoontap weinig direct bewijs oplevert. Er wordt veel gesproken maar weinig inhoudelijks gezegd.

"Er zijn weinig gesprekken waarin gezegd wordt: 'kun je mij 17 kilo heroïne leveren voor 20.000 euro per kilo?' en dan wordt er ja gezegd. Dat zie je echt niet." - RC

Er wordt veelal in versluierd taalgebruik gesproken over de telefoon (zie ook Kleemans et al. 1998, p. 114-115; Kleemans et al., 2002, p. 89), wat wel een indicatie kan geven dat men in de goede richting zit maar wat op zichzelf niet voldoende is om zonder steunbewijs als bewijs gebruikt te worden. De inhoud van deze gesprekken is vaak alleen te begrijpen in combinatie met ander bewijsmateriaal. Tapgesprekken leveren voornamelijk indirect bewijs op, ondersteunend aan ander bewijsmateriaal. Het is een 'stukje van de puzzel'.
Bij zogenaamde 'zwakke schakels' daarentegen, personen die zich niet bewust zijn dat ze getapt kunnen worden zoals ouders of vriendinnen van de verdachte, levert de tap nog wel eens bewijs op. Dat kan een reden zijn om juist de omgeving van de verdachte te gaan tappen en niet de verdachte zelf.

6.12.2 Sturing

Informatie die uit de telefoontap naar voren komt, kan worden gebruikt om de richting van het onderzoek te kunnen bepalen. Dit wordt ook wel sturingsinformatie genoemd. Hiervoor blijkt de tap een nuttig middel te zijn. De tap verschaft inzicht in het levenspatroon van

degene die wordt getapt: wat doet hij, met wie heeft hij contact, hoe beweegt hij zich? Via de tap hoort het rechercheteam bijvoorbeeld waar de verdachte afgesproken heeft, en kan zo het observatieteam gericht aansturen. Indien wenselijk kan men bepaalde contacten van een verdachte ook in het opsporingsonderzoek betrekken. Een respondent zegt:

> "De waarde van de telefoontap zit grotendeels in sturing van het onderzoek." - OvJ

Een mobiele telefoon wordt in de opsporing ook gebruikt om geografische bewegingen in kaart te brengen. Verkeersgegevens van de tap laten zien via welke telefoonpaal contact is gemaakt met het netwerk. Locaties van een getapte persoon kunnen zo in beeld worden gebracht. Of men hoort in een tap dat de verdachte communiceert via internet, wat een aanleiding kan zijn om een internettap te plaatsen. Een respondent vindt het tappen om sturingsinformatie te krijgen typisch iets voor zijn regio. Hij zegt hierover:

> "Wij in [regio A] gebruiken van nature een tap om sturingsinformatie te krijgen. Dat is zo ooit gegroeid al rechercherend in [regio A]. Terwijl andere regio's hem krijgen ter bevestiging van hun sturingsinformatie. Met andere woorden: wij tappen ons een versuffing. Krijgen daar heel veel informatie uit en sturen dan ons onderzoek daar op. En in andere grote regio's (…), daar heeft men al informatie en om die informatie te veredelen gaat men pas tappen." - politie

6.12.3 Traceren

Respondenten geven aan dat de waarde van de telefoontap niet zozeer zit in bewijsgaring, maar steeds meer in traceren van verdachte en gezochte personen. De tap blijkt bijvoorbeeld ook nuttig om bewegingen van een persoon vast te leggen, zowel door de inhoud van gesprekken als door verkeersgegevens van de gesprekken. Daarmee wordt de tap dus ook een instrument waarmee de gangen van een getapte persoon kunnen worden gevolgd. Men kan bijvoorbeeld door middel van een tap de locatie achterhalen van een voortvluchtige verdachte, indien hij gebruik maakt van zijn afgetapte telefoon. Wanneer hij wel de afgetapte telefoon bij zich heeft maar niet actief gebruikt, kan een opsporingsteam gebruik maken van een stealth-sms. Een stealth-sms kan ook worden ingezet wanneer een arrestatieteam de locatie van een verdachte wil verifiëren voordat ze op een locatie naar binnen gaat om de verdachte aan het houden.

6.12.4 Restinformatie

Naast informatie die voor het onderzoek van belang is, levert de tap vaak ook informatie over andere delicten op. In dit soort gevallen geldt soms het doorlaatverbod (artikel 126ff Sv) dat voorschrijft dat een opsporingsambtenaar die door uitvoering van een bijzondere opsporingsmethode op de hoogte raakt van de vindplaats van een verboden voorwerp, verplicht is deze in beslag te nemen. Inbeslagname mag alleen worden uitgesteld in het belang van het onderzoek met het oogmerk daartoe later over te gaan. Uit de interviews blijkt dat men op verschillende manieren omgaat met restinformatie uit de tap. Hoe men ermee omgaat, is afhankelijk van de ernst van het delict, de capaciteit van het rechercheteam en het belang van het eigenlijke onderzoek.
Als de informatie van bepaalde ernst is, zal erop gereageerd moeten worden. Zo kan het bijvoorbeeld voorkomen dat men bezig is met een onderzoek naar drugshandel en men er via de tap achter komt dat de verdachte ook in wapens handelt.

> "Er gebeurden allemaal rare dingen op de tap, verdachte heeft een pistool. Ik ben naar het bureau gereden en heb geluisterd en dan hoor je haar ook heel trots met iemand bellen en moet je horen en dan hoor je het vuurwapen doorladen en het magazijn. En ik denk, nou moet ik ingrijpen, maar dat wil ik niet want ik wil eerst die andere boef hebben. Dan maak je een kluisverbaal. Dat houdt in dat je af gaat schermen. Het andere team gaat dan

ingrijpen om het spul aan te houden. Ze zijn ook aangehouden, bleek zo'n balletjespistool uit Spanje te zijn maar wel levensecht om te zien. [...] Er zijn momenten dat je harde informatie hebt waarop je moet ingrijpen. Kan niet anders. Uiteindelijk is het spul weer heengezonden na een nachtje zitten en konden wij gewoon weer verder met onze zaak." - politie

Wat door respondenten als een ernstig delict wordt beschouwd kan verschillen per regio. Zo kan men in een kleine regio het de moeite waard vinden om door te rechercheren op 'onsjes', maar een respondent uit regio A zegt dat zij dat een peulenschil vinden en dat zij bij dat soort informatie de vingers in de oren stoppen. Behalve als er letterlijk wordt gesproken over cocaïne en heroïne, dan moet er wel worden ingegrepen.
Naast de ernst van het delict speelt ook capaciteit een rol bij het omgaan met restinformatie. Indien er informatie binnenkomt over andere delicten, kan het rechercheteam besluiten er zelf onderzoek naar te doen. Het gevaar bestaat dat men het eigenlijke onderzoek (de hoofdweg) uit het oog verliest en alleen maar bezig is met de andere strafbare feiten die voorbij komen, waardoor het onderzoek 'uit de bocht vliegt'. Dit uit de bocht vliegen komt vaker voor bij projectmatige onderzoeken dan bij TGO's, aldus een respondent, waar men de doelstelling strakker voor ogen houdt.
Wanneer men krap in de capaciteit zit, kan de informatie worden weggezet bij een ander team. Er wordt dan een proces-verbaal opgemaakt, waarin staat dat 'uit lopend onderzoek is gebleken dat…'. Het andere team zorgt er voor dat ze inspringen op de informatie die er ligt, zonder dat het schadelijk is voor het eigenlijke onderzoek. Sommige teams moeten in verband met het gebrek aan capaciteit altijd restinformatie wegzetten. Zo geeft een wijkteam aan dat zij beseffen dat ze zich moeten concentreren op hetgeen ze tot doelstelling hebben omdat het onderzoek anders te groot wordt en ze het op hun niveau niet meer kunnen behappen.

"Je moet jezelf beschermen om niet te enthousiast te worden. We rechercheren in Nederland erg graag in de breedte." - politie

Een andere optie is om na sluiting van een onderzoek restinformatie aan de afdeling analyse te geven, die vervolgens het materiaal analyseert op mogelijke misdrijven waar een verdachte of een groep van verdachten zich nog meer mee bezighoudt. Dit kan uiteraard alleen in die gevallen waar het doorlaatverbod (artikel 126ff Sv) niet voor geldt.
Het belang van het eigenlijke onderzoek speelt ook een rol. Wanneer er restinformatie binnenkomt dat ernstiger is dan het misdrijf waar het eigenlijke onderzoek zich op richt, kan men ervoor kiezen om door te rechercheren op de restinformatie.

6.13 Geliefd en waardevol?

Bij aanvang van dit onderzoek was één van de ideeën dat de tap achterhaald zou zijn en steeds minder op zou leveren omdat verdachten zich ervan bewust zijn dat hun telefoons afgetapt kunnen worden. Daarnaast bestaan er al enige tijd alternatieve communicatievormen en encrypted telefoons waarmee een tap eenvoudig kan worden omzeild. Maar deze ideeën zijn in dit onderzoek slechts ten dele bevestigd. Vooral de opsporingscapaciteit die met het tappen gepaard gaat, wordt vaak genoemd als groot negatief punt. Maar ook andere negatieve punten van de tap zijn tijdens de gesprekken naar voren gebracht;

"Als je in de tunnel van tappen zit, is het heel lastig om eruit te komen." – politie
"Een tap kost gewoon gigantisch veel capaciteit, en de capaciteit is schaars." – politie
"Het zit met name in die taps die worden aangesloten voor bewijs. Dat levert heel weinig op in principe." – politie

"Je kan een hele hoop informatie om het delict heen met de tap naar boven halen, maar waar het daadwerkelijk om gaat komt er haast niet uit." – politie
"Er zit wel af en toe een interessant gesprek tussen maar het oninteressante wat er tussen zit is zoveel, we kunnen het niet meer uitwerken." - FIOD

Echter, de onderzoeksresultaten wijzen uit dat ondanks de negatieve aspecten de telefoontap nog steeds heel waardevol wordt gevonden en een tap voor de respondenten eigenlijk altijd wel wat oplevert.

"echt een onmisbaar middel" - politie
"tappen nog steeds effectief" - politie
"tappen is een sterk middel" - OvJ
"wij tappen veel, maar er komt ook veel uit" - politie
"het is op dit moment nog een heel waardevol middel" - PIDS
"een tap heeft altijd zin" - OvJ
"die tap is voor ons cruciaal" - politie
"op het moment dat we niet tappen, merk je gewoon dat je heel veel mist" - OvJ
"(…) het valt me iedere keer weer op dat ook in ZwaCri onderzoeken we heel veel meekrijgen over de telefoon" - OvJ
"de tap is geen heilig middel, maar wel een heel goed hulpmiddel. En in een aantal gevallen een goed bewijsmiddel" - politie
"het levert eigenlijk altijd wel wat op" - politie

Deze positieve uitspraken zijn gebaseerd op de ervaringen van respondenten en de informatie die wordt verkregen met de telefoontap. Het is natuurlijk onduidelijk hoeveel en wat voor informatie niet wordt opgevangen met een tap. Daar is geen zicht op. Sommige respondenten geven wel aan dat ze merken dat niet alle communicatie wordt afgevangen. Daarnaast stelt een aantal respondenten zichzelf de vraag of het tappen voldoende rendement oplevert gezien de grote investering die gedaan moet worden in tijd en mankracht.

6.14 Wat beïnvloedt de opbrengst?

Twintig jaar geleden was de telefoontap een uniek middel en werd er nog openlijk gesproken over de telefoon en leverde het bewijs op. Tegenwoordig raakt men steeds meer doordrongen van het feit dat de politie telefoons kan afluisteren en dat je niet moet praten over de telefoon. Er moet steeds meer moeite worden gedaan om hetzelfde resultaat met de tap te halen als twintig jaar geleden. Een respondent omschrijft dit als de 'aardolie-metafoor': er moet steeds dieper worden geboord om dezelfde hoeveelheid olie uit de grond te krijgen als twintig jaar geleden. Zo is het ook met de tap vandaag de dag, aldus deze respondent.

"Twintig jaar geleden als je een tap aansloot dan kwam alle informatie er tegelijk uit, je wist met wie die belde, er kwam informatie over. Nou de criminelen zijn tegenwoordig veel gehaaider, dus veel meer versluierd (…) het scala van communicatie is veel breder. Dus wat zie je nou, net als met aardolie, moet je veel dieper, veel intensiever, veel meer moeite ervoor doen en dus ook veel breder je tapnetwerk uitbouwen om toch iets van dezelfde informatie boven water te krijgen als twintig jaar geleden." - politie

Toch zien we dat de telefoontap nog steeds resultaat oplevert. De opbrengst van het tappen is sterk afhankelijk van meerdere factoren: het gepleegde of te plegen feit, de doelgroep waartoe de verdachte behoort, of er al dan niet reuring wordt veroorzaakt, of er een analist

betrokken is bij het onderzoek, het afnemend gebruik van spraaktelefonie en ook gewoon van het toeval.

Of de tap iets oplevert is afhankelijk van de *doelgroep* waarbinnen wordt getapt. Volgens respondenten wordt er door verdachten van zwaardere misdrijven altijd wel versluierd gesproken over de telefoon, maar hoe gedisciplineerd dat gebeurt, is afhankelijk van de doelgroep waar men zich op richt. Beginnelingen zijn zich vaak nog niet zo bewust van het feit dat ze kunnen worden afgetapt. Codetaal wordt vaak niet consequent gebruikt waardoor er altijd fouten in het voordeel van de politie worden gemaakt. Daardoor levert de tap bewijstechnisch nog wel iets op.
Bij doorgewinterde criminelen daarentegen, levert de tap vaak bewijstechnisch niet veel op. Men is zich bewust van wat de politie aan opsporingsmogelijkheden heeft en probeert daarop in te spelen. Met de tap kan hooguit indirect bewijs worden verkregen. Wel levert het opsporings- of sturingsinformatie op. Op zwacri-niveau zien respondenten dat bepaalde verdachten heel erg gedisciplineerd zijn in het gebruik van hun telefoon. Ze maken alleen gebruik van prepaid SIM-kaarten, die regelmatig worden vervangen. Inhoudelijk wordt er niets besproken over de telefoon, er worden alleen afspraken gemaakt om elkaar te ontmoeten. Er wordt gebruik gemaakt van één-op-één lijnen, zogenaamde gesloten circuits, die enkel worden gebruikt tussen twee personen. Ook worden SIM-kaarten en batterij uit de telefoons gehaald, zodat geen locatie kan worden gevonden. Zo zegt een respondent:

> "Ik heb een zaak waarbij bij iemand thuis 150 verschillende telefoons en 380 SIM-kaarten zijn gevonden. Aan iedereen met wie hij sprak gaf hij zelf een telefoon, alleen met die telefoon op dat nummer mocht met hem gebeld worden. Hij had dus ook voor iedereen een andere telefoon om mee te bellen. En het zijn allemaal prepaid kaartjes." - RC

Binnen bepaalde kringen wordt ook gebruik gemaakt van communicatie die verloopt via internet zoals Whatsapp, Ping, social media en via telecommunicatiediensten op internet zoals Skype. Om dat te kunnen onderscheppen is een internettap nodig, maar inhoudelijk meeluisteren of meekijken is niet altijd mogelijk door versleuteling van de data. Communicatie kan hierdoor technisch niet zichtbaar gemaakt worden. Het gebruik van een internettap blijkt tevens voor veel respondenten een obstakel, doordat het interpreteren van afgetapte internetgegevens specialistische kennis vereist die niet bij alle rechercheteams aanwezig is. In hoofdstuk 7 gaan we hier verder op in.
De opbrengst van de tap is niet alleen afhankelijk van de doelgroep waar men zich op richt, ook het soort *misdrijf* bepaalt wat de tap aan informatie oplevert. Wanneer sprake is van misdrijven die nog moeten plaatsvinden, denk aan een drugtransport, dan is de kans dat er communicatie moet plaatsvinden om het misdrijf te kunnen plegen groot. Men moet contact met elkaar hebben over de levering en betaling, de locatie ervan, etc. Vaak zijn dit internationale contacten die veelal via de telefoon plaatsvinden. Bij mensenhandel, wat een voortdurend misdrijf is, levert de tap bewijstechnisch altijd wel wat op. Bij mensenhandel worden de vrouwen continue telefonisch onder controle gehouden of onder druk gezet, omdat fysieke aanwezigheid van de pooier in het prostitutiegebied teveel zou opvallen (zie ook Verhoeven et al, 2011).
Bij misdrijven die al hebben plaatsgevonden, denk aan een moord, is de kans op communicatie over het misdrijf een stuk kleiner, behalve als het misdrijf met meerdere personen is gepleegd (Zie hierover ook De Poot, et al., 2004; Bokhorst, 2004). Een manier om de opbrengst van de tap te vergroten is door het *veroorzaken van reuring*, ook wel 'ruis op de lijn' genoemd (zie ook De Poot et al., 2004, p. 167). Zeker als een misdrijf al een tijd geleden heeft plaatsgevonden wordt er door betrokkenen niet zomaar uit het niets over gesproken.

> "Een nare gebeurtenis ga je wegzetten. En pas als je eraan herinnerd wordt ga je met een vriend bellen 'wat er nu gebeurt, ze hadden het er weer over'." – politie

Volgens respondenten kan de opbrengst van de tap worden vergroot door een *analist* aan het opsporingsteam te verbinden. Analisten kunnen tijdens het opsporingsonderzoek van waarde zijn omdat ze de informatie uit de tap systematisch kunnen koppelen aan informatie die voortvloeit uit andere opsporingsmiddelen. Daarnaast kunnen analisten worden ingezet om na afloop van het onderzoek een groep verdachten in kaart te brengen door middel van de informatie die uit de tap naar voren is gekomen.[27] Doordat ook operationele analysecapaciteit schaars is, wordt de informatie die door middel van de tap wordt opgespoord niet in alle zaken systematisch in kaart gebracht.
Wat een steeds grotere invloed op de opbrengst van de telefoontap zal gaan hebben, is de *veranderde manier van communiceren*. Zoals we in hoofdstuk 2 van dit rapport al aangaven, wordt er steeds vaker gecommuniceerd door middel van tekst in plaats van spraak. Door de komst van de smartphones wordt meer en meer gebruik gemaakt van communicatie via het internet, zoals Ping, Whatsapp en WLM. Deze vormen van communicatie worden met een 'gewone' telefoontap gemist, en zouden dus feitelijk met een datatap moeten worden afgevangen.
Uiteindelijk is de opbrengst van de tap, net als de opbrengst van andere opsporingsmiddelen, zeker ook afhankelijk van *toeval*. Meerdere respondenten wijzen erop dat men het moet hebben van fouten die verdachten maken in hun telefoondiscipline.

> "En sommige jongens realiseren zich natuurlijk wel dat ze over de telefoon niets moeten zeggen. Het is net als met te hard rijden, je let er altijd op, zeker op ring Rotterdam ofzo, dan zit je met je gedachten ergens anders en word je toch een keer geflitst. Zo is het met die jongens ook natuurlijk." – RC

6.15 Stealth-sms

Wanneer iemand een sms-bericht ontvangt of verstuurt, wordt door de mobiele telefoon contact gemaakt met een zendmast. Opsporingsdiensten kunnen hiervan gebruik maken om een telefoon mee te lokaliseren. Het lokaliseren van een mobiele telefoon kan normaliter alleen als de telefoon wordt gebruikt. Door het zenden van een *stealth-sms*, een 'stille sms' hoeft niet te worden gewacht totdat de gebruiker van de telefoon zelf belt of een bericht verstuurt (zie paragraaf 6.2.1).
In de jurisprudentie omtrent de inzet van stealth-sms is nog geen vaste lijn te ontdekken. Zo oordeelt de Rechtbank Amsterdam dat artikel 2 Pw genoeg rechtsgrond biedt voor inzet van stealth-sms, zolang er met het opsporingsmiddel slechts in beperkte mate inbreuk wordt gemaakt op het recht van de verdachte op eerbiediging van zijn persoonlijke levenssfeer. In deze zaak werd al gebruik gemaakt van de tap en de extra inbreuk op de privacy die wordt veroorzaakt door stealth-sms is daarom marginaal te noemen, aldus de rechtbank (Rechtbank Amsterdam, 08 maart 2011, *LJN* BP7233). Hiermee lijkt de rechtbank aan te geven dat het toestaan van stealth-sms en de rechtsgrond ervan dus casusafhankelijk is en er gekeken dient te worden naar de mate van inbreuk dat het gebruik van stealth-sms maakt op het recht van de verdachte op eerbiediging van zijn persoonlijke levenssfeer.
In een andere zaak werd eveneens gebruik gemaakt van stealth-sms. Diezelfde rechtbank oordeelde in deze zaak dat indien er al een vordering verstrekking verkeersgegevens (artikel 126n Sv) of opnemen telecommunicatie (artikel 126m Sv) is gedaan, het niet valt in te zien dat deze bevoegdheden alleen kunnen worden ingezet voor het passief kennis nemen van telecomgegevens (Rechtbank Amsterdam, 31 mei 2011, *LJN* BQ9049). Daarmee lijkt de Rechtbank Amsterdam aan te geven dat stealth-sms op basis van artikel 126n Sv en/of artikel 126m Sv ingezet kan worden.
Ondanks het feit dat er een bevel verstrekking verkeersgegevens of een tapbevel ligt, kan de politie stealth-sms niet zomaar inzetten. De OvJ moet er toestemming voor geven. Een respondent zegt hierover;

[27] Zie ook Bloem & Aarts, 2000, p. 136-137, voor meer informatie over de meerwaarde van een goede analyse van gegevens die uit de tap naar voren komen.

> "Het valt niet onder je tapbevel, wij hebben het met de officier zodanig afgedekt dat wij dat in mogen zetten" - politie

Veel respondenten geven aan regelmatig gebruik te maken van dit opsporingsmiddel. Een aantal respondenten vertelt dat ze het een prettig middel vinden om mee te werken;

> "Het is een prachtig middel. Anders moet je wachten tot je verdachte een keer gaat bellen." - politie

Een stealth-sms wordt vlak voor een aanhouding ingezet om de locatie van de verdachte op het laatste moment nog even te controleren. Dit om te voorkomen dat een arrestatieteam op een verkeerde plek naar binnen gaat. Een respondent vertelt dat door de inzet van stealth-sms een overval is voorkomen. Via de telefoontap waren de plannen van de overvaller en het vertrekpunt duidelijk. Niet het doel, daarvan had men slechts een vermoeden:

> "…we wisten niet waar ze naar toe gingen. We zagen dat er iets ging gebeuren. We hadden met de officier uitgemaakt, dat wanneer ze binnen een straal van zoveel kilometer bij die plek zouden komen het dan kassa zou zijn voor ons. We hebben op dat moment een stealth-sms uitgedaan om te kijken waar hij was." – politie

Het actief kennis nemen van verkeersgegevens biedt de opsporing dus nieuwe mogelijkheden voor de locatiebepaling van personen en wordt als zodanig door de rechter geaccepteerd.

6.16 IMSI-catcher

Wanneer het opsporingsteam de indruk heeft dat een verdachte wel veel belt maar zij de gesprekken mist omdat ze dat telefoonnummer niet onder de tap hebben, dan kan het opsporingsteam door middel van de International Mobile Subscriber Identity (IMSI)-catcher proberen het telefoonnummer te achterhalen. Een IMSI-catcher is een apparaat dat, door zich voor te doen als een zendmast, in staat is om alle telefoongesprekken in de omgeving van die IMSI-catcher op te vangen. Het is de OvJ die inzet van de IMSI-catcher beveelt. Het bevel kan gegeven worden voor een week. Daarna zal moeten worden bezien of er een nieuw bevel kan worden verstrekt. De IMSI-catcher mag, blijkens artikel 126nb/126ub Sv, enkel worden ingezet om de toepassing van het vorderen van verkeersgegevens (artikel 126 n/126u Sv) of het opnemen van telecommunicatie (artikel 126m/126t Sv) mogelijk te maken (Nieuwenhuis, 2007, p. 53-54). Daarmee lijkt het niet toegestaan om de IMSI-catcher enkel in te zetten om de locatie van een telefoon te achterhalen. Echter, in artikel 3.10 Tw is wel een zelfstandige bevoegdheid opgenomen om de IMSI-catcher in te zetten om de locatie van een mobiele telefoon te achterhalen. Dit mag enkel worden gedaan indien het noodzakelijk is ter voorkoming, beëindiging of opsporing van een misdrijf als omschreven in artikel 67 lid 1 Sv, dat gezien zijn aard of samenhang met andere strafbare feiten een ernstige inbreuk op de rechtsorde oplevert (sub a); ter vaststelling van de verblijfplaats van een aan te houden persoon (sub b); ter vaststelling van de plaats waar zich een persoon bevindt van wie moet worden gevreesd dat deze in acuut levensgevaar verkeert of ter beëindiging van een zodanig acuut levensgevaar (sub c); of ten behoeve van oefendoeleinden.[28]

[28] In een zaak (waarin sprake was van diefstal van diamanten en edelstenen ter waarde van ruim 1,5 miljoen euro exclusief btw) die speelde voor het Hof Arnhem werd met behulp van de IMSI-catcher de locatie achterhaald van een mobiele telefoon. Het hof oordeelde dat bij kortstondige, niet-stelselmatige inzet van de IMSI-catcher, artikel 2 Pw voldoende rechtsgrond biedt voor inzet ervan (Hof Arnhem, 24-01-2012, *LJN* BV3076). In deze zaak werd de IMSI-catcher ingezet om de locatie te achterhalen van de mobiele telefoon, een daarmee hopelijk van de verdachten en de buit. Er lijkt

Om het telefoonnummer te achterhalen dient de verdachte geobserveerd te worden en dient men met de IMSI-catcher achter de verdachte aan te rijden om op verschillende locaties een zendmast over te nemen. Als men dit drie keer doet, kunnen deze databases worden vergeleken en zal waarschijnlijk één telefoonnummer op alle drie de locaties voorkomen. Dit is dan hoogstwaarschijnlijk het telefoonnummer van de verdachte. Een respondent vertelt hierover:

> "Als je geen telefoonnummer hebt van de verdachte, dan gaan we met een IMSI-catcher rijden. Dat gebeurt regelmatig. Maar dan moeten we aanwijzingen hebben dat ie meerdere telefoons heeft. De OT's beschikken bijna allemaal wel over een IMSI-catcher. Die zijn redelijk succesvol en zo halen we de nieuwe telefoonnummers binnen." - politie

Een andere respondent geeft aan dat de IMSI-catcher steeds vaker wordt ingezet. Niet elk team heeft echter de beschikking over een IMSI-catcher. Een wijkteam uit regio A zegt dat zij er niet de beschikking over hebben omdat zij zich met zogenaamde 'kleine' criminaliteit bezighouden.

6.17 Geheimhouders

Informatie uit gesprekken met personen die vallen onder het verschoningsrecht mogen niet in het opsporingsproces terecht komen. In het verleden is dat wel gebeurd en naar aanleiding daarvan zijn maatregelen getroffen om dit in de toekomst te voorkomen. Dit is het, zoals in paragraaf 3.5 besproken, systeem van nummerherkenning. Vanaf 15 mei 2011 konden alle advocaten de zakelijke telefoon- en faxnummers registreren. Navraag begin januari 2012 leert dat het nummerherkenningsysteem officieel in werking is getreden maar in de praktijk nog niet optimaal functioneert. Dit heeft te maken met het feit dat nog niet alle advocaten zich hebben kunnen registreren in het nieuwe systeem door een registratieprobleem. Wanneer dit probleem is opgelost is nog onduidelijk. Alhoewel het systeem van nummerherkenning is ingevoerd, zal de 'oude' werkwijze[29] omtrent geheimhoudersgesprekken nog moeten worden nageleefd. Het is namelijk niet uitgesloten dat een advocaat gebruik maakt van een nummer dat (nog) niet in het systeem staat geregistreerd en daarnaast wordt het systeem op dit moment alleen gebruikt voor advocaten. Wellicht dat het in de toekomst uitgebreid kan worden naar andere beroepsgroepen waarvoor het verschoningsrecht geldt. De politie en het OM blijven, ook in de nieuwe situatie, verantwoordelijk voor het op een juiste manier vernietigen van geheimhoudergesprekken. Wanneer een gesprek met een geheimhouder die onder het nummerherkenningsysteem valt toch wordt gedetecteerd, dan moet dit onmiddellijk worden vernietigd (artikel 4a Besluit bewaren en vernietigen niet-gevoegde stukken). Respondenten is gevraagd hoe de procedure rondom het aftappen van geheimhoudersgesprekken verloopt. Ten tijde van de interviews, die zijn afgenomen voor augustus 2011, was de nieuwste Instructie vernietiging geïntercepteerde gesprekken met geheimhouders (OM, 2011) nog niet in werking getreden. De door de respondenten weergegeven situatieschets betreffende de verwerking van geheimhoudergesprekken moet dan ook in dit licht worden beoordeeld. In beide regio's lijkt hier verschillend mee om te worden gegaan. Respondenten in zowel regio A als B geven aan dat er speciaal aangewezen opsporingsambtenaren verantwoordelijk zijn voor het uitluisteren en verwerken van geheimhoudersgesprekken. Dit zijn rechercheurs die geen onderdeel uitmaken van het opsporingsteam dat belast is met de zaak waarvoor getapt wordt. Wanneer op de tapkamer een geheimhoudersgesprek wordt gesignaleerd, wordt dit gesprek stopgezet en in het systeem als geheimhouder gemarkeerd. Vervolgens wordt dit gesprek door de externe rechercheur uitgewerkt en doorgegeven aan de officier. Echter, andere respondenten in regio

dus geen eenduidigheid te bestaan over de rechtsgrond op basis waarvan de IMSI-catcher ter locatiebepaling ingezet kan worden.

[29] Instructie vernietiging geïntercepteerde gesprekken met geheimhouders

A en B geven aan dat de tapcoördinator in zijn 'eigen' onderzoek verantwoordelijk is voor de geheimhoudersgesprekken. Deze werkt de gesprekken uit en legt de uitgewerkte gesprekken voor aan de ovj. De teamleider wordt in beide gevallen alleen op de hoogte gesteld van het bestaan van het gesprek, maar niet van de inhoud. Vervolgens beoordeelt de officier de relevantie van het gesprek. Dit kan een officier zijn die buiten het onderzoek staat, maar ook de zaaksofficier zelf. De officier kan vervolgens zelf de keuze maken om het gesprek wel of niet te beluisteren. Het gesprek wordt meestal alleen beluisterd wanneer er twijfel bestaat over de 'geheimhouderstatus' van het gesprek.
Ondanks dat de zaaksofficieren aangeven de informatie die via deze weg tot hun komt te negeren, is het aan te bevelen om deze gesprekken door iemand van buiten het team te laten beluisteren. Uit wetenschappelijk onderzoek is bekend dat het is niet mogelijk is om informatie te elimineren of te isoleren nadat deze het geheugen is binnen gekomen. Dat betekent dat deze kennis onbewust een rol kan gaan spelen (zie Schacter, 2001).

> "Als officier word je gebeld door de tapcoördinator van 'er is een geheimhoudergesprek'. Ik vraag meestal wat is de geheimhouder, huisarts, advocaat. Dan hoef ik de inhoud van die gesprekken niet meer te horen. Dat is een keuze van mij als officier. Ik heb zoiets van, daar kan ik alleen maar last van hebben, dat hoef ik niet te weten." – OvJ

Bij de gesprekken kwam naar voren dat andere geheimhouders dan advocaten nogal eens over de lijnen komen. Bijvoorbeeld gesprekken met artsen voor het maken van afspraken of het bespreken van 'kwaaltjes'. Gesprekken tussen verdachten en zijn of haar advocaat met voor het onderzoek relevante informatie, komt nooit tot bijna nooit voor. De geïnterviewde advocaten bespreken bewust niet inhoudelijk over de zaak aan de telefoon met het oog op een mogelijke tap. Een advocaat zegt hierover:

> "Ik zeg het ook tegen m'n klanten 'als je iets wilt bespreken, kom maar naar kantoor of ik kom naar je toe in de bajes. Maar we gaan het niet telefonisch bespreken'." - advocaat

> "Ik praat nooit over de telefoon. Ik ga graag uit van de integriteit van de Nederlandse politie en het Openbaar Ministerie maar er zijn zaken die zo belangrijk kunnen zijn dat men gewoon ook tegen de regels in desnoods een advocaat zou willen tappen. Ik kan me dat voorstellen ook." - advocaat

Men hoopt op niet te lange termijn het nummerherkenningssysteem goed draaiend te hebben. Een argument dat wordt aangevoerd tegen het systeem is eventueel misbruik. De NOvA heeft tot dusver nog geen systeem ontwikkeld om de naleving te controleren. Wel probeert de NOvA het bewustzijn onder advocaten betreffende de naleving van de verordening te vergroten. In de nieuwe situatie ligt de verantwoordelijkheid voor het zorgvuldig omgaan met geheimhoudergesprekken bij de advocaat zelf.[30] Er is dan geen controle meer van buitenaf. Advocaten zouden in theorie de 'niet afluisterbare' telefoon aan hun cliënt kunnen uitlenen zodat deze ongestoord (crimineel beladen) telefoontjes kan plegen. Deze angst is door verschillende respondenten geuit. Een advocaat zegt hierover:

> "Ja, stel dat een cliënt bij mij op kantoor komt bellen om aan allerlei zaakjes te werken. Dat hangt dus ook af van de integriteit van de advocaat. (…) We hebben bepaalde privileges als advocaat, waaronder één van de belangrijkste is het verschoningsrecht. Dat moet je dus niet misbruiken. Ik kan me goed voorstellen dat daar met enig wantrouwen door politie en Openbaar Ministerie naar wordt gekeken. Ik denk ook dat de advocatuur aan haar stand verplicht is om als op enig moment duidelijk wordt dat er iets fout is, gewoon keihard op te treden. Dat soort mensen schaadt ook het aanzien van mijn vak en daarmee indirect mij dus." - advocaat

[30] Artikel 7, Verordening op de nummerherkenning

6.18 Privacy

Sinds de wetwijziging van 1 februari 2000 is tappen niet meer enkel voorbehouden aan communicatie waaraan de verdachte deelneemt. Ook betrokkenen, mensen die op één of andere manier in relatie staan tot de verdachte of mogelijk iets weten over het gepleegde misdrijf, kunnen worden getapt. Soms wordt een betrokkene, bijvoorbeeld de moeder van de verdachte, enkel getapt om het nummer van de verdachte te achterhalen. Dat tappen een inbreuk op de privacy oplevert is duidelijk. Maar in hoeverre is de privacy van degene die wordt getapt iets waar het opsporingsteam, de OvJ en de RC rekening mee houden? Maakt men onderscheid in het tappen van verdachten of betrokkenen? Houdt men rekening met de termijn waarbinnen wordt getapt? Hieronder wordt nader op deze vragen ingegaan.

6.18.1 Verdachte of betrokkene

De geïnterviewden zijn zich er terdege van bewust dat tappen een behoorlijke inbreuk maakt op de privacy van personen. Het besluit om de tap in te zetten is steeds een afweging van belangen die spelen en de te verwachten resultaten. Eén van die belangen is het recht op privacy dat regelmatig conflicteert met het belang van waarheidsvinding. Een RC uit regio A zegt hierover:

> "Je blijft die afweging maken: welke belangen zijn er in het spel? Op het moment dat je van de hoofdverdachte zijn nummer kwijt bent en je wilt een maand zijn moeder tappen, want iedereen belt zijn moeder, dan zit je met de privacy van die moeder die geen verdachte is en misschien niet eens weet wat haar zoon uitspookt. Op dat moment is dat privacybelang veel groter dan als je een gestolen telefoon wilt gaan tappen. Dan kun je zeggen we doen dat niet, ga het maar op een andere manier uitzoeken, maar ja, het is best lastig om bij prepaidtelefoons erachter te komen wie van welk nummer gebruik maakt. Wat je dan vaak kan doen, is dat je die periode waarin getapt mag worden ernstig bekort, dat je zegt een week of drie dagen. Als hij dan niet belt is het jammer." - RC

Aan het privacybelang van betrokkenen wordt door de meeste respondenten meer waarde gehecht dan het privacybelang van verdachten. Wanneer uit feiten en omstandigheden een redelijk vermoeden van schuld is ontstaan dat een persoon betrokken is bij een gepleegd of een nog te plegen misdrijf, dan heeft men er minder moeite mee om deze persoon te gaan tappen. Meer gereserveerd is men met het aanvragen of aansluiten van een tap op betrokkenen, zoals familie, vrienden en buren die mogelijk niets met het misdrijf te maken hebben. Zo zegt een politiefunctionaris uit regio A:

> "Wij willen niet de privacy schenden van de eerzame burger, maar dat we de privacy schenden van de boef, dat maakt ons echt niet uit." - politie

Als de te tappen persoon een betrokkene is, geven de OvJ's en de RC's aan de lat hoger te leggen. Het opsporingsteam moet dan nog beter motiveren waarom ze deze betrokkene willen gaan tappen en wat het voor het onderzoek kan opleveren. Een andere manier om de inbreuk op de privacy van betrokkenen te minimaliseren, is de termijn waarbinnen getapt mag worden kort te houden. De maximale termijn waarvoor een tapbevel kan worden afgegeven is vier weken. De meeste respondenten geven echter aan dat ze in geval van betrokkenen de tap voor slechts één of twee weken aanvragen (politie/OvJ) en afgeven (RC). In sommige gevallen betreft het slechts een paar dagen.
Een respondent benadrukt dat betrokkenen soms veel belangrijker kunnen zijn dan verdachten. Het zijn, volgens deze respondent, vaak mensen die profiteren van het strafbare feit. Ook kunnen ze belangrijker zijn omdat ze minder bedacht zijn op het feit dat ze getapt kunnen worden. Verdachten met een criminele achtergrond zouden eerder op hun hoede zijn (zie ook Bokhorst, 2004, p. 88). De afweging om een betrokkene te tappen is dus afhankelijk van het te verwachten resultaat:

> "Je kijkt natuurlijk heel erg naar wat ga je ervan verwachten? Dat is eigenlijk het criterium wat je hebt. En als een betrokkene heel dicht tegen een verdachte aan zit, dan zal het mij een worst zijn dat het een betrokkene is, dan tap ik hem even lief als de verdachte. Het gaat meer om het resultaat wat je wilt behalen dan of iemand toevallig betrokken is in zo'n zaak." – OvJ

6.18.2 Mate van inbreuk

Dat de telefoontap een inbreuk maakt op de privacy staat dus volgens de respondenten wel vast. Maar hoe wegen de respondenten de inbreuk op de privacy die andere opsporingsmiddelen maken ten opzichte van de telefoontap? Een respondent zegt hierover:

> "We tappen veel omdat we in Nederland vinden dat de inbreuk op de privacy minder is dan met het gebruik van andere middelen. Terwijl men in het buitenland daar precies andersom over denkt. Ik ben het daar niet mee eens. Bij een vaste lijn is de kans wel aanwezig dat je een ander gezinslid dan de verdachte over de lijn krijgt, maar bij mobiele telefonie is die kans heel klein. Daar maakt alleen de verdachte zelf gebruik van meestal. Bij internet ligt dat anders, dan tap je de hele familie. Er zit dus onderscheid in, terwijl de wet dit onderscheid niet maakt." - politie

Bij de inzet van ieder opsporingsmiddel zou nagedacht moeten worden of de inzet ervan gepast is, aldus een respondent. Wat gepast is, is blijkbaar cultureel bepaald en verschilt per land. Het voordeel van tappen is, zo legt deze respondent uit, dat je geen invloed hebt op wat iemand zegt of doet aan de telefoon. Dit is anders bij bijvoorbeeld infiltratie, een opsporingsmiddel wat in de VS veel wordt ingezet. In geval van infiltratie moet je als politie contact leggen met de verdachte en is de kans op beïnvloeding van de verdachte aanwezig. Respondenten zeggen zorgvuldig om te gaan met de tap. De tap wordt alleen ingezet wanneer men er resultaat van verwacht. Daarom vraagt een respondent zich af of tappen wel zo'n grote inbreuk op de privacy is.

> "Op de manier zoals wij het gebruiken he? Als iemand er niks mee te maken blijkt te hebben, gaat ie er ook meteen af. Ik ga toch niet luisteren naar iemand die niet met mijn zaak van doen heeft? En daarbij het interesseert me ook niet. We worden doodziek van die gesprekken!" - politie

Een respondent uit de advocatuur zegt de telefoontap wél een heel vergaande privacyschending te vinden. Dit omdat er naast de gesprekken die mogelijk voor justitie interessant zijn, over veel meer onderwerpen gesproken wordt.
Als men de inzet van de telefoontap vergelijkt met de inzet van de internettap zijn de meningen verdeeld over welk opsporingsmiddel meer inbreuk maakt op de privacy. De één zegt dat het surfen naar websites via internet of het incidenteel sturen van e-mails minder persoonlijk van aard is dan een telefoontap. Een andere respondent vindt de inbreuk die een telefoontap en een internettap maken op de persoonlijke levenssfeer redelijk gelijkwaardig. Weer een andere respondent is van mening dat de internettap meer inbreuk op de privacy maakt dan de telefoontap omdat je met een internettap vaak de hele familie tapt. Een telefoontap wordt vaak op een mobiele telefoon geplaatst die maar door één persoon wordt gebruikt. Ook vergelijkt een respondent het gebruik van internet met het gebruik van een dagboek. Je tikt soms dingen in op de computer die je met niemand anders deelt. Een advocaat zegt hierover:

> "Het tappen van internetgedrag is natuurlijk ook heel privé. Ik weet niet wat voor rotzooi je op internet hebt, van politieke aard tot seks, drugs en alles. Als de overheid het allemaal ongebreideld kan volgen en monitoren en opslaan, dan krijg je toch een beeld van een individu dat raakt aan de meest wezenlijke kern van de privacy." - advocaat

Het gebruik van internet en bellen vloeit, mede door de smartphone, steeds meer samen waardoor de discussie over de zwaarte van privacyschending op den duur niet meer uit maakt, aldus een respondent. Een advocaat geeft aan dat de privacyschending van het tappen met name zit in het opnemen van gesprekken, smsjes en internetverkeer in het strafdossier die niet ter zake doende zijn, maar wel erg gevoelig kunnen liggen zoals het bezoek van pornowebsites en contacten met maîtresses. Het opnemen van deze informatie in het strafdossier maakt het openbaar toegankelijk.

6.19 Notificeren en vernietigen

Zoals eerder in paragraaf 3.6 is beschreven dienen personen tegen wie een bijzondere opsporingsbevoegdheid is ingezet, achteraf genotificeerd te worden. Doel van deze wettelijke verplichting is personen op de hoogte stellen van het feit dat er door inzet van een bijzonder opsporingsmiddel een inbreuk op de privacy is gemaakt. Uit onderzoek van Beijer et al. uit 2004, blijkt dat er destijds slechts incidenteel werd genotificeerd. Op de meeste parketten ontbrak het aan duidelijk beleid over het notificeren en heerste angst voor het moeten prijsgeven van gebruikte opsporingstactieken. Hoe is de situatie anno 2011? Hoe gaan het landelijk parket, het functioneel parket en de twee onderzochte regio's om met de notificatieplicht? Wordt deze nageleefd? En staat men nog steeds negatief tegenover de plicht tot notificatie van personen? Hieronder wordt op deze vragen ingegaan.

6.19.1 Plichtsgetrouw?

In tegenstelling tot wat de onderzoeksresultaten uit 2004 laten zien, blijkt dat er anno 2011 in de onderzochte parketten doorgaans wordt genotificeerd. Hoewel de wettelijke regeling betreffende het notificeren duidelijk is, geeft ieder parket er zijn eigen invulling aan. Er zijn duidelijke verschillen in de naleving en uitvoering van de notificatieplicht. In regio A zeggen meerdere respondenten dat het notificeren jarenlang een lage prioriteit heeft gehad, maar dat er vanuit justitie druk wordt gelegd om deze plicht na te leven. Momenteel is een inhaalslag gaande om personen te notificeren en politie de bevelen tot vernietiging te geven. De verantwoordelijkheid van het notificeren ligt volgens de wet bij de OvJ. Echter, in regio A is het de parketsecretaris die OvJ's op de hielen zit om te gaan notificeren:

> "Niemand loopt warm voor het notificeren maar het gebeurt wel." - parketsecretaris

Een andere parketsecretaris geeft aan dat in minder dan de helft van de zaken wordt genotificeerd. Redenen om niet te notificeren zijn in regio A: er is geen recent adres bekend van de te notificeren persoon, het bewijs komt niet rond in een zaak en blijft op de plank liggen, een onderzoek levert restinformatie op, het gaat om een ZwaCri-zaak of er is sprake van onwil. Een OvJ geeft aan dat hij niet notificeert totdat de parketsecretaris echt veel druk op hem gaat uitoefenen. De OvJ zegt hierover:

> "De reden dat ik notificeren vaak voor me uitschuif is dat personen die zijn getapt en die nu niet van waarde lijken, een aantal jaar later van belang kunnen zijn. (…) Het kan dus een ongewenst neveneffect hebben als je mensen voortijdig gaat informeren dat ze in een opsporingsonderzoek in beeld zijn gekomen. Wanneer is een onderzoek afgerond? Wat mij betreft staat dat behoorlijk ver in de sterren geschreven." - OvJ

Respondenten uit regio B daarentegen geven aan dat het notificeren strikt wordt nageleefd. Daarmee zijn ze naar eigen zeggen uniek in Nederland. Door meerdere respondenten uit deze regio wordt bevestigd dat het zelden voorkomt dat er niet wordt genotificeerd. Ook in zaken die uiteindelijk niet op zitting komen en in ZwaCri-zaken wordt in principe genotificeerd, 'mits toekomstig opsporingsbelang niet wordt geschaad'. Een respondent die op de BOB-kamer werkt en zich fulltime bezighoudt met notificeren, zegt dat in ongeveer 10 tot 20 gevallen per jaar wordt besloten niet te notificeren. Dit op een totaal van 2000 te notificeren personen per jaar. Niet genotificeerd wordt er in mogelijke cold case-, embargo- en zedenzaken. Dat het in regio B wel lukt om 'bij' te zijn met notificeren en geen achterstand te hebben zoals in regio A het geval is, ligt volgens deze medewerker van de BOB-kamer aan het feit dat er in regio B geld is vrijgemaakt om er iemand fulltime op te zetten. Van collega's uit regio A hoort hij dat ze er geen tijd en geld voor krijgen om eraan te werken. Daarnaast lijkt de administratie in regio B beter op orde te zijn, onder andere omdat ze daar jaarlijks kleinere hoeveelheden zaken te verwerken hebben.
Naast de twee onderzochte regio's is ook aan andere opsporingsinstanties gevraagd hoe wordt omgegaan met de notificatieplicht. Een OvJ van het Functioneel Parket (FP) geeft aan dat hij de plicht uitvoert en notificeert waar de wet dat vraagt. De FIOD tapt veelal verdachten, en weinig betrokkenen, waardoor de hoeveelheid te notificeren personen is te overzien. Uitzonderingen worden gemaakt wanneer notificeren mogelijk schadelijk is voor ander onderzoek of wanneer informatie verkregen in een onderzoek tevens gebruikt wordt in een ander onderzoek. Een opsporingsteam op landelijk niveau geeft aan dat na gebruik van de tap bij het opsporen van voortvluchtige personen niet genotificeerd wordt door de OvJ.

6.19.2 Moment van notificeren

In de onderzochte regio's wordt het notificeren gecoördineerd door de BOB-kamer. De BOB-kamer is een administratief onderdeel van het OM dat zich bezighoudt met de administratie rondom de inzet van BOB-middelen, waaronder ook het notificeren valt. In regio A is de afspraak gemaakt dat een jaar na start van een onderzoek door de administratie wordt gevraagd aan de desbetreffende OvJ hoe de stand van zaken in dat onderzoek is, en of er genotificeerd kan worden.
In regio B wordt twee maanden na sluiting van een onderzoek op initiatief van de BOB-kamer en in samenspraak met de OvJ besloten om te notificeren.

6.19.3 Meningen over notificeren

Naast de vraag of er wordt genotificeerd, is ook gevraagd hoe men tegen de notificatieplicht aankijkt. De meerderheid van de respondenten, ongeacht de regio waarin of het niveau waarop ze werkzaam zijn, vindt de notificatieplicht een onzinnige regel. Dat bleek reeds uit onderzoek van Beijer et al. (2004), maar bij een meerderheid van de respondenten in dit onderzoek is deze opvatting niet veranderd, ondanks het feit dat deze verplichting nu wordt nageleefd. Uit de interviews blijkt dit meerdere redenen te hebben. Sommige respondenten zijn bang dat, met het notificeren van personen, opsporingstactieken op straat komen te liggen. Een OvJ geeft aan nooit iets van die plicht te hebben begrepen:

> "Notificeren, ik vind het prima maar je krijgt meer vragen dan dat je er iets mee opschiet. (…) Terwijl als je het niet had geweten, is dat nou zo erg? (…) Kijk voor schuin oversteken gaan we echt niet afluisteren, we hebben het gewoon echt over zware criminaliteit waarvan iedereen op zijn achterste benen staat dat het opgelost moet worden. Welke middelen heb je? Nou dit, dus vinden we het een goed middel, maar moet je daar dan achteraf iedereen van in kennis stellen zodat boef X ook weet dat ie de volgende keer geen telefoon meer moet gebruiken? Ik vraag me dat werkelijk af." - OvJ

Het idee van slapende honden wakker maken wordt juist betwijfeld door een andere OvJ. Hij zegt:

> “Er zijn zaken die helemaal niks opleveren. Dan krijgt die café-eigenaar een brief dat 126mn is toegepast, verdere informatie wordt niet verstrekt. Dan kan ie eruit afleiden dat zijn nummer getapt is, so what? Daar deden we in het begin een beetje spastisch over, zo van dan maken we slapende honden wakker. Nee, ik kan geen voorbeeld noemen dat door notificeren een zaak niks is geworden. (…) In het begin dachten we je maakt slapende honden wakker, maar dat blijkt reuze mee te vallen.” - OvJ

Andere respondenten hebben moeite met de notificatieplicht omdat zij van mening zijn dat de notificatiebrief meer vragen oproept dan het beantwoordt. In de brief (te vinden in bijlage 2) wordt vermeld welke bijzondere opsporingsbevoegdheden tegen een persoon zijn ingezet, maar niet of je verdachte of betrokkene was in het onderzoek en om wat voor onderzoek het ging. Volgens deze respondenten moet je als gewone burger langs de bibliotheek om het juridische taalgebruik te begrijpen. Een andere OvJ beschrijft de brief als inhoudsloos:

> “Ik vind het echt een volstrekt zinloze exercitie. Iemand wordt getapt, als dat niks oplevert kun je ‘m een briefje sturen ‘je bent getapt’, maar hij kan niks met dat briefje. Het levert alleen maar ergernis op voor de personen in kwestie, want wat weet de overheid? Als hij er vragen over heeft, kunnen we er niks over vertellen. Het enige wat je doet met zo’n briefje is mensen de stuipen op het lijf jagen.(…) De privacy is al geschonden, dat notificeren maakt dat niet anders” - OvJ

De inhoud van de notificatiebrief verschilt per arrondissement, maar de strekking is hetzelfde: op grond van artikel 126bb Sv dient een persoon wiens privacy door inzet van een bijzonder opsporingsmiddel is geschonden hiervan op de hoogte te worden gebracht. Daarbij wordt aangegeven welk opsporingsmiddel is ingezet en de duur ervan. De afsluitende alinea laat weten dat nadere informatie niet wordt verstrekt. In bijlage 2 zijn de notificatiebrieven, zoals deze in de onderzochte regio’s gebruikt worden, opgenomen. De meerwaarde van een dergelijke brief wordt door de meeste respondenten niet ingezien. Men is transparant naar de rechter en vraagt zich af waarom ze dat ook naar de individuele burger moet zijn in een inhoudsloze brief die alleen maar vragen oproept. Een parketsecretaris zegt hierover:

> “Je kunt je afvragen wat het doel is. Na Van Traa wilde men helderheid en transparantie, maar wij sturen iemand een brief waarin staat dat hij of zij getapt is in die periode en verder zeggen we niks.(…) Mensen worden eigenlijk het bos ingestuurd. Ze kunnen een beroep doen op de Wet Openbaarheid Bestuur en de Ombudsman. Daar horen wij verder niks meer over. Dus we weten ook niet of dat resultaat heeft. Ik vind het een transparantie van niks.” – parket-secretaris

Ook een advocaat is van mening dat de brief ‘heel leeg’ is. Maar niet iedereen is het daarmee eens. Een andere advocaat is van mening dat de notificatieplicht gewoon nageleefd moet worden, ook al lijkt deze vrij inhoudsloos. Hij zegt:

> “Ik vind dat waarde hebben. Heel abstract gewoon, dat je weet dat het gebeurd is. Als je er bezorgd van raakt, dat is terecht want je bent afgeluisterd door de overheid. Dat daar dus belletjes over komen en onrust over ontstaat, dat geeft ook een rem op de toepassing van het middel. Als je namelijk 10.000 mensen aftapt en ze gaan allemaal bellen, dan staat je telefooncentrale plat. Dan is het een reden om je voordat je 10.000 mensen aftapt af te vragen, willen we dat en ook het gedoe wat daarbij komt. Dat het compliceert is ook de bedoeling. Dus ik vind het waarde hebben. Het feit dat er niets gedetailleerd in staat is absoluut geen smoes om het af te schaffen. De vervolgvraag is inderdaad, of je niet iets meer zou kunnen zeggen. Bijvoorbeeld, het onderzoek is inmiddels afgesloten en wij hebben vastgesteld dat u geen verdachte bent.” - advocaat

Slechts één OvJ zegt dat zij het wel netjes vindt om te notificeren. Immers, er zijn telefoongesprekken afgeluisterd. De politie weet van alles over je. Deze OvJ geeft aan dat zij zelf ook op de hoogte gesteld zou willen worden als zij was afgeluisterd.
Hoewel de respondenten dus overwegend negatief aankijken tegen de notificatieplicht, wordt deze door de meeste respondenten toch uitgevoerd maar dan wel zonder prioriteit. Men vindt het een administratieve klus die niet bij de OvJ zou moeten liggen. In de praktijk is het echter de parketsecretaris of de BOB-kamer die zich met de uitvoering van het notificeren bezighoudt. De OvJ beslist alleen of al dan niet genotificeerd dient te worden en ondertekent vervolgens het formulier. Een OvJ uit regio A zegt dat de notificatieplicht geen reden is om minder te gaan tappen, terwijl een politiefunctionaris uit dezelfde regio zegt dat het notificeren een directe aanleiding is om selectiever te gaan tappen omdat men nu weet dat deze personen op een gegeven moment aangeschreven moeten worden.

6.19.4 Nadere informatievoorziening en klachten

Hoewel in de notificatiebrief staat vermeld dat nadere informatie niet wordt verstrekt, komt het toch voor dat mensen bellen voor vragen of nadere uitleg.
Regio A had in het verleden een notificatiebrief waar veel over werd gebeld. Deze brief bevatte veel juridische termen waar de gewone burger geen wijs uit werd. Inmiddels is de brief aangepast en zijn er, na het versturen van een beter leesbare versie, volgens een parketsecretaris en medewerkers van de BOB-kamer, geen telefonische vragen meer binnen gekomen over de notificatiebrief. Men is momenteel bezig achterstanden weg te werken. Echter, de adressen van de te notificeren personen worden uit het strafdossier gehaald en zijn vaak al jaren oud. De medewerkers van de BOB-kamer geven aan eventuele adreswijzigingen en andere mutaties niet te kunnen controleren in de gemeentelijke basisadministratie omdat men geen toegang heeft tot de gegevens. Vermoedelijk zal de notificatiebrief hierdoor niet alle personen bereiken. Mogelijk dat dit ook bijdraagt aan het uitblijven van vragen over de notificatiebrief. Wanneer er wel een vraag komt, geeft men overigens niet meer informatie dan al in de brief staat vermeld.
In regio B daarentegen geeft een medewerker van de BOB-kamer aan dat hij, als mensen hem in paniek opbellen hij nog wel eens het dossier erbij wil pakken om ze gerust te stellen. Hij informeert dan beknopt over het onderzoek en legt hij uit dat deze brief juist dient om ze gerust te stellen omdat het niet tot vervolging heeft geleid. De BOB-kamer in regio B werd in het begin 5 tot 10 keer per dag gebeld door mensen die een notificatiebrief hadden ontvangen. Dat is toen doorgeschoven naar de parketsecretaris. Nu staat er een algemeen telefoonnummer op de brief, waardoor degene die belt bij de centrale binnenkomt. Dit blijkt als een soort filter te werken voor de BOB-kamer of voor de parketsecretaris, die nu nog slechts sporadisch (1 à 2 keer per maand) een telefoontje hierover binnenkrijgen.

De klachtenregeling van het OM blijkt dus voor verbetering vatbaar. In de notificatiebrieven van de onderzochte regio's wordt geen melding gemaakt van een klachtenregeling of van organisaties waartoe men zich kan wenden bij vragen. De onderzoekers hebben getracht te achterhalen waar men wel heen kan gaan met vragen of klachten. Er is contact opgenomen met het Juridisch Loket, waar de vraag is voorgelegd of zij wel eens vragen krijgen over een ontvangen notificatiebrief. Dit verzoek is uitgezet bij alle 30 vestigingen en van de 10 vestigingen die hebben gereageerd geven allen aan dat ze er nog nooit een vraag over dit onderwerp hebben gekregen.
Tevens kan men zich met een klacht richten tot de Nationale Ombudsman. Ook deze is door onderzoekers benaderd met de vraag of er wel eens klachten binnenkomen met betrekking tot de notificatieplicht. De Nationale Ombudsman geeft aan dat 'zeer sporadisch' klachten binnenkomen hieromtrent. In één geval klaagde een verzoeker over het geheel ontbreken van verdere toelichting door het OM, nadat hij schriftelijk geïnformeerd was over de toepassing tegen hem van een bijzondere opsporingsmethode. In een ander geval werd de verzoeker wel geïnformeerd dat zijn telefoon gedurende enige tijd werd afgetapt, maar bleef aanvullende informatie – ondanks een verzoek daartoe – uit. Beide klachten zijn ter kennisneming aan de betrokken instanties (OM en politie) doorgezonden. In één geval heeft de verzoeker nadere informatie ontvangen en was hij daarmee tevreden. In het andere geval was de (notificatie)klacht een ondergeschikte vraag bij een aantal andere vragen over de

informatievoorziening en de behandeling door de politie. In die klachtbehandeling is na kennisgeving, zonder verdere bemoeienis van de Nationale Ombudsman, een verdere afspraak gemaakt tussen klager en politie.
De Nationale Ombudsman geeft te kennen dat het zo lijkt te zijn dat mensen het er maar bij laten zitten als ze de brief ontvangen, de weg niet weten om beklag te doen of wellicht helemaal niet worden geïnformeerd. Daarmee is bij de Nationale Ombudsman de indruk ontstaan dat de notificatieplicht en met name de aanvullende informatievoorziening aan betrokkenen – niet verdachten – voor verbetering vatbaar is.
Een derde optie om aanvullende informatie te verkrijgen na ontvangen van een notificatiebrief, is het doen van een WOB-verzoek. Dit lijkt echter nog nooit te hebben plaatsgevonden.[31]

6.19.5 Derdenbescherming

Personen die zijn getapt, dienen dus genotificeerd te worden. Daarnaast zijn er nog heel veel mensen die communiceren met de getapte persoon en daardoor ook in hun privacy worden geschonden. Deze personen worden echter niet genotificeerd. Een respondent van Bits of Freedom pleit voor uitbreiding van de notificatieplicht met de personen die frequent contact hebben gehad met een getapt persoon.

> "Een vriend van mij die zelf bij de politie werkt die werd ineens, overigens geheel onterecht bleek later, voor intern onderzoek kwam er iets ter sprake. Hij zei je moet me niet meer bellen want ik weet zeker dat ik word afgetapt. Daar schrok ik wel van. Derdenbescherming is dus ook wel een belangrijk punt. Als er 26.000 taps lopen dan zijn er in feite veel meer mensen afgetapt."- BoF

Op de vraag hoe die derdenbescherming ingericht zou moeten worden, antwoordt de respondent:

> "Notificatieplicht zou zich kunnen uitstrekken naar mensen met wie herhaaldelijk contact is geweest. Het is toch belangrijk als burger om te weten of je bent afgeluisterd. Zegt niet alleen iets over dat concrete opsporingsonderzoek maar ook, en dat is ook een belangrijk onderdeel van de EVRM jurisprudentie, over het chilling effect wat afluisteren en bewaren van je gegevens op je telecommunicatieve handelingen kan hebben." - BoF

In de praktijk lijkt dit echter niet haalbaar te zijn gezien de grote hoeveelheid werk dat het met zich mee zou brengen. Van al deze personen zouden de naam- en adresgegevens achterhaald moeten worden, waarna zij zouden moeten worden aangeschreven.

6.19.6 Vernietigen

Artikel 126cc lid 2 Sv schrijft voor dat twee maanden na notificatie van een persoon, de processen-verbaal waaraan gegevens kunnen worden ontleend die zijn verkregen door het opnemen van telecommunicatie, vernietigd dienen te worden. Hoe gaat dit vernietigen er in de praktijk aan toe?
Het doel van vernietiging van processen-verbaal is de persoonlijke levenssfeer van betrokken burgers te beschermen. Omwille van dit privacy-belang wordt het onwenselijk geacht om gegevens die door inzet van bepaalde bijzondere opsporingsbevoegdheden zijn verkregen tot

[31] Op http://www.rijksoverheid.nl/documenten-en-publicaties/wob-verzoeken kan men zoektermen invoeren en kijken of er op een betreffend onderwerp wel eens een WOB-verzoek heeft plaatsgevonden. De onderzoekers hebben op diverse zoektermen gezocht (telecommunicatie, tap, telefoontap, BOB, bijzondere opsporingsbevoegdheden, 126m, 126n, 126na, de wet BOB), maar geen van deze zoektermen heeft resultaat opgeleverd.

in lengte der dagen in de politiesystemen te bewaren. Het is de OvJ die de vernietiging van processen-verbaal beveelt. De uitvoering wordt gedaan door het rechercheteam dat het onderzoek waarin is getapt heeft gedraaid. Onder processen-verbaal en andere voorwerpen worden niet alleen de originelen verstaan, maar ook eventuele kopieën ervan. Bij voorwerpen kan gedacht worden aan gegevensdragers waarop tekstbestanden of gedetecteerde signalen worden geregistreerd, zoals cd-roms en diskettes, maar ook een integraal uitgewerkt tapverslag (Blom, 2009, p. 630).

Uit de interviews blijkt dat men in regio A nog niet zo lang systematisch aan het vernietigen is. Sinds kort is er iemand binnen de politie aangesteld die de coördinatie op zich heeft genomen van het vernietigen van processen-verbaal. Deze persoon stuurt teamleiders stapels met te vernietigen processen-verbaal. Sommige respondenten geven aan wel bezig te zijn met het vernietigen van processen-verbaal, anderen houden zich er nog niet mee bezig. Een teamleider TGO zegt hierover:

> "Drie weken geleden heb ik mijn collega-teamleiders bijeen geroepen en gevraagd hoe zij dat nou doen. Een team had een verdwaalde collega die dat deed, de rest zat een beetje van nou wij doen dat eigenlijk ook niet. Nu proberen we het naar een hoger niveau te brengen om te proberen dat het niet bij de tactische poot komt te liggen. Ondertussen zwelt de stroom van papieren aan. Dus hoe langer je daarmee wacht. Tot nu toe besteed ik er geen aandacht aan." - politie

De achterstand in het vernietigen van processen-verbaal is volgens een politiefunctionaris te wijten aan de OvJ's;

> "Zolang we niet notificeren blijft het bewaard. Op het moment dat we gaan notificeren, wordt het vernietigd. Daar komt ook de achterstand vandaan, want officieren hebben heel vaak niet genotificeerd." - politie

Met ongeveer dertig mensen wordt in regio A fulltime gewerkt aan het vernietigen van dossiers. De teams zelf zouden niet veel van het vernietigen moeten voelen qua capaciteit, omdat er rechercheassistenten rondlopen die zijn aangenomen om dit soort taken verrichten. Maar een aantal respondenten geeft aan dat zij dat wel degelijk voelen, omdat zij deze taak niet bij anderen kunnen wegzetten. Het gaat soms om 50 tot 100 bevelen vernietiging per keer.
Regio B geeft aan dat zij zich een aantal jaar geleden hebben voorbereid op het notificeren en vernietigen. Door aan de voorkant van het proces zaken op een gestandaardiseerde wijze te borgen, is het vernietigen aan de achterkant zo gebeurd. Standaard wordt sinds een aantal jaar een zogenaamd 'nul dossier' opgemaakt, waarin alle ingezette bijzondere opsporingsbevoegdheden zijn weergegeven, zodat men niet het hele dossier door hoeft op zoek naar ingezette bijzondere opsporingsbevoegdheden. Regio B is dan ook bij met vernietigen. Regio B vernietigt tussen de 200 en 300 zaken op jaarbasis[32]. Men heeft daar de indruk dat ze hiermee redelijk uniek zijn in Nederland.

> "Het vernietigen kost niet veel tijd, want het is op dusdanige manier weggezet dat het eenvoudig te vinden is. Zowel digitaal als in het papieren dossier wordt er een mapje BOB-middelen aangemaakt, waardoor je het er zo uit kunt halen en kunt vernietigen. Het kost wel capaciteit, maar je bent niet dagen bezig met opschonen. Het gebeurt altijd in de losse uurtjes." - politie

[32] De cijfers hieromtrent voor regio A zijn ons onbekend.

De respondent van de FIOD geeft aan dat er bij hem nog geen bevelen ter vernietiging zijn binnengekomen. Wel heeft hij onlangs bericht gehad dat alles van voor 2007 vernietigd moet gaan worden, voor zover dat nog niet is gebeurd. De zaken die daarna hebben plaatsgevonden, moeten eerst goed worden bekeken.
Wanneer de processen-verbaal zijn vernietigd, maakt de politie proces-verbaal van vernietiging op en stuurt dit weer naar de OvJ. De BOB-kamer kan de zaak dan uit de kast halen en naar het archief brengen.
Het vernietigen van de informatie die met de tap is opgespoord is van belang voor verdachten en betrokkenen, wier privacy door de opsporingsinstanties is geschonden. Respondenten onderkennen dit, maar geven tevens aan dat deze vernietigingsplicht voor de opsporingsinstanties zelf veel minder gunstig is. Eén van de nadelen hiervan is dat met het vernietigen van processen-verbaal waarin gegevens staan opgetekend die zijn verkregen door middel van de tap, veel 'toetsbare informatie' verloren gaat die op een later moment in andere onderzoeken gebruikt zou kunnen worden voor de opsporing of als bewijs. Informatie uit telefoontaps laat zien wie met wie in contact staat, de frequentie van contact, waar subjecten het met elkaar over hebben etc. In de toekomst zou deze informatie van waarde kunnen zijn. Gezien het feit dat met het tappen en met het uitwerken van de tap zoveel opsporingscapaciteit is gemoeid, lijkt het vernietigen van deze processen-verbaal niet erg efficiënt te zijn en niet goed te passen bij het Nationaal Intelligence Model (NIM) (Strategische Beleidsgroep Intelligence, 2008) dat door de politie wordt nagestreefd. Het NIM is erop gericht om de informatie die de politie bij het uitoefenen van haar werk heeft vergaard optimaal te benutten om toekomstige criminaliteit - gestuurd door deze kennis - gerichter op te kunnen sporen of tegen te kunnen gaan.

6.19.7 Uitzonderingen

In twee gevallen kan vernietiging worden uitgesteld. Gegevens die verkregen zijn door het opnemen van telecommunicatie hoeven – in afwijking van artikel 126cc lid 2 Sv – niet te worden vernietigd, wanneer ze gebruikt kunnen worden voor een ander strafrechtelijk onderzoek. In dat geval mag de vernietiging worden uitgesteld totdat het andere onderzoek is beëindigd (artikel 126dd lid 1 sub a Sv). Daarnaast kunnen gegevens worden bewaard die betrekking hebben op personen die, op een wijze bij de Wet politieregisters bepaald, betrokken zijn bij zware criminaliteit (artikel 126dd lid 1 sub b Sv). Uit navraag blijkt dat zowel bij het landelijk parket als ook bij de arrondissementsparketten met enige regelmaat informatie verkregen met inzet van een tap, wordt opgeslagen op grond van artikel 126dd lid 1 sub b Sv. Vernietiging van deze informatie vindt plaats indien de Wet politiegegevens de opslag van de gegevens niet meer toestaat.

> "In regio B is de afspraak dat het de individuele OvJ is die beslist of er wel of niet vernietigd gaat worden, afhankelijk van de ernst van het feit. Er zijn zaken waarvan ik zeg (…) het mag nog niet vernietigd worden, want er kan over 5 jaar nieuwe informatie naar voren komen. Maar als je na 2 jaar geen nieuwe info hebt is de kans dat je uiteindelijk nog iets gaat vinden zo klein dan laat ik het vernietigen." - OvJ

> "Als je een zaak gedraaid hebt en die mensen zijn veroordeeld, dan kun je niet zeggen, we gaan niet vernietigen. Als het niet tot een zaak heeft geleid, kun je het 5 jaar in het ZwaCri-register zetten. Vervolgens kan die termijn nog een keer worden verlengd." - politie

6.19.8 Concluderend

Uit dit onderzoek blijkt dat er wordt genotificeerd, maar dat de afhandeling verschilt tussen de onderzochte parketten. Zo is de uitvoering in regio B heel strikt en wordt in alle gevallen (op een paar kleine uitzonderingen na) genotificeerd. In regio A gebeurt dit, mede door het grote aantal zaken per jaar, minder structureel en heeft men te kampen met achterstanden.

Respondenten van opsporingsteams op landelijk niveau geven aan de notificatieplicht in het algemeen uit te voeren waar de wet dat vraagt. Veruit de meeste respondenten – zowel op landelijk als op regionaal niveau – hadden twijfels over het nut van het notificeren. Zij benadrukten vooral de nadelen die aan het notificeren verbonden zijn. Voor hen wegen de mogelijke voordelen van het notificeren niet op tegen deze nadelen.

6.20 Administratieve last van de tap

De Commissie Van Traa deed, naar aanleiding van de IRT-affaire, de aanbeveling dat de opsporing controleerbaar en transparant diende te zijn. De inzet van opsporingsmiddelen moet worden vastgelegd in processen-verbaal, zodat het inzichtelijk is voor de rechter en verdediging wat er tijdens het opsporingsonderzoek heeft plaatsgevonden.
Zo geldt dit dus ook voor de tap. Een tapaanvraag moet per telefoonnummer worden onderbouwd. In een tapaanvraag dient onder andere te worden beschreven waarom men wil gaan tappen en wat men ermee denkt te bereiken. Deze onderbouwing van een tapaanvraag levert vaak meerdere A4-tjes op. Volgens sommige respondenten is de verantwoording van de inzet van opsporingsmiddelen doorgeslagen:

> "Men heeft er zo langzamerhand wel een sport van gemaakt om zoveel mogelijk papier te produceren. Het lijkt alsof niemand meer binnen een half A4-tje kan uitleggen waar de zaak omdraait." - RC

Als blijkt dat de persoon wiens telefoonnummer wordt getapt, nog meer telefoonnummers in gebruik heeft, dient ook voor elk van deze telefoonnummers een aparte tapaanvraag opgesteld te worden. In die gevallen waarin de verdachte bijvoorbeeld 20 verschillende telefoonnummers heeft, is het papierwerk omtrent de tapaanvragen aanzienlijk.
Een tapaanvraag gaat door vele handen, zoals die van de politie, de OvJ, de parketsecretaris, de administratief medewerker van de BOB-kamer, de RC en de ULI. De kans dat er werkfouten insluipen is aanwezig. Soms wordt een tapaanvraag bijvoorbeeld diverse malen gefaxt waardoor het formulier op een gegeven moment onleesbaar kan worden. Sinds begin 2011 is er wetgeving over de elektronische handtekening (Staatsblad, 2011).[33] Ten tijde van de gevoerde gesprekken was de digitale handtekening nog niet operationeel en kwamen problemen als onleesbare faxen regelmatig voor. Het in gebruik nemen van de digitale handtekening zal zeker bijdragen aan verbetering van het proces.

De inzet van bijzondere opsporingsbevoegdheden wordt bijgehouden in een BOB-dossier. Het BOB-dossier is een zogenaamd 'groeidossier': er komt steeds meer papierwerk bij naarmate er meer opsporingsmiddelen worden ingezet of verlengd. Dit levert een hoop werk op:

> "Het is toch van de zotte, dat als wij een langdurig onderzoek hebben en dat we bijvoorbeeld drie lijnen willen tappen, dat we bij alle drie de nota's dezelfde onderliggende stukken moeten voegen, terwijl ze die al hebben. Gaan we die lijnen verlengen, dan moeten we nogmaals die zelfde stukken plus de aanvulling voor de verlenging bijvoegen." politie

Respondenten geven dan ook aan deze papierwinkel rondom het tappen als last te zien.
In onderzoek van Brummelkamp & Linssen (2006) wordt ook reeds geconcludeerd dat de invoering van de Wet BOB tot een verzwaring van administratieve lasten heeft geleid. Een aantal respondenten doet dan ook de aanbeveling om tapaanvragen op een persoon te doen in plaats van een telefoonnummer. Zeker in geval van personen die meerder telefoonnummers gebruiken en daarnaast regelmatig van telefoon wisselen, kan dit

[33] Sinds januari 2011 (Staatsblad, 2011, nr. 1533) kan een tapmachtiging met een elektronische handtekening worden ondertekend.

aanzienlijk schelen in de administratieve lasten. De verlichting van de administratieve lasten bij de politie is iets wat het ministerie van Veiligheid en Justitie als speerpunt heeft. In 2014 moeten de administratieve lasten met 25 % zijn verminderd wat tot meer 'blauw op straat' moet leiden (zie het actieprogramma Minder regels, meer op straat, 2011). Administratieve druk is te verminderen door de procedure van tapaanvragen en toekenningen nader te bezien. Winst is te behalen door tapaanvragen en tapbevelen aan een persoon te verbinden in plaats van aan een telefoon- of toestelnummer. Dit zou de administratieve last aanzienlijk verminderen. Respondenten vanuit het OM geven aan dat men bezig is met gedachtevorming hieromtrent.
Verdergaande lastenverlichting is te behalen door ook tussentijdse wijzigingen van telefoonnummers of communicatievormen te ondervangen zonder grote administratieve handelingen. Dit zou bijvoorbeeld gerealiseerd kunnen worden door de RC de mogelijkheid te geven om te beoordelen of een verdenking tegen een persoon zwaar genoeg is om binnen de wettelijk toegestane periode van maximaal 4 weken, alle telecommunicatiemiddelen die door deze verdachte worden gebruikt te mogen tappen en om daarvoor dan één algemene machtiging af te kunnen geven.

6.21 Knelpunten van de tap

Tijdens de interviews is aan de respondenten gevraagd of ze knelpunten en/of verbeterpunten konden aangeven over het werken met de telefoon- en/of internettap. De reacties op deze vraag zijn te bundelen in de volgende onderwerpen: de transparantie van de opsporing, de aftapbaarheid en het administratieproces van het tappen. De door de respondenten genoemde knelpunten worden hieronder nader besproken.
Het knelpunt 'de transparantie van de opsporing' wordt voornamelijk genoemd door respondenten die zich bezighouden met zwacri-zaken. Zij zijn van mening dat het gebruik van bepaalde opsporingsmiddelen goed moet worden verantwoord, bijvoorbeeld tegenover de RC, maar de respondenten zouden de gebruikte opsporingsmiddelen liever niet in de openbaarheid willen brengen.

> "Alles wat je op papier zet lezen de boeven en advocaten van de boeven ook. Mijn idee is dat men buitengewoon goed geïnformeerd wordt over wat wij kunnen en wat wij niet kunnen." - OvJ

Wanneer het gebruik van een opsporingsmiddel naar buiten wordt gebracht, omdat het in het dossier verschijnt, is het middel eigenlijk al 'stuk'. De gedachte is dat criminelen elkaar informeren en men zo kan inspelen op de opsporingsmethoden van de politie. Door het gebruik van een opsporingsmiddel niet in de openbaarheid te brengen zou het middel veel langer bruikbaar zijn, aldus een respondent.
Het in gevaar komen van de aftapbaarheid is een ander vaak genoemd knelpunt. Beschikbare communicatiediensten en telefoontypen zijn niet altijd gemakkelijk aftapbaar. Doorgaans zijn de aftapproblemen na enige tijd opgelost en kan de opsporing vanaf dat moment wel beschikken over de inhoud van de communicatie. Men heeft hierdoor echter het gevoel achter de feiten aan te lopen en het idee dat de criminelen de opsporing steeds een stap voor zijn. Ook het huidige gebruik van de telefoon wordt genoemd als extra hindernis bij het tappen. Criminelen hebben vaak meerdere telefoons en prepaid telefoonnummers waardoor het soms een hele uitdaging is om de juiste telefoon en/of het juiste telefoonnummer te achterhalen. Dit kost bovendien ook erg veel capaciteit.

6.22 Samenvattend

In dit hoofdstuk is beschreven hoe de tap in de Nederlandse opsporingspraktijk wordt ingezet en gebruikt. Onderzocht is bij welk soort misdrijven een tap wordt ingezet, met welk doel dit gebeurt en wat de overwegingen daarbij zijn. Hieruit blijkt vooral de diversiteit waarmee de tap bij verschillende misdrijven wordt ingezet. De doelstellingen die men met

het tappen wil behalen zijn: het verkrijgen van achtergrondinformatie over een persoon of netwerk, richting geven aan het opsporingsonderzoek en het aansturen van andere opsporingsmiddelen (sturing), en het verkrijgen van bewijs (bewijs) of een combinatie van deze drie. Maar ook wordt het gebruikt om personen te lokaliseren en reisbewegingen in kaart te brengen.
Bij het besluit om te gaan tappen spelen verschillende overwegingen een rol: proportionaliteit en subsidiariteit, capaciteit van het opsporingsteam, persoonlijke voorkeur en het gemak waarmee een tap kan worden gerealiseerd. Het aantal taps dat per onderzoek wordt ingezet wisselt sterk en is afhankelijk van het aantal verdachten dat bij een zaak betrokken is en het aantal telefoons- en simkaarten dat zij gebruiken.
Uit de gesprekken met de respondenten blijkt dat het tappen van telefoons zeer arbeidsintensief is. Alle gesprekken moeten uitgeluisterd en uitgewerkt worden. Dit vergt dan ook veel capaciteit van het opsporingsteam. Tevens komt uit het onderzoek naar voren dat het specialistisch werk is. Wanneer een andere taal dan het Nederlands wordt gesproken worden er tolken in geschakeld.
Een voordeel dat door sommige respondenten wordt genoemd van het werken met tolken is dat het een extra paar handen zou opleveren voor het opsporingsteam. Daar tegenover staat het door de respondenten vaak genoemde nadeel van het volledig afhankelijk zijn van een tolk. Maar de respondenten zijn overwegend positief over het werk dat tolken leveren.
De overweging om een tap al dan niet af te sluiten of te verlengen blijkt afhankelijk te zijn van de verhouding tussen de informatie die de tap oplevert en de capaciteit die het kost om een tap uit te werken. Een tapmachtiging wordt voor een bepaalde periode met een maximum van 4 weken door de RC afgegeven. Het afsluiten van taplijnen voordat de afgegeven periode is verstreken komt vaak voor. Redenen die respondenten noemen voor het voortijdig afsluiten zijn: het uitblijven van relevante informatie - soms omdat de getapte lijnen niet (meer) worden gebruikt, een tekort aan capaciteit om de lijnen uit te luisteren en uit te werken, en het feit dat een onderzoek ten einde loopt of wordt afgesloten.
Sinds de wetwijziging van 1 februari 2000 mogen, naast verdachten, ook betrokkenen worden getapt. Respondenten geven aan een tap op een betrokkene te overwegen als ze verwachten daarmee belangrijke opsporingsinformatie te kunnen vergaren die niet of niet zo snel met behulp van andere opsporingsmiddelen kan worden achterhaald. Verder geven de respondenten aan een tap op een verdachte anders te wegen dan een tap op een betrokkene vanuit het oogpunt van privacyschending van betrokkenen. Bij de overweging om een tap op een betrokkene aan te sluiten wordt de lat, zowel door de politie als door de OvJ en de RC, hoger gelegd. Een RC zoekt de bescherming van de privacy van een betrokkene tevens in de periode waarvoor een tapbevel wordt afgegeven. Deze is doorgaans korter dan wanneer een tapbevel wordt afgegeven op een verdachte.
In dit hoofdstuk hebben we kunnen zien dat het nummerherkenningssysteem dat is opgezet om te voorkomen dat gesprekken met geheimhouders in het opsporingsproces terechtkomen, nog niet optimaal functioneert. Totdat het probleem met het registreren van advocaten in het systeem is opgelost, zal de 'oude' werkwijze omtrent geheimhoudersgesprekken nog moeten worden nageleefd.
Uit dit deel van het onderzoek blijkt dat de telefoontap vooral sturingsinformatie voor het opsporingsonderzoek oplevert. Daarnaast blijkt het opsporingsmiddel informatie te genereren waarmee verdachten of slachtoffers kunnen worden opgespoord. In steeds mindere mate levert de tap direct bewijs op.
Tapgesprekken zijn volgens de respondenten vooral van belang vanwege het indirecte bewijs, informatie die ondersteunend is aan ander bewijsmateriaal. Hoewel het niet wordt nagestreefd, blijkt de tap ook vaak restinformatie op te leveren over andere misdrijven of personen.

Ten opzichte van 20 jaar geleden moet er volgens respondenten steeds meer moeite worden gedaan om hetzelfde resultaat uit de tap te halen. De opbrengst van het tappen is afhankelijk van meerdere factoren: het gepleegde of te plegen feit, de doelgroep waartoe de verdachte behoort, of er al dan niet reuring wordt veroorzaakt, of er een analist betrokken is bij het onderzoek, het afnemend gebruik van spraaktelefonie en ook gewoon van het toeval.
Nadat er een bijzonder opsporingsmiddel tegen een persoon is ingezet dient deze persoon achteraf hierover ingelicht te worden. Uit dit onderzoek blijkt dat het zogenaamde notificeren

van personen tegen wie een bijzondere opsporingsbevoegdheid is ingezet in de onderzochte parketten – zowel op regionaal als op landelijk niveau – daadwerkelijk gebeurt. Regio A is bezig met een inhaalslag om personen te notificeren en de politie de bevelen tot vernietiging te geven. Respondenten uit regio B daarentegen geven aan dat het notificeren strikt wordt nageleefd en ze geen achterstand hebben in het notificeren en vernietigen. Op landelijk niveau geeft men aan te notificeren waar dat wettelijk is vereist. Echter, de meerderheid van de respondenten, ongeacht de regio, vindt de notificatieplicht een onzinnige regel die onnodige administratieve rompslomp geeft. Men is bang dat opsporingstactieken op straat komen te liggen en de notificatiebrief roept meer vragen op dan het beantwoordt. Hoewel veel respondenten dus overwegend negatief aankijken tegen de notificatieplicht, blijkt deze plicht te worden uitgevoerd, zij het zonder veel prioriteit. Er wordt in de notificatiebrief geen melding gemaakt waartoe iemand zich kan wenden met vragen. De klachtenprocedure rondom de notificatiebrief blijkt dan ook voor verbetering vatbaar.
Respondenten noemen de volgende knelpunten en/of verbeterpunten over het werken met de telefoon- en/of internettap: 1) het feit dat criminelen goed op de hoogte zijn van de opsporingstechnieken van de politie; 2) het feit dat online telecommunicatie vaak met encryptieprogramma's wordt versleuteld; 3) Het omvangrijke administratieproces dat gepaard gaat met het tappen. Volgens sommige respondenten wordt er te veel in de openbaarheid gebracht over de opsporingsmethoden die de politie hanteert. Dit heeft tot gevolg dat daders rekening houden met het feit dat er heimelijke opsporingsmiddelen tegen hen worden ingezet en daar op in spelen. Hierdoor komt de aftapbaarheid van communicatie in gevaar. Criminelen zoeken alternatieve manieren om te communiceren en manieren om een tap te ontwijken. Zo blijken doorgewinterde criminelen bijvoorbeeld gebruik te maken van technische mogelijkheden om hun communicatie te versleutelen. Verreweg de meeste opmerkingen die gemaakt zijn over knelpunten rond het tappen, hadden te maken met de bureaucratie en de papierwinkel die gepaard gaat met het aanvragen van een tap.

7 De internettap in de praktijk

Het internet is vanaf 2001 aftapbaar, echter tot 2006 werd er niet veel meer mee gedaan dan het tappen van e-mail. Na 2006 werd de blik verruimd en zijn applicaties ontwikkeld waarmee het mogelijk werd om de resterende datastroom af te tappen. Door het intensieve gebruik van het internet worden de opsporingsdiensten ertoe aangezet de internettap steeds verder te ontwikkelen en te verfijnen. Momenteel is het aantal internettaps dat jaarlijks wordt ingezet binnen opsporingsonderzoeken, in vergelijking met het aantal telefoontaps, nog zeer bescheiden. Maar de verwachting is dat de toepassing van het opsporingsmiddel flink zal toenemen. Het circuitgeschakelde telefonienetwerk zal namelijk de komende jaren geheel IP-gebaseerd worden. De oude telefoontap zal dan alleen de VoIP omvatten die door Nederlandse aanbieders wordt aangeboden.
Ook kunnen verkeersgegevens betreffende het internet- en e-mailgebruik worden opgevraagd. Bij het opvragen van deze gegevens wordt inzichtelijk gemaakt welke IP-adressen door iemand zijn bezocht en van welke IP-adressen er e-mails zijn ontvangen. Voor deze gegevens is in de Telecommunicatiewet (hoofdstuk 13.2a, lid 3, sub b) een bewaartermijn gesteld van 6 maanden. De inhoud van telefoongesprekken of e-mails wordt niet bewaard en is dan ook niet opvraagbaar.
De wettelijke eisen voor de inzet van de internettap zijn dezelfde als die voor een telefoontap. Bij een internettap kan ervoor worden gekozen om alle gegevens die van en naar een bepaald IP-adres gaan te onderscheppen of om alleen het de binnenkomende e-mailberichten te onderscheppen.[34] Meerdere respondenten geven aan dat vooral het groeiend aantal smartphones een belangrijke drijfveer is achter de vernieuwingen van de internettap. Bij het aansluiten van een telefoontap, waarbij enkel telefoongesprekken worden onderschept, wordt op smartphones mogelijk cruciale communicatie gemist die via het internet verloopt. De verwachting van meerdere respondenten is dan ook, dat een tap op een smartphone in de toekomst vanzelfsprekend een internettap zal zijn. Maar zover is het in de praktijk nog lang niet. De internettap verschilt op cruciale punten met de telefoontap. Zo wordt bij een telefoontap een gesprek tussen twee mensen onderschept. De signalen die worden onderschept zijn bedoeld om te worden opgevangen door menselijke oren en te worden begrepen door menselijke hersenen. Het signaal dat normaal gesproken naar een telefoontoestel zou gaan, gaat nu naar de koptelefoon van de tapper, die precies dezelfde functie vervult als het telefoontoestel van de getapte persoon. Een internettap daarentegen, bevat signalen tussen de computers van het target aan de ene kant en aan de andere kant een veelheid van duizenden computers van diensten en andere gebruikers. Het signaal is niet uniform waardoor per tap vaak individuele aanpassingen nodig zijn om het signaal te kunnen begrijpen. De analysetools van de ULI kunnen bij de eenvoudigste signalen helpen, maar voor lang niet alle signalen is een decoderingsmodule gebouwd. Dat maakt het analyseren van een internettap moeilijk.

7.1 De inzet van de internettap

Als de internettap wordt ingezet, gebeurt dat vaak naar aanleiding van onderzoeksresultaten van andere opsporingsmiddelen, zoals een gesprek die met een telefoontap is onderschept waaruit blijkt dat men gebruik maakt van het internet om te communiceren met elkaar. Zo zeggen politiefunctionarissen:

> “We krijgen over de tap sms-verkeer mee en daar stond ondermeer in: ‘Ik heb dat en dat gekocht van die en die, kijk op je mail.’ Dan is het handig dat je weet wat er in die mail staat.” - politie

[34] Met een e-mailtap worden enkel de inkomende e-mails onderschept. Om de uitgaande e-mails te kunnen onderscheppen is een IP-tap nodig.

> “Ze zeiden: ‘We gaan wel even op MSN’. En dat wil je niet missen. Je voelt aan je water dat ze het over de zaak gaan hebben.” - politie

Historische internetverkeersgegevens worden veelal opgevraagd naar aanleiding van een internettap of naar aanleiding van specifieke feiten die met behulp van het internet zijn gepleegd, zoals internetoplichting. Deze gegevens kunnen opgevraagd worden voor een IP adres maar ook bij bepaalde websites. In dat geval wordt de bezochte site - bijvoorbeeld marktplaats - benaderd om historische gegevens te leveren met betrekking tot één of meerdere specifieke IP-adressen. Dit zijn dan vaak datum en tijd gegevens, soms aangevuld met een gebruikt e-mailadres, waarmee een bezoek van een bepaald IP-adres aan de betreffende site aangetoond kan worden.
Geïnterviewden geven aan dat steeds er steeds vaker een internettap wordt aangesloten op een smartphone. De leeftijd van de gebruiker van een telefoon is hierin vaak bepalend omdat jeugdige personen grotere gebruikers zijn van social media op internet dan oudere generaties.
Op de vraag hoe vaak men gebruik maakt van de internettap, wordt uiteenlopend gereageerd. Ten eerste is er een groep respondenten die tot nu toe nog nooit een internettap heeft ingezet en ook niet het idee heeft het opsporingsmiddel te missen. Zo geeft een respondent uit een wijkteam aan, geen gebruik te maken van de internettap omdat het niet bij zijn doelgroep past.

> “De mannen waar we hier mee te maken hebben leven uit een sporttas. Die staat vanavond bij Marie, morgen bij Joop. Die hebben vaak niet eens een echte vaste woon- of verblijfplaats. Dus ook die computer is niet echt hun ding. De verdachten zijn niet op dat niveau en daarom ook het onderzoek niet.” – politie

> “Dat met die smartphones begint nu te komen. Maar de meeste hebben nog telefoons die ze zo snel mogelijk weggooien. De termijn dat ze een bepaald nummer hebben is maximaal 2 weken tot een maand.” - politie

Bij deze doelgroep valt dan ook niet veel resultaat van de internettap te verwachten.
Een respondent vertelde in zijn jarenlange carrière ooit één e-mailtap gedraaid te hebben. Op zijn afdeling is een internettap wel eens overwogen, maar na advies van het KLPD is daarvan afgezien vanwege de hoeveelheid werk die erbij komt kijken. Dat hij de internettap sporadisch inzet is volgens deze respondent te wijten aan het type misdrijf waar hij op acteert.

> “We hebben bijvoorbeeld omzetbelastingfraude. Dat is een aangifte die wordt ingestuurd via internet, maar het IP adres wordt vastgelegd bij de belastingsdienst. Dus wij rechercheren terug van dat IP adres, daar zit de verdachte, we gaan daar zoeken en nemen zijn computer mee en zijn klaar. Met sigarettensmokkel heb je helemaal niks met internet te maken.” - politie

Ten tweede is er een groep respondenten die zegt de internettap wel met enige regelmaat in te zetten. Deze respondenten zijn enthousiast over de inzet en vertellen over de successen die ze ermee hebben behaald. Een deel van deze respondenten geeft zelfs aan in bepaalde type onderzoeken niet zonder te kunnen. Terrorisme wordt genoemd als type misdrijf waarbij de opsporingsdiensten in hun onderzoeken niet zonder internettap kunnen. In hightech crime zaken wordt vaker gebruik gemaakt van de internettap dan van een telefoontap. De beslissing om een internettap aan te sluiten blijkt afhankelijk van het type verdachte en de mate waarin deze zich op internet begeeft. Zo geeft een respondent een voorbeeld van een zaak waarin de verdachten actief op internet waren en de inzet van de internettap, in combinatie met andere opsporingsmiddelen, succesvol is gebleken:

> “We hadden een internettap op overvallers. Daardoor zagen we dat ze heel bewust op zoek waren naar een bepaald type auto op marktplaats. Toen hebben we zelf zo’n auto gekocht en daar techniek in gehangen. Deze hebben we te koop gezet op marktplaats en verkocht aan die jongens.” - politie

Ten derde is een grote groep respondenten te onderscheiden die in het verleden wel eens te maken heeft gehad met de internettap maar de inzet nu zoveel mogelijk probeert te vermijden. Uit de gesprekken komt naar voren dat de eerste ervaringen met het opsporingsmiddel dateren van enige tijd geleden. De eerste applicaties die toentertijd beschikbaar waren, waren verre van ideaal en verschillende respondenten refereren er nog aan:

> “Eén dag internettap daar was je ongeveer twee weken mee bezig om uit te werken.” - politie

Het lijkt alsof de moeizame start van de internettap een grote groep respondenten nog steeds negatief beïnvloedt in hun bejegening van het opsporingsmiddel. Inmiddels is de programmatuur, zeker in vergelijking met een aantal jaren terug, sterk verbeterd maar volgens meerdere respondenten is het nog steeds behelpen.

> “De infrastructuur is niet klaar, de applicaties die eigenlijk met elkaar moeten communiceren die zijn er niet. We hebben nog teveel losse applicaties. We hebben nu een team dat een smartphone gaat tappen, voor die betreffende type telefoon zijn drie applicaties nodig om de gegevens bij elkaar te krijgen.” - politie

Maar dit is niet het enige obstakel. Naast de niet gebruiksvriendelijke applicaties worden ook genoemd: de grote capaciteit die nodig is voor de uitwerking, een tekort aan digitale expertise binnen het team en de grote hoeveelheid data die een internettap kan opleveren. Op dit laatste punt komen we later in de tekst uitgebreider terug.
De inzet van een internettap kost, volgens alle respondenten, meer capaciteit van het opsporingsteam dan de inzet van een telefoontap. Dit wordt dan ook vaak aangegeven als reden om af te zien van dit opsporingsmiddel. Ook vraagt het uitwerken van een internettap andere, meer specialistische kennis dan het uitwerken van een telefoontap. Deze specialistische kennis is niet altijd voorhanden, en dat heeft weer direct gevolgen voor de snelheid en de adequaatheid waarmee een afgetapte datastroom kan worden verwerkt. De continue ontwikkelingen in de techniek die nodig zijn om datastromen te kunnen interpreteren vragen om constante investeringen in kennis op dit gebied. De respondenten vertellen dat hierop wordt geacteerd door het aanbieden van cursussen en het aantrekken van digitaal rechercheurs, maar dit was op het moment van onderzoek nog niet op peil. Bovendien, zo zegt een respondent, weten de meeste digitaal rechercheurs niets van internet. Zij hebben kennis van gegevens die op een computer of op een telefoon staan, maar niet zozeer van het onderscheppen en interpreteren van gegevens die via het internet binnenkomen. Zo zijn er korpsen waar niemand verstand heeft van stromende internetdata. Dit is voor sommige korpsen dan ook een reden om geen IP-taps meer te vragen, aldus een respondent.

> “Het dilemma met de internettap is dat rechercheurs geen specialisten zijn” - politie

7.2 Uitwerken en verbaliseren

De ULI adviseert een internettap uit te laten werken door rechercheurs met kennis van de digitale wereld. Volgens een respondent van de ULI is voor het uitwerken van de internettap specialistische kennis nodig en vereist het vaardigheden waarover een telefoontapper niet

hoeft te beschikken. Een moeilijkheid bij het uitwerken van de internettap is het gegeven dat de software die wordt gebruikt om de onderschepte data te kunnen analyseren niet exact hetzelfde resultaat te zien geeft als wat de gebruiker van de computer op zijn scherm zag tijdens zijn internetactiviteit. Wel is het zo dat alle gegevens die de gebruiker genereert worden opgeslagen, en in theorie doorzoekbaar zijn, aldus een respondent. Uit de gesprekken blijkt dat specialistische kennis betreffende de internettap in de beleving van veel respondenten schaars is waardoor niet het maximale resultaat uit de internettap wordt gehaald.

> "Digitaal rechercheurs daar zijn er te weinig van, waardoor de resultaten van de uitgewerkte IP-taps ook een vraagteken zijn." - politie

Er bestaan geen standaarden of richtlijnen over hoe een internettap dient te worden uitgewerkt en opgenomen in een proces-verbaal. De internettaps worden door tactisch rechercheurs zelf uitgewerkt. Dit zijn vaak mensen die enige affiniteit hebben met het internet. De respondenten vertellen dat de informatie die interessant is voor de opsporing wordt uitgewerkt. Echter, wat dit uitwerken precies inhoudt en welk format het moet krijgen daar is men niet eenduidig over.

> "Normale taps werken we uit in het BVO-systeem, maar een internettap moet je in Word knippen en plakken." - politie

> "Hoe moet ik dat nou verwoorden in een proces-verbaal? Moet ik een schermafdruk maken? We werken allemaal in BVO,(…) daar kun je geen foto in plakken. Wat moet ik met de informatie? Stel je voor ik heb een foto van een of ander, waar moet ik die laten? Moet ik die in een bijlage plakken? (…) Geef er een visie over. Geen flauw idee wat ze willen. De politie doet nu maar iets. Bepaal ik als politieman wat relevant is voor mijn onderzoek? Of moet ik die advocaat ook laten zien wat ik gezien heb?" - politie

> "Je maakt een samenvatting van wat je ziet. Omdat het digitale data is kun je gelukkig knippen en plakken, zodat je echte delen uit die tap kunt gebruiken als voorbeeld, zoals plaatjes of stukken tekst. Maar je kunt niet alles weergeven. Als een rechter ons verzoekt om een overzicht te verschaffen van alles wat we gezien hebben, dan kunnen we daar niet aan voldoen. Wat we wel kunnen is verschaffen wat we hebben getapt, maar daar heeft de rechter niets aan want dan moet je wel de kennis hebben om er vervolgens naar te kijken." – politie

Een advocaat vertelt over een zaak waarin zijn cliënt onder een internettap stond, waarbij er afdrukken van webpagina's opgenomen waren in het dossier. Hieruit bleek dat de man regelmatig bezoeker was van pornowebsites. Deze informatie had volgens de advocaat niks met de zaak te maken.

> "Het was een grote aantasting van zijn privacy. Het lag enorm gevoelig in de persoonlijke levenssfeer van deze persoon. Maar het diende geen enkel doel." - advocaat

Uit de interviews komt naar voren dat er behoefte is aan duidelijke richtlijnen over de uitwerking en verbalisering van de internettap. Ook pleit een respondent voor een kwaliteitscontrole van het verbaliseren van de internettap.

7.3 Hoeveelheid opgeslagen data en privacy

De hoeveelheid met een internettap afgevangen data kan enorm zijn. Wanneer een verdachte een actief internetgebruiker is worden, naast de e-mails en chatgesprekken, ook

films en muziek opgeslagen samen met alle andere bestanden die de verdachte binnenhaalt en verstuurt. Deze afgetapte informatie wordt in zijn geheel opgeslagen in de systemen van de ULI. Regelmatige gebruikers van de internettap zijn zich bewust van de grote hoeveelheid data die onderschept kan worden met een internettap.

> "Je moet van een internettap niet alles willen bekijken, je gaat bijvoorbeeld alleen voor de mail, de rest niet. Puur om de capaciteit. (…) Je moet het afkaderen: dat willen wij, dat is het doel. Maar als je een heel open doel maakt, dat je alles wilt tappen, dat is niet goed." - politie

Een respondent wijst erop dat de politie wordt geconfronteerd met een exponentiële groei van de hoeveelheid data. Niet alleen in IP-taps, maar overal (snellere computers, administraties, financiële gegevens, sensoren, twitter-feeds). Volgens haar is het probleem niet de grote hoeveelheid data, maar het feit dat de politie niet in staat is hoogwaardige analyses uit te voeren waarmee snel en eenvoudig belangrijke zaken uit die grote hoeveelheid data kunnen worden gehaald.
Voor het aansluiten van de internettap blijkt het hebben van een doel waarmee gezocht gaat worden in de getapte informatie dus essentieel. Bij het idee van 'een beetje meekijken' verliest men zich in de hoeveelheid informatie. Dit beginsel heeft niet elke respondent helder voor ogen.

> "Er komt veel te veel informatie binnen, waarvan 9 van de 10 stukjes niet bruikbaar zijn." - politie

> "In eerder onderzoek hebben we een internettap ingezet. Ervaringen daarmee zijn dramatisch. Het levert heel veel data op. Je verzuipt erin. Of hij doet het niet. Ze hebben er ook niks aan gehad." - politie

Het is niet ondenkbaar dat het 'ten ondergaan aan een overvloed aan data' voortkomt uit een tekort aan kennis over het middel. Maar ook de specialisten beamen dat de hoeveelheid afgetapte data gigantisch kan worden, wat het zoekproces naar bruikbare informatie erg moeilijk kan maken.
Een respondent vertelt dat er bij het doorzoeken en bekijken van de afgevangen informatie gebruik gemaakt kan worden van filtersets. Dit is programmatuur waarmee een selectie gemaakt kan worden op grond van zoektermen of type informatie. In de data zit immers veel informatie die niet relevant is voor de opsporing. Met behulp van een filterset kan het verkeer afkomstig van bepaalde webpagina's tijdens het doorzoeken worden geblokkeerd. Het voordeel hiervan is dat niet relevante sites niet hoeven te worden bekeken, bijvoorbeeld de door de verdachte bekeken pornosites. Deze sites zouden dan als groep geverbaliseerd kunnen worden in plaats van ze één voor één met naam en toenaam te noemen. Het gebruik van filtersets bij het analyseren van de onderschepte data wordt echter slechts door enkele respondenten genoemd.

Tijdens de voor dit onderzoek gevoerde gesprekken opperen digitale specialisten de mogelijkheid om de hoeveelheden onderschepte data te beperken door het inzetten van een techniek genaamd *deep-packet inspection.* Bij het inzetten van deze techniek kan elk pakketje internetverkeer, nog voordat het opslagen wordt bij de ULI, digitaal op inhoud geïnspecteerd worden om te zien of het voldoet aan bepaalde criteria. Op basis van de gemaakte selectie worden de pakketjes verschillend behandeld. Zo kan bijvoorbeeld muziek in de datastroom worden herkend om vervolgens uit de getapte datastroom te worden geweerd. Met de huidige regelgeving en technieken wordt *alle* informatie die van en naar een IP adres gaat opgeslagen, tenzij gekozen is voor het meelezen van alleen e-mail.[35] Daarbij is

[35] Alleen de e-mail die wordt verzorgd door een Nederlandse ISP, geen Gmail of Hotmail.

het onvermijdelijk dat privacygevoelige informatie van iemand wordt vastgelegd. Door het internetgedrag te volgen, te monitoren en op te slaan wordt immers een gedetailleerd beeld gevormd van iemand dat, volgens een respondent, raakt aan de meest wezenlijke kern van de privacy. Een andere respondent omschrijft het aftappen van internetgedrag als een grotere schending van de privacy dan de inzet van een telefoontap. En deze privacygevoelige informatie kan zijn weg vinden tot het strafdossier.

> "Er zitten dingen in een internettap die helemaal niet erg zijn als andere personen die kunnen zien, maar er zitten ook dingen in die veel persoonlijker zijn dan een telefoontap zou kunnen vermelden, namelijk omdat er informatie inzit die jij nooit met een persoon zou delen. (..) Het heeft de potentie van een dagboek lezen. " - politie

> "Er moet veel meer behoedzaam omgegaan worden met dit soort materiaal, ook met het opnemen in strafdossiers." - advocaat

Sommige respondenten zien de inzet van deep-packet-inspection als een duidelijke vermindering van de privacyschending van een getapte persoon. Wanneer deze techniek ingezet zou worden, wordt namelijk heel gericht gezocht en getapt in een datastroom. Informatie waarvan men denkt dat het niet relevant is voor de opsporing zou uit de getapte datastroom kunnen worden geweerd. Echter, op dit moment is het gebruik ervan voor opsporingsdoeleinden niet expliciet geregeld in de wet. Verschillende respondenten zouden dit in de toekomst graag veranderd zien.

> "Het stelt de aanbieder in staat om niet meer dan hetgeen strikt noodzakelijk is door te geven aan de opsporing, daarmee wordt naar de opsporing toe de privacy beter beschermd" - OvJ

> "De automatische selectie van de informatie is iets dat de opsporingsambtenaar op dat moment niet meer kan beïnvloeden. Maar stelt de opsporingsambtenaar wel in staat om bijvoorbeeld alleen MSN-verkeer binnen te krijgen. (…) Datgene wat je weg filtert, krijg je dus ook niet te zien. Dat blijft ook niet ergens bestaan, want dat is de angst die veel mensen hebben. Als je dat wettelijk en procedureel goed regelt is de inbreuk op de privacy misschien wel minder groot dan wanneer je gewoon gaat tappen." – politie

De verwachting is dat in de toekomst meer en meer communicatie via het internet zal gaan verlopen en dat tevens de snelheid van het internet zal toenemen. Dit zijn ontwikkelingen waardoor met de huidige internettap mogelijk nog grotere hoeveelheden data worden binnengehaald. Het opslaan en doorzoeken van grote hoeveelheden afgetapte data is in theorie mogelijk. Maar uit de gevoerde gesprekken blijkt dat goede programmatuur en kennis om hoogwaardige analyses uit te kunnen voeren ontbreken. Daarnaast maakt het vooraf bepalen en selecteren welke data men wil aftappen de inzet van de internettap volgens de respondenten meer gericht en effectief (zie ook Custers, 2008). Tevens wordt de privacyschending van de verdachte verminderd doordat alleen voor de opsporing relevante informatie wordt afgevangen. De inzet van een techniek als deep-packet-inspection zou behulpzaam kunnen zijn bij het selecteren van data die wel of juist niet afgevangen moet worden met de tap. Maar wellicht zijn er ook andere of toekomstige technieken die een bijdrage zouden kunnen leveren aan het meer gericht inzetten van een internettap.

7.4 Geheimhouders en de internettap

Gesprekken met geheimhouders opgenomen met een telefoontap hebben in het verleden tot situaties geleid die men in de toekomst probeert te voorkomen. Sinds kort is een nummerherkenningsysteem actief. Wanneer een getapt telefoonnummer contact heeft met

een nummer dat geregistreerd is in het systeem, wordt dat gesprek niet opgenomen en is het niet meer toegankelijk voor het opsporingsteam. Voor communicatie met geheimhouders onderschept door middel van een internettap bestaan echter geen protocollen en zijn geen procedures afgesproken. De meeste respondenten die werken met de internettap gaan ervan uit dat het ongeveer hetzelfde werkt als bij een telefoontap. Ook de advocaten zien hier niet direct een probleem.
Echter, de digitale specialisten zijn zich er wel terdege van bewust dat dit een probleem is dat niet eenvoudig te repareren valt. Een respondent legt uit dat een telefoongesprek een kop en een staart heeft, maar IP-internet niet. Bij het tappen van een internetlijn is alles met elkaar verweven in één datastroom. De getapte data is uiteindelijk te reduceren tot nulletjes en eentjes maar om daarin het juiste te vinden en vervolgens te verwijderen is niet eenvoudig. Bij het wissen van stukjes informatie is het niet ondenkbaar dat onbedoeld meer informatie wordt gewist dan gewenst.

> "Omdat er zoveel data in één keer over die lijn gaat, is het heel moeilijk om dat geheimhoudersgesprek eruit te filteren. Althans om in die nullen en enen te gaan knippen, dat alleen het audio deel is. Dat is technisch gewoon heel moeilijk." - politie

> "Dan komt er nog bij, hoe communiceer je, wat communiceer je? Is het alleen via mail dan is het niet zo moeilijk. Maar communiceer je ook nog eens middels foto's, gebruik je een hotmailbox, ja dat wordt gewoon ontzettend moeilijk om dat technisch allemaal te onderkennen van dit is een geheimhouder." - politie

Handmatig scannen en verwijderen van geheimhoudersinformatie, voor zover mogelijk, is geen doen door de grote hoeveelheid data die afgetapt wordt met een internettap. Het wordt volgens een respondent wel gedaan maar alleen waar nodig en het is zeer tijdrovend. Een politiefunctionaris vertelt dat hij nog zaken van twee jaar terug open heeft liggen waarbij geheimhoudersinformatie in internettapdata zit.
Indien men informatie van geheimhouders tegenkomt in getapte data, wordt dit volgens alle respondenten vernietigd. Maar naast de technische moeilijkheden van het vernietigen bestaat een ander probleem. Het uitgangspunt van de wet, dat de opsporingdiensten communicatie met geheimhouders moet verwijderen uit de getapte data, is onuitvoerbaar bij een internettap.

> "Bij de internettap wordt geselecteerd wat nodig is. Volgens de wet, die stamt uit de tijd van de bakelieten telefoon, moet je de complete tap bekijken en uitsluiten dat daar informatie van geheimhouders in zitten die niet vernietigd is. Maar dat is praktisch gezien niet mogelijk bij een internettap. Wat we wel kunnen aangeven is dat wat we aan data eruit halen en bekeken is, geen geheimhouders meer bevatten." - politie

> "Geheimhouders verwijderen kan alleen als je het hebt gevonden. Er is een discussie ontstaan of in alle oude internettaps gezocht moest worden naar geheimhouders. Dan ga je zoeken naar informatie die de politie niet mag zien. Als niemand het heeft gezien, laat het dan gewoon rusten." - politie

Over de mogelijkheden van het filteren van informatie afkomstig van geheimhouders wordt hard nagedacht. Een mogelijke oplossing die genoemd is door een respondent is het filteren door de aanbieder waarna alleen 'schone' data aan de opsporingsteams wordt doorgegeven. Maar dat is volgens andere respondenten technisch nog niet uitvoerbaar. Bij de ULI is men bezig protocollen te ontwikkelen om het scannen naar geheimhouders automatisch te laten verlopen. Men hoopt op korte termijn een oplossing te vinden.
De verantwoordelijkheid van het verwijderen van communicatie met geheimhouders uit getapte data ligt bij de OvJ. Een respondent opperde het idee dit alleen voor de telefoontap te laten gelden aangezien dat goed is gereguleerd. Advocaten en andere geheimhouders dienen zich ervan bewust te zijn dat communicatie anders dan via de telefoon in een tap

opgevangen kan worden en dat dit onbedoeld zichtbaar kan zijn voor de opsporingsdiensten. Deze respondent stelt voor om de rechter uiteindelijk te laten beslissen of de onbedoeld bekeken informatie in het voordeel of nadeel werkt van de verdachte.
Bij geen van de respondenten zijn zaken bekend waarin informatie van geheimhouders verkregen met een internettap een probleem is geweest. Dit kan komen doordat, zeker in vergelijking met de telefoontap, de inzet van de internettap beperkt is, en lang niet alle zaken waarin de internettap is ingezet voor de rechter komen. De verwachting is, zeker met het verbeteren en verfijnen van de programmatuur waarmee de onderschepte data bekeken kan worden, dat het gebruik van de internettap zal toenemen. De geheimhoudersproblematiek bij een internettap is daarom een vraagstuk dat aandacht behoeft, want zoals een respondent zei;

> "Het is natuurlijk wachten tot er een bommetje gedropt wordt. Het is wachten op een moment dat het verkeerd gaat of dat de advocaat zo slim is en zegt; ik heb over IP gecommuniceerd." - politie

7.5 Aftapbaarheid

In de inleiding van dit rapport is het onderwerp betreffende de aftapbaarheid van het internet al aan de orde geweest. Vaak wordt de internettap gezien als een opsporingsmiddel met een grote toekomst, maar specialisten zien dit anders.

> "Er zijn een aantal indicatoren die erop wijzen dat steeds meer diensten in de komende jaren versleuteld gaan worden. De politie kan dan in principe niet meelezen. Dat betekent dat je steeds minder leesbare communicatievormen in de internettaps zal krijgen, dus zullen deze gegevens gevorderd moeten worden bij de aanbieders." - politie

Encryptie wordt door een aantal respondenten gezien als een tool die wordt gebruikt wanneer iemand iets te verbergen heeft. Een gratis dienst op het internet voor het versleutelen van e-mail wordt door een respondent beschreven als "een dienst die stiekeme mensen faciliteert." Een andere respondent vertelt dat het feit dat er versleuteld gecommuniceerd wordt, "een interessante" bevinding op zichzelf is. Echter, diensten en verbindingen op internet worden niet enkel versleuteld om dingen te verbergen. Zo worden websites juist meer en meer beveiligd om te voorkomen dat mensen bijvoorbeeld naar valse websites worden omgeleid. Een e-mail verandert bij het versleutelen van een denkbeeldige briefkaart naar een brief in gesloten envelop. Betere beveiliging van het internet is van groot belang voor de veiligheid van personen, hun geld, privacy en goederen. Dat deze beveiliging het opsporingsapparaat bemoeilijkt wanneer criminelen er gebruik van maken is lastig, maar onvermijdelijk, aldus een respondent. Beveiliging door middel van encryptie blijft aanbevelenswaardig bij de toenemende digitalisering van diensten.
Meerdere respondenten vertellen dat ze regelmatig zien dat verdachten met VoIP-diensten via het internet bellen en dat de signalen die zijn binnengehaald met een internettap niet te ontsleutelen zijn. De aanbieders van telecommunicatiediensten op internet zijn encryptie bijna standaard gaan toepassen. Wanneer gebruik gemaakt wordt van een Nederlandse aanbieder is dit geen probleem, omdat deze aanbieder onder hoofdstuk 13 van de Telecommunicatiewet valt waarin de aftapplicht beschreven staat. Er ontstaan echter problemen wanneer de aanbieder van een online telecommunicatiedienst uit het buitenland afkomstig is en blijkbaar niet onder deze aftapplicht valt. In dat geval is bij een internettap meestal nog wel zichtbaar wie met wie contact heeft, hoewel dit uiteraard ook fictieve namen kunnen zijn, maar de inhoud van de gesprekken is niet te ontsluiten. Het is een groeiend probleem dat eerder al in een onderzoek van Stratix (2009) is opgemerkt.
Nederlandse aanbieders van online telecommunicatiediensten hebben de gesprekken doorgaans ook versleuteld en deze dienen gedecodeerd te worden om de aftapbaarheid mogelijk te maken. Deze decodering is geen standaard analysetool en decoderingsmodules

moeten regelmatig aangepast worden voor het betreffende signaal. Volgens een specialist gaat hier soms onnodig tijd overheen.

De digitale specialisten constateren dat afscherming en encryptie in toenemende mate de opsporing bemoeilijkt. Een mogelijke oplossing die hiervoor door deze respondenten wordt aangedragen is het meeluisteren of meekijken nog voordat de encryptie of afscherming heeft plaatsgevonden. Het binnendringen van een computer of smartphone op afstand is een techniek die dit mogelijk maakt. Het biedt mogelijkheden om, nog voordat de communicatie versleuteld wordt, te gaan tappen. Bij de huidige internettap onderschept de aanbieder alle data zoals deze over het kabeltje dat achter uit de modem steekt wordt verstuurd. Bij de techniek van het op afstand binnendringen van de computer worden data daarentegen onderschept nog voordat het versleuteld of verpakt het kabeltje ingaat. Op afstand binnendringen zou volgens een respondent in sommige opsporingonderzoeken zeer effectief zijn en daarmee zouden heel gericht voor de opsporing relevante gegevens kunnen worden veiliggesteld. Daarbij is de uiteindelijke inbreuk op de persoonlijke levenssfeer minder groot dan wanneer er langdurig getapt moet worden, waarbij mogelijk cruciale informatie in de afgetapte datastroom niet toegankelijk is. Deze techniek van het op een afstand binnendringen in een computer is op dit moment wettelijk niet expliciet geregeld (zie hierover Oerlemans, 2011). Specialisten geven aan dat deze techniek vanuit veel verschillende invalshoeken een overweging voor de toekomst kan zijn. Vanuit het OM is aan de minister geadviseerd om de mogelijkheden van het op afstand binnendringen van computers te onderzoeken.

> “De politiek moet zich afvragen: willen we zo min mogelijk inbreukmakende middelen inzetten? Ook als dat meebrengt dat je ze voor langere tijd moet inzetten, of dat de middelen ten opzicht van meer mensen moeten worden ingezet. Of vinden we het aanvaardbaar dat we gerichte, kortstondige inzet plegen? Die misschien wel wat dieper gaat, maar zich alleen richt op één persoon of computer waardoor je veel efficiënter kunt werken. En de privacyschending beperkter is.” – OvJ

Echter, de respondenten wijzen erop dat het op afstand binnendringen in een (mobiele) computer een actieve techniek is en dus altijd gedetecteerd kan worden. Daarnaast moet de techniek elke keer aangepast worden aan het desbetreffende individuele apparaat, waardoor de toepassing waarschijnlijk beperkt blijft tot inzet op kleine schaal. Daarnaast mag verwacht worden dat vanwege het grote inbreukmakende karakter van de techniek de inzet enkel voorbehouden zal zijn aan het opsporen en bestrijden van zeer ernstige delicten of zware criminaliteit.
Een andere mogelijkheid die respondenten noemen om communicatie via het internet toegankelijk te houden voor opsporingsdiensten is het aanscherpen van wettelijke kaders omtrent de aftapbaarheid. Nederlandse aanbieders van online telecommunicatiediensten vallen onder hoofdstuk 13 van de Telecommunicatiewet waarin de aftapbaarheid staat beschreven. In Nederland zijn buitenlandse dienstenaanbieders actief die zich nadrukkelijk op de Nederlandse gebruikersmarkt richten en daarbij commerciële belangen bij hebben. Echter, door zich achter het buitenlandse moederbedrijf te verschuilen ontlopen ze de aftapplicht. Ook van diensten die worden aangeboden op internet is niet altijd duidelijk of ze in Nederland worden aangeboden en daarmee binnen de Nederlandse jurisdictie vallen. Het gevolg hiervan is dat online communicatie die via deze dienstenaanbieder verloopt niet ontsleuteld kan worden wanneer het wordt afgetapt met een internettap. Volgens enkele respondenten worden opsporingsdiensten hierdoor feitelijk genoodzaakt om ingrijpender opsporingsmethodieken te ontwikkelen en toe te passen om de opsporing op peil te kunnen houden.

7.6 Concluderend

Uit de gesprekken blijkt dat de internettap in zijn huidige vorm wordt gezien als een log en moeilijk te gebruiken instrument, terwijl het tegelijkertijd ook een onmisbaar opsporingsmiddel wordt genoemd in de hedendaagse digitale samenleving.
Goede regelgeving en procedures ontbreken voor het uitwerken en verbaliseren van de onderschepte data. Ook over afgetapte informatie afkomstig van geheimhouders ontbreken afspraken. De respondenten zijn nagenoeg unaniem van mening dat de kennis bij de gemiddelde politiefunctionaris onvoldoende is om doelgericht en goed om te kunnen gaan met het opsporingsmiddel. Scholing of extra toevoeging van specialisten is zonder twijfel nodig, maar er is ook winst te behalen door een modernisering van de huidige internettap. Het versnellen van aanpassingen van de decoderingsmodules die nodig zijn om VoIP-gesprekken inhoudelijk te kunnen openen wordt door een specialist genoemd als één daarvan. Als tweede punt wordt niet zozeer de internettap zelf bedoeld maar het toevoegen van kennis over hoogwaardige data-analyse aan de politieorganisatie om grote bestanden met onderschepte data goed te kunnen doorzoeken.
Verder is het uitbreiden van de internettap met een selectiemethode als deep-packet-inspection door meerdere respondenten genoemd als overweging om het opsporingsinstrument te moderniseren. Door het onderzoeksteam vóór het aansluiten van een internettap een selectie te laten maken van het soort informatie dat afgetapt moet worden, zou de internettap veel doelgerichter kunnen worden ingezet. Tevens zou dit de privacyschending van de verdachte kunnen verminderen, doordat er een aanzienlijk deel van het internetverkeer van een verdachte niet afgevangen zal worden door de opsporingsdiensten. Deze geweerde informatie wordt nergens opgeslagen en kan ook op een later tijdstip dus niet worden doorzocht.

Er zijn in Nederland buitenlandse bedrijven actief die online telecommunicatiediensten aanbieden en zich daarbij geheel richten op de Nederlandse gebruikersmarkt. Respondenten geven aan dat deze online communicatiediensten niet altijd even goed aftapbaar zijn. Een respondent merkt op dat door het ontbreken van voldoende wettelijk kader om deze buitenlandse dienstenaanbieders onder de aftapplicht te scharen, de opsporing feitelijk genoodzaakt wordt om zeer ingrijpende methodieken te ontwikkelen, zoals het op afstand binnendringen van een computer of een mobiel, om bij de communicatie te kunnen komen en de opsporing op peil te houden. De verminderde aftapbaarheid van online telecommunicatiediensten is eerder gesignaleerd door Stratix (2009). Om technieken als het binnendringen van een computer op afstand of het toepassen van selectie methoden met behulp van *deep-packet-inspection* in de opsporing te kunnen gebruiken, en om online telecommunicatiediensten van buitenlandse aanbieders aftapbaar te houden, zijn wettelijke veranderingen noodzakelijk.

Echter, ook een moderne, verfijnde versie van de internettap is niet zaligmakend. Er is niet veel kennis nodig over digitale snufjes om een internettap te kunnen ontlopen. Overal is immers toegang tot internet en de basale kennis die nodig is om anoniem zaken af te kunnen handelen op het internet is volgens een van de respondenten echt wel doorgedrongen tot de mensen die dit perse willen.

> “Soms laten we ook kansen lopen omdat het te moeilijk wordt gemaakt. Er zijn teveel mogelijkheden voor een crimineel om op internet heimelijk hun dingetjes te doen.” – politie

8 Alternatieven voor de tap

8.1 Factoren

Binnen een opsporingsonderzoek worden meestal meerdere opsporingsmiddelen ingezet. Welke opsporingsmiddelen dat zijn, is afhankelijk van een aantal factoren. Hieronder gaan we in op deze factoren. Daarnaast bekijken we waarom de telefoontap zo vaak wordt ingezet in vergelijking met andere bijzondere opsporingsbevoegdheden en gaan we in op de vraag of er eigenlijk wel alternatieven zijn voor de tap.

8.1.1 Misdrijf

De keuze voor een bepaald opsporingsmiddel wordt mede bepaald door het soort misdrijf dat is gepleegd. Bij zogenaamde kleine of veelvoorkomende criminaliteit wordt meestal geen gebruik gemaakt van een telefoontap, omdat bij zulke delicten vaak niet aan de proportionaliteitseis is voldaan. De telefoontap kan alleen worden ingezet bij de wat zwaardere misdrijven.

> "Het algemene gevoel is dat er wel heel makkelijk getapt wordt in Nederland, maar er moet altijd sprake zijn van een ernstig misdrijf." - RC

Bij de onderzoeken naar ernstige delicten, georganiseerde misdaad en seriematige misdrijven, wordt volgens de respondenten vrijwel altijd gebruik gemaakt van de telefoontap. De reden daarvoor is drieledig. In de eerste plaats gaat het bij dit soort misdrijven om vormen van voortdurende criminaliteit. Door een goed beeld te krijgen van de handel en wandel van verdachten en door hun communicatiestromen en sociale netwerk in kaart te brengen, wordt gepoogd hier zicht op te krijgen en om een heterdaadsituatie te creëren. Het is moeilijk om op een andere manier informatie over dergelijke misdrijven te krijgen. Getuigen laten meestal weinig los, en van een verdachtenverhoor is vaak ook weinig heil te verwachten. Het gaat hierbij om professionele criminelen die hun activiteiten goed afschermen. Traditionele opsporingsmiddelen, zoals het horen van mensen en het verrichten van sporenonderzoek, leveren doorgaans niet de informatie op die nodig is om deze vormen van criminaliteit te kunnen bewijzen (zie hierover ook Bokhorst et al., 2011).
In de tweede plaats is de telefoontap feitelijk één van de weinige opsporingsmiddelen waarmee een opsporingsteam relatief snel een beeld kan krijgen van de activiteiten van de verdachten en van hun sociale netwerk. Hoewel informatie daarover ook achterhaald kan worden met de inzet van andere bijzondere opsporingsbevoegdheden, geven de respondenten aan dat met bijvoorbeeld de inzet van infiltratie vaak meer kosten zijn gemoeid. Niet alleen is het moeilijker om een dergelijk traject te organiseren, ook kost het vaak veel voorbereidingstijd voordat er met de inzet hiervan bruikbare informatie kan worden verkregen. Dit betekent dat er in de praktijk altijd eerst wordt nagegaan of de benodigde informatie met tappen, het opvragen van historische verkeersgegevens en observatie kan worden achterhaald.
Een derde reden hiervoor is dat de observatie- en infiltratiecapaciteit in Nederland zeer beperkt is, wat de inzet van andere bijzondere opsporingsbevoegdheden ingewikkeld maakt. Daarbij komt dat infiltratie ook als een ingrijpender middel wordt gepercipieerd, waardoor het niet in alle gevallen als een bruikbaar alternatief voor de telefoontap wordt gezien. Het inzetten van een ander bijzonder opsporingsmiddel is hierdoor niet altijd zonder meer mogelijk. Respondenten geven aan dat er wel over de mogelijkheden daartoe nagedacht zou moeten worden. Zo zou bijvoorbeeld vaker gebruik gemaakt moeten worden van observatie en pseudokoop via internet, aldus respondenten. Op die wijze zouden deze bijzondere opsporingsmiddelen beter binnen het bereik van de opsporingsteams kunnen komen. Ook het plaatsen van een OVC zou vaker tot de mogelijkheden moeten behoren, aldus respondenten. Hierop komen we later in deze paragraaf nog terug.

Als het gaat om reactieve onderzoeken, waarbij het opsporingsteam niet gericht is op het bewijzen van vormen van voortdurende criminaliteit, maar op het oplossen van een misdrijf dat in het verleden heeft plaatsgevonden, wordt de tap niet standaard ingezet. Er wordt in die zaken een afweging gemaakt tussen de wens of noodzaak om de zaak op te lossen en de kans dat er met een tap zinvolle informatie over de zaak kan worden achterhaald.
Bij zeer ernstige misdrijven, zoals moordzaken, waarvoor een TGO wordt opgezet wordt vaak meteen een telefoontap ingezet om bijvoorbeeld snel een beeld te krijgen van de leefwereld van het slachtoffer of om bepaalde scenario's die men heeft opgesteld te kunnen toetsen. Bij dit soort zaken is de range van in te zetten opsporingsmethoden die informatie over de gebeurtenis kunnen opleveren in eerste instantie relatief groot. Men kan de sociale kring waarin het slachtoffer zich bewoog in dit soort zaken immers ook in kaart brengen door daar veel mensen over te horen. Bij onderzoeken naar georganiseerde criminaliteit is dat veel moeilijker, omdat betrokkenen door de inzet van dit soort opsporingshandelingen op de hoogte raken van de belangstelling die de politie voor hen heeft. Als de opsporing minder gericht is op actuele activiteiten van de verdachten, maar op het bewijzen van een misdrijf uit het verleden, speelt dit een minder grote rol.
Daarnaast is bij reactieve onderzoeken vaak meer heil te verwachten van forensische sporen, van opgeslagen beeldmateriaal en van verklaringen van getuigen die mogelijk iets gezien hebben in de omgeving van de plaats delict. In reactieve zaken wordt de telefoontap veel meer gezien als een aanvulling op een hele range van in te zetten opsporingsmethoden. Alleen als er bij aanvang van het onderzoek al verdachten in beeld zijn, worden andere bijzondere opsporingsbevoegdheden, die meer inbreuk maken op de privacy, al bij de start van het onderzoek overwogen. Uit onderzoek van De Poot et al. (2004) blijkt dat er in deze zaken in beginsel vrij breed op niet-verdachte personen wordt getapt, en dat er pas later verdachten in beeld komen, waartegen dan vaak ook al bewijs in handen is. Soms kunnen verdachten in deze zaken direct aan de hand van het opgespoorde bewijsmateriaal worden aangehouden en worden verhoord. Alleen als dit niet het geval is, wordt de tap ingezet om bewijs tegen hen te verzamelen. In die situaties worden er soms ook meer ingrijpende bijzondere opsporingsbevoegdheden overwogen en ingezet. Het genoemde onderzoek laat zien dat dit bij reactieve onderzoeken slechts bij uitzondering het geval is.
Bij reactieve onderzoeken gaat het dus veel meer om de vraag of er al of niet gebruik moet worden gemaakt van bijzondere opsporingsbevoegdheden om informatie over de zaak te kunnen vergaren, dan bij de opsporing van voortdurende criminaliteit of van seriematige delicten.

8.1.2 Capaciteit en prioriteit

De mate waarin bijzondere opsporingsbevoegdheden kunnen worden ingezet is niet alleen afhankelijk van de wensen van een opsporingsteam, maar vooral ook van de capaciteit van zowel het opsporingsteam als van de ondersteunende teams. Zo kunnen undercoverbevoegdheden bijvoorbeeld niet in elk opsporingsonderzoek worden ingezet. Zo vertelt een respondent:

> "Nee. Dan zit je meer in de georganiseerde misdaad. Kost teveel geld. Capaciteit. Dat kunnen wij niet betalen. Zit je toch op een ander niveau onderzoek." - politie

De ondersteunende teams prioriteren de onderzoeken waarvoor hun diensten worden gevraagd. Of een zaak prioriteit krijgt is afhankelijk van de ernst van het misdrijf en van de uitvoerbaarheid van het in te zetten opsporingstraject. Volgens respondenten hebben grote landelijke onderzoeken meestal prioriteit. Daarmee is de variëteit aan opsporingsmiddelen waaruit kleinere teams kunnen kiezen dus kleiner.
Ook de inzet van observatie is niet altijd mogelijk. Niet-stelselmatige observatie wordt vaak door het rechercheteam zelf gedaan, maar wanneer er sprake is van stelselmatige observatie, of van een hoog afbreukrisico, wordt observatie uitbesteed aan een observatieteam. Zo'n observatieteam wordt echter door meerdere rechercheteams ingehuurd en zal de schaarse capaciteit moeten verdelen tussen de inhurende teams. Andere

opsporingsmiddelen kosten volgens respondenten veel voorbereiding en ook daar is niet altijd capaciteit en tijd voor.

> "De tap is een behoorlijk privacy inbreukmakend middel. Minder inbreukmakende middelen, zoals het stelselmatig inwinnen van informatie, kosten verschrikkelijk veel tijd en capaciteit om daar resultaat uit te halen. Ook niet iedere situatie leent zich voor het stelselmatig inwinnen van informatie. De capaciteitsafweging, efficiëntie in de opsporing, is dus zeker een belangrijke: ga je 4 man wekenlang zetten op si [stelselmatige informatie-inwinning] of ga je een week tappen en heb je genoeg?" - OvJ

De telefoontap is een opsporingsmiddel dat snel kan worden ingezet, en dat in theorie ook snel resultaten kan opleveren. Maar tappen kost een rechercheteam wel veel capaciteit vanwege het feit dat alle tapgesprekken uitgewerkt en uitgeluisterd moeten worden. Bovenstaande laat echter zien dat er in de praktijk niet altijd een ander middel voorhanden is waarmee hetzelfde doel kan worden bereikt.

8.1.3 Voorkeur

De keuze voor een opsporingsmiddel wordt mede bepaald door de mogelijkheden binnen het onderzoek en het te verwachten effect van het opsporingsmiddel. Daarnaast speelt persoonlijke voorkeur ook een rol in de keuze voor een opsporingsmiddel. Iedere OvJ en politiefunctionaris ontwikkelt in de loop der tijd een manier van werken waarbij de ervaringen die zijn opgedaan met bepaalde opsporingsmiddelen mede bepalend zijn voor de inzet van deze opsporingsmiddelen in de toekomst. Zo zijn er voorstanders van de telefoontap en personen die liever niet tappen. Een OvJ is van mening dat tappen een minder grote inbreuk maakt op iemands persoonlijke levenssfeer. Daarnaast heeft de tap als voordeel dat er geen sprake kan zijn van beïnvloeding van de verdachte, aldus de OvJ:

> "Wat ik persoonlijk vind, een tap heeft geen invloed op wat iemand zegt en doet over de tap. Je hebt geen enkele invloed op wie die belt, wat 'ie zegt, wat 'ie sms't en doet. En als je het over infiltratie hebt, dan is dat voor mij een heel ander verhaal, dat is veel dichter bij iemand komen omdat je dus contact met die persoon aangaat." - OvJ

De tegenstanders vermijden de telefoontap het liefst omdat het capaciteit vreet. Deze personen proberen juist andere opsporingsmiddelen uit. Teams die het zonder de tap proberen te doen komen echter vaak tot de conclusie dat ze niet zonder de tap kunnen (zie paragraaf 8.2).
Naast een persoonlijke voorkeur, zijn er ook opsporingsmiddelen die in bepaalde korpsen niet worden ingezet, zoals undercoverbevoegdheden. Hier geldt dus dat een heel korps soms een voorkeur of afkeer tegen een bepaald opsporingsmiddel heeft. Zo zijn sommige korpsen door de IRT-affaire wat huiverig geworden voor de toepassing van undercoverbevoegdheden (zie Kruisbergen & De Jong, 2010).

8.1.4 Kennis en ervaring

Sommige opsporingsmiddelen worden niet vaak ingezet. Hierdoor wordt er geen ervaring mee opgedaan en denkt men er gewoonweg niet aan om het in te zetten. Volgens één van de respondenten is onbekendheid en gebrek aan ervaring met bepaalde andere opsporingsmiddelen dan de tap een reden waarom ze weinig worden ingezet. Er leven hierdoor allerlei veronderstellingen over bijvoorbeeld de hoeveelheid werk die gepaard gaat met de inzet van een dergelijk middel, die niet altijd blijken te kloppen.
Met de tap heeft men zeer veel ervaring. Bovendien is de infrastructuur om te kunnen tappen in Nederland uitstekend geregeld. Mogelijk is het daardoor een veel gebruikt opsporingsmiddel.

8.1.5 Doorlooptijd onderzoek

Ook de doorlooptijden van een onderzoek kunnen van invloed zijn op de in te zetten opsporingmethoden. In regio A worden geen langlopende onderzoeken meer gedraaid. Na drie maanden wordt het onderzoek geëvalueerd, daarna krijgt het team nog hooguit twee maanden verlenging en wordt het onderzoek stopgezet. Volgens een respondent hangt daarmee samen dat in regio A het maximale wordt gevraagd aan opsporingsmiddelen en liever wordt afgeschaald dan opgeschaald. Er is immers niet veel tijd, en om in een korte tijd voldoende informatie te kunnen vergaren moet je fors rechercheren. Dit gebrek aan tijd zorgt er ook voor dat andere opsporingsmiddelen die veel voorbereidingstijd vereisen niet worden ingezet. Er wordt in deze regio dus vooral ingezet op het snel verkrijgen van resultaten. Middelen die daaraan kunnen bijdragen worden benut. Middelen die een lange adem vereisen worden vermeden.

8.1.6 Administratieve hobbels en stroperige procedures

Door respondenten wordt erop gewezen dat de tap snel kan worden ingezet, in tegenstelling tot veel andere opsporingsmiddelen. De administratieve hobbels die genomen moeten worden om andere opsporingsmiddelen in te zetten zijn veel groter.

> "Ik vergelijk het wel eens met de VS. De VS doen heel veel in het kader van intelligence of undercoverwerk. Ik denk dat dat ook de balans is. Onze tapaantallen zijn hoger dan in de VS, omdat wij het middel dat zij heel veel gebruiken om informatie te verzamelen weer niet makkelijk in kunnen zetten. We kunnen het middel infiltratie wel inzetten, maar het gebruik van dit middel is voorbehouden aan één speciaal aangesteld en opgeleid onderdeel binnen de politie in Nederland, waarvoor je een speciale machtiging nodig hebt. Dat is volgens Nederlands recht een veel ingrijpender middel dan een tap. Dus je kiest uiteindelijk voor het minst ingrijpende middel om daarmee eruit te halen wat in je doelstelling is opgenomen." - politie

Voor opsporingsmiddelen die een grotere inbreuk maken op de privacy dan de tap, moet men langs de Centrale Toetsingscommissie (CTC) gaan. Ook vergt dit soort opsporingsmiddelen vaak een veel langere voorbereidingstijd. Bijvoorbeeld omdat alleen gecertificeerd personeel, dat schaars is, de apparatuur mag aanbrengen en bedienen. Hierdoor kan kostbare informatie in de tussentijd verloren gaan. De tap daarentegen, kan binnen een uur (indien sprake is van een spoedprocedure) lopen.

> "Tappen is een middel dat je inzet op het moment dat je denkt dat je niet verschrikkelijk lang moet wachten met het verzamelen van je essentiële bewijs omdat dat de beste manier is. Je kunt ervoor kiezen eerst verkeersgegevens op te vragen, dan weet je waar iemand is geweest, maar zegt niets over met wie een overvaller bijvoorbeeld was en waar die de buit heeft verstopt. Dat is informatie die je over een tap wel kunt krijgen." - OvJ

De vraag is hoe de opsporing eruit zou zien als de tap niet zou bestaan? Een respondent zegt hierover:

> "Dan denk ik dat we veel creatiever zouden moeten zijn en dat we tegen onmogelijkheden aan zouden lopen. Wij kunnen de tap heel snel inzetten. Op het moment dat je de tap niet hebt, word je ertoe gedwongen om andere BOB-middelen in te zetten die heel veel voorbereiding vereisen. Dan moet je dus bijvoorbeeld gaan denken aan OVC, dat moet dan weer door een Centrale Toetsingscommissie heen, en er moet apparatuur worden geplaatst. Dat kost heel veel tijd." - politie

Opsporingsteams lijken, indien er sprake is van een korte doorlooptijd en beperkt budget, in zekere zin veroordeeld te zijn tot de tap, wat mogelijk de creativiteit in de opsporing beperkt.

8.2 Bewust opsporen zonder de tap

Twee teams, één op landelijk niveau en één team in regio A, zijn bewust bezig om opsporingsonderzoeken te verrichten zonder (grootschalige) inzet van de tap. Hieruit blijkt dat men beseft dat de tap veel wordt ingezet en dat daarmee mogelijk de creativiteit van het opsporen een beetje is verdwenen. Deze teams staan nog in de kinderschoenen. Het landelijke team heeft nu één onderzoek naar hotelescort succesvol afgerond. In dat onderzoek is geprobeerd om de geconstateerde criminaliteit tegen te gaan, of zoals een respondent het verwoordde "zand in de machine te strooien". Het onderzoek was dus minder gericht op het tot stand brengen van een strafzaak. Het betrof een meer programmatische/thematische aanpak, waarbij de strafzaak ondergeschikt is gemaakt aan de meer algemene aanpak van het geconstateerde probleem, waarvoor ook preventieve en bestuurlijke maatregelen werden ingezet. Dit is in overeenstemming met de visie van de Nationale Recherche: van opsporen naar bestrijden. Het is het landelijke opsporingsteam niet gelukt om dit onderzoek het helemaal zonder de tap te verrichten, maar men heeft het gebruik van de tap in dit onderzoek tot een minimum beperkt. Dat het hen is gelukt hun doel te bereiken zonder eindeloos te tappen heeft volgens hen te maken met het feit dat ze geen harde strafzaak hoefden te hebben en dus minder gericht waren op het vinden van bewijs. Als je een strafrechtelijk onderzoek verricht op het gebied van mensenhandel, ben je volgens de respondent veelal veroordeeld tot een tap.
Het team uit regio A geeft aan al enige tijd bezig te zijn met fenomeen- en probleemgericht onderzoek. Het doel van dit team is ook niet primair gericht op een strafrechtelijk onderzoek, maar eerder op 'het opwerpen van barrières' waardoor voortdurende criminele activiteiten worden bemoeilijkt. Veel bedrijven hebben er geen weet van dat ze criminelen faciliteren. Deze bedrijven worden na een strafrechtelijk onderzoek – waarin het fenomeen in kaart is gebracht -benaderd met de vraag om mee te werken aan het opwerpen van barrières, waarmee het voor criminelen moeilijker wordt om hun criminele activiteiten te verrichten. Wel merkt het team uit regio A dat nieuwe dingen proberen, innoveren, erg moeilijk is en niet gedaan kan worden zonder medewerking van het OM. Het team is nu aan het 'experimenteren' in kleine zaken en wil deze zaken voor de rechter brengen om zo jurisprudentie te verkrijgen over de opsporingsmethoden die zij inzetten.

8.3 Alternatieven voor de tap?

Uit de jaarlijkse tapcijfers blijkt dat de telefoontap veelvuldig wordt ingezet. Zijn er eigenlijk wel alternatieven voor de telefoontap? En kan opsporend Nederland wel zonder de tap? Om deze vragen te kunnen beantwoorden hebben we respondenten gevraagd naar de opsporingsmiddelen die ze naast de tap inzetten en of de tap wel alternatieven kent. Hieruit blijkt dat er zeker ook gebruik wordt gemaakt van andere opsporingsmiddelen, maar dat de tap niet echt een gelijkwaardig alternatief kent. Zeker wanneer verdachten bedacht zijn op politieaandacht is het lastig bepaalde andere opsporingsmiddelen in te zetten omdat het afbreukrisico – de kans op 'stuk gaan', door de mand vallen – groot is. De teams die proberen zonder de inzet van de tap op te sporen zien een alternatief voor het verzamelen van informatie in het praten met mensen in de wijk. Rechercheurs zouden zich actiever op kunnen stellen en de straat op moeten om te gaan praten met mensen in de wijk. Een andere optie is dat het blauw op straat zich sterker gaat richten op het achterhalen van opsporingsinformatie over bepaalde criminaliteitsfenomenen, en deze informatie vervolgens doorspeelt aan de rechercheteams.

> "Mensen weten veel meer dan ze ons in eerste instantie vertellen in een officieel bezoek." – politie

Zo vertelt een respondent dat ze in een onderzoek naar mensenhandel met hoerenlopers hebben gesproken.

> "Dat is een bron van informatie die veel meer vertelt dan je over een tap hoort." – politie

Het praten met mensen gebeurt momenteel niet genoeg, aldus de respondent. Het praten met mensen levert volgens hem ook niet altijd wat op omdat bepaalde gemeenschappen zodanig gesloten zijn dat je daar niets uit kunt krijgen. In dat soort gevallen is de tap waarschijnlijk waardevoller. Maar er wordt ook gewezen op de rol van de CIE. Als de CIE in bepaalde circuits een goede informatiepositie zou hebben dan zou er minder getapt hoeven te worden, aldus een aantal respondenten. De informatie die de CIE vergaart, sluit volgens deze respondenten vaak niet aan bij de informatie die de tactische teams nodig hebben. Door het opvragen van (historische) verkeersgegevens kun je een beeld krijgen van de contacten van de verdachte en van de nummers die mogelijk interessant zijn om te gaan tappen. Het voordeel is dat je, in tegenstelling tot de telefoontap, niets uit hoeft te werken, wat tijd en mankracht scheelt. Nadeel is dat de analyse van verkeersgegevens geen echte vervanging vormt van de tap is omdat de inhoudelijke informatie ontbreekt. Het opvragen en analyseren van verkeersgegevens is meer een voorbereidend middel.

Om in dit rapport een beeld te kunnen schetsen van de frequentie waarmee andere bijzondere opsporingsbevoegdheden worden ingezet, hebben we bij de CTC cijfers opgevraagd van bijzondere opsporingsbevoegdheden die bij de CTC werden aangevraagd en waarvoor door het College van PG's – na een positief advies van de CTC – toestemming heeft verleend. Het gaat hierbij om de inzet van OVC en infiltratie in de jaren 2009 en 2010.[36] Wat betreft OVC is er alleen toestemming van het CvPG's vereist wanneer het opsporingsteam dit middel wil inzetten in een penitentiaire inrichting of in een woning. Voor alle overige inzetten, bijvoorbeeld in een auto of openbare ruimte, is geen toestemming nodig. Hier zijn dan ook geen cijfers over bekend bij de CTC. In 2009 is 76 keer positief advies uitgebracht door de CTC en toestemming verleend door het CvPG's voor de inzet van OVC. In 2009 is geen enkele keer een infiltratietraject gestart. Daartegenover staat dat in 2009 24.724 keer door een RC een bevel tot het aftappen van (tele)communicatie is verleend. In 2010 is 73 maal een positief advies uitgebracht door de CTC en toestemming verleend door het CvPG's voor de inzet van OVC. Daarnaast is 2 keer positief advies door de CTC en toestemming verleend door het CvPG's voor de inzet van infiltratie. Als we kijken naar het aantal tapbevelen dat in 2010 is uitgereikt door een RC, dan komen we op een totaal van 22.006 bevelen.
Hoewel de cijfers niet één op één te vergelijken zijn en het vergelijken van het aantal keer dat verschillende opsporingsmiddelen worden ingezet zonder daarbij over achtergrondinformatie te beschikken, alleen oppervlakkige inzichten biedt (zie voor de vergelijking van cijfers betreffende de inzet van opsporingsmiddelen ook Kruisbergen & De Jong, 2010, p. 136-137) wordt wel duidelijk dat de telefoontap veel vaker wordt ingezet dan OVC in een woning of penitentiaire inrichting en infiltratie.
Wanneer andere opsporingsmiddelen worden ingezet is de tap vaak nodig als informatiebron om het betreffende opsporingsmiddel adequaat in te kunnen zetten. Zo is het voor observatie belangrijk om te weten waar verdachten elkaar treffen. Het is namelijk onmogelijk iemand 24 uur per dag, 7 dagen in de week te observeren. Om efficiënt gebruik te kunnen maken van bijvoorbeeld observatie is, om deze reden, toch een tap nodig.
Aan plaatsing van OVC-apparatuur gaan ook vaak observaties en taps vooraf om te kijken met wie de verdachte contact heeft en waar belangrijke ontmoetingen plaatsvinden. Op basis van die informatie wordt bepaald waar de OVC-apparatuur geplaatst moet worden.

[36] Van andere bijzondere opsporingsmiddelen waarvoor geen toestemming van het CvPG's is vereist, hebben we helaas geen overzicht van het aantal keer dat deze zijn ingezet en kunnen we de inzet ervan dus ook niet vergelijken met de inzet van de tap.

Dit geldt ook voor stelselmatige informatie-inwinning en infiltratie. Ten eerste is voor de opbouw van een dekmantel[37] van een undercoveragent informatie nodig over de verdachte. Deze informatie wordt vaak uit een telefoontap gehaald. Daarnaast wordt tijdens de duur van het undercovertraject door middel van de telefoontap de veiligheid van de undercoveragent in de gaten gehouden. Met de inzet van de verschillende opsporingsmiddelen worden vaak verschillende doelen gediend, en het onderzoek bevindt zich – op het moment dat voor bepaalde heimelijke opsporingsmiddel wordt gekozen – ook vaak in een in een andere fase. Observatie, stelselmatige informatie-inwinning en infiltratie zijn daarom geen bijzondere opsporingsbevoegdheden die zonder meer als gelijkwaardig alternatief kunnen dienen voor de tap.

8.4 Concluderend

Het voorgaande laat zien dat er naast de telefoon- en internettap ook andere bijzondere opsporingsmiddelen worden ingezet. De keuze voor een opsporingsmiddel wordt bepaald door het soort misdrijf (proportionaliteitseis), de beschikbare capaciteit, persoonlijk voorkeur, kennis en ervaring van het opsporingsteam, de doorlooptijd van het onderzoek en door administratieve hobbels en stroperige procedures. Om andere heimelijke opsporingsmiddelen in te kunnen zetten is echter vaak een tap nodig. Daardoor kent de tap in feite niet echt een alternatief. Mogelijk kan door de inzet van andere bijzondere opsporingsmiddelen de inzet van de tap wel worden verkort of gerichter worden ingezet.
De keuze voor de telefoontap is met name ingegeven door de snelheid waarmee het opsporingsmiddel kan worden ingezet en doordat er is zo goed als geen afbreukrisico verbonden aan het middel.

> "Als men zegt dat er teveel getapt wordt en dat gaan we terugdraaien, voorzie ik een paar sombere scenario's voor de opsporing in Nederland." – politie

Andere bijzondere opsporingsbevoegdheden vergen voorbereidingstijd, waardoor de kans dat kostbare informatie wellicht verloren gaat aanwezig is. Daarnaast kennen deze opsporingsmiddelen vaak een groter afbreukrisico. De subsidiariteitseis is hiermee eigenlijk een toets die altijd dezelfde uitkomst heeft.
Respondenten wijzen erop dat er vaak een samenspel van opsporingsmiddelen nodig is om tot bewijs te komen.

> *"Het is vaak een samenspel van de waarneming op straat door een observatieteam en je tap eroverheen en eventueel je bakengegevens. Dat moet je in elkaar schuiven en dat is het bewijs. Maar los van elkaar is het moeilijk."* - politie

> *"Maar alleen aan de taps heb je ook natuurlijk niks als je niet een observatie erbij hebt. Als je op de tap hoort dat er bruin of wit of nat spul wordt afgeleverd, of in codetaal dat je zegt dat zou wel eens een aflevering kunnen zijn, als er dan geen observatie is om dat te zien, te filmen of gewoon te bekijken, ja dan heb je nog niks."* - OvJ

Verschillende opsporingsmiddelen vullen elkaar aan en zijn van elkaar afhankelijk om succesvol ingezet te kunnen worden. Bepaalde opsporingsmiddelen, zoals de telefoontap, worden echter veel vaker ingezet dan andere. Dit is niet los te zien van de maatschappelijke context. De IRT-affaire heeft ervoor gezorgd dat men terughoudender is geworden met het toepassen van bepaalde opsporingsmiddelen, zoals infiltratie. Tegelijkertijd is er veel geïnvesteerd in de infrastructuur van het tappen. Tappen is in Nederland een geaccepteerd

[37] De opsporingsambtenaar, een undercoveragent, opereert daarbij vanuit een bepaalde cover/dekmantel en speelt een rol, bijvoorbeeld die van 'collega-crimineel'.

en breed ingezet opsporingsinstrument, terwijl er voor andere opsporingsmiddelen zoals infiltratie en het plaatsen van OVC apparatuur een ethische drempel lijkt te bestaan.

Deel III

Het gebruik van de tap in Engeland en Wales, Zweden en Duitsland

Inleiding

In dit derde deel van het rapport worden de vergelijkingslanden behandeld. Zoals in Deel I in paragraaf 1.2.2 is aangegeven hebben de variëteit in juridische verwantschap aan het Nederlandse strafrechtssysteem en het lidmaatschap van de Raad van Europa (*Council of Europe*) als selectiecriteria gediend. Ter verantwoording van de keuze wordt daarom per vergelijkingsland ingegaan op deze selectiecriteria, waarbij het betreffende strafrechtssysteem kort wordt beschreven.

Als vergelijkingslanden zijn Engeland en Wales, Zweden en Duitsland gekozen. In de volgende hoofdstukken wordt voor elk van de vergelijkingslanden wordt allereerst een algemeen beeld geschetst van de wijze waarop het strafrechtssysteem functioneert en wordt besproken welke overheidsorganen bij de inzet van de telefoon- of internettap betrokken zijn, voorts wordt besproken hoe de telefoon- en internettap in de praktijk worden ingezet, daarna wordt ingegaan op de waarborgen rond de inzet van heimelijke opsporingsmiddelen, en elk hoofdstuk sluit af met een samenvatting van de belangrijkste bevindingen.
Hoofdstuk 9 handelt over het gebruik van de tap in Engeland en Wales, hoofdstuk 10 over het gebruik van de tap in Zweden en hoofdstuk 11 over de wijze waarop de tap in Duitsland wordt ingezet in de opsporingspraktijk.

9 Het gebruik van de tap in Engeland en Wales

Engeland en Wales behoren samen met Schotland en Noord-Ierland tot het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland, waarvan de totale bevolkingsomvang 61.7 miljoen bedraagt.[38] Het Verenigd Koninkrijk is een constitutionele monarchie. Schotland en Noord-Ierland hebben een eigen rechtstelsel en een binnenlands bestuur, maar zijn evenals Engeland en Wales geen zelfstandige soevereine staten. De Britse parlementaire democratie wordt tot een van de oudste ter wereld gerekend, maar beschikt niet over een geschreven constitutie.[39] Het Britse parlement bestaat uit twee kamers, het Lagerhuis (*House of Commons*) en het Hogerhuis (*House of Lords*) en is de belangrijkste bron van geschreven recht (*Act of Parliament*) binnen het Verenigd Koninkrijk (Holdsworth, 2006, p. 2). Anders dan in Nederland zijn de ministers tevens lid van het parlement (*Members of Parlement*, MP). De koningin (of koning) is het staatshoofd maar bezit geen politieke macht. De regering (*Her Majesty's Government*) wordt geleid door een Prime Minister. Het Verenigd Koninkrijk is lid van de Raad van Europa sinds de oprichting (5 mei 1949) en heeft als eerste land het Europees Verdrag voor de Rechten van de Mens (EVRM) geratificeerd op 8 mei 1951.[40]

In paragraaf 9.1 komt allereerst het Engelse strafrechtsysteem aan de orde. Hier wordt kort ingegaan op de algemene trekken van het systeem en worden de overheidsorganen die te maken hebben met de telefoon- en internettap als opsporingsmiddel beschreven. In paragraaf 9.2 komt de praktijk van de telefoon- en internettap aan de orde. Hierin wordt het autorisatieproces, het gebruik van verkeersgegevens (gegevens *over* het telefoon- en internetverkeer), het gebruik van de telefoon- en de internettap en afluisterapparatuur en het gebruik van (tele)communicatiedata als bewijs besproken. In paragraaf 9.3 worden de waarborgen rond het gebruik van heimelijke opsporingsmiddelen beschreven. Dit deel wordt in paragraaf 9.4 afgesloten met een samenvatting van de belangrijkste punten.

9.1 Het Engelse strafrechtssysteem

9.1.1 Karakteristieken

Engeland en Wales, Schotland en Noord-Ierland hebben ieder hun eigen rechtstelsel. Het Engelse rechtssysteem, dat als het Common Law stelsel bij uitstek wordt gezien, heeft een eeuwenoude traditie van rechtsontwikkeling via rechtspraak en gewoonterecht (Spencer, 2002, p. 142 e.v.). In het Engelse systeem wordt geen uitdrukkelijk onderscheid gemaakt tussen publiekrecht en privaatrecht. Dit onderscheid wordt in Engeland traditioneel dan ook beschouwd als een continentale distinctie (Jurgens & Van Ommeren, 2009). Desondanks bestaat er wel een verdeling in burgerlijk (proces)recht en straf(proces)recht (Holdsworth, 2006, p. 15). Een wetboek van strafrecht en van strafprocesrecht, zoals dat gebruikelijk is binnen een Civil Law stelsel, kent het Engelse recht echter niet. Toch is tegenwoordig de belangrijkste rechtsbron van het Engelse strafprocesrecht de zogenaamde Acts of Parliament (wettenrecht) (Spencer, 2002, p. 143). Belangrijk om in dit verband te noemen is de Human Rights Act 1998 (HRA), die in 2000 in werking is getreden. Deze wet brengt het EVRM binnen de nationale Engelse rechtsorde en verplicht alle overheidsinstanties te handelen in overeenstemming met de regels van het EVRM. Alleen indien een Act of Parliament uitdrukkelijk bepaalt dat een dergelijke instantie niet in overeenstemming met het EVRM hoeft te handelen, mag hier van worden afgeweken (Section 6.2 HRA).

[38] Zie http://europa.eu/abc/european_countries/eu_members/unitedkingdom/index_en.htm. Het inwoners aantal van Engeland en Wales bedraagt ruim 50 miljoen.

[39] Gerekend vanaf de opstelling van de *Magna Carta* in 1215 als het beginpunt van de parlementaire democratie in het Verenigd Koninklijk.

[40] Het duurde vervolgens nog bijna zestig jaar voordat het EVRM onderdeel werd van het nationale Engelse recht.

Het Engelse strafproces wordt veelal aangeduid als een *adversarial* stelsel. Binnen de literatuur bestaat evenwel geen consensus over de inhoud van de term *adversarial* (zie bijvoorbeeld: Spencer, 2002, p. 5-27; Bleichrodt, Mevis & Volker, 2011, p. 14-48). Indien wordt uitgegaan van de volgende betekenis van adversarial, zijnde dat het gerecht of de (zittings)rechter geen onderzoek doet naar de (feitelijke) toedracht van het vermeend strafrechtelijk gebeuren, dan vallen drie aspecten op die kenmerkend zijn voor het Engelse strafproces in vergelijking met andere Europese stelsels (Spencer, 2002, p. 164). Ten eerste is dat de relatief passieve rol van de zittingsrechter in het Engelse strafproces. Het wordt niet gezien als een taak van de Engelse rechter om actief aan waarheidsvinding te doen, waar in Nederland, Frankrijk en Duitsland dit juist een centrale taak is van de strafrechter. Overigens kan de rechter buiten de procespartijen om wel vragen om (aanvullend) bewijs, indien de procespartijen dit hebben nagelaten. Een tweede aspect dat voortvloeit uit het eerste betreft de positie van de verdachte ter zitting. In Frankrijk, Duitsland en Nederland, neemt de ondervraging van de verdachte door de strafrechter een centrale rol in tijdens het onderzoek ter zitting. In Engeland is dat niet het geval, de zittingsrechter ondervraagt de verdachte niet en als de laatste besluit ter zitting geen verklaring af te leggen, kan hij door niemand worden ondervraagd. Als derde punt, ten slotte, lijkt in Engeland meer nadruk te liggen op het mondeling presenteren van bewijs ter zitting dan in bijvoorbeeld een land als Nederland (zie onder andere Spencer, 2002, p. 164). De gedachte die hier achter schuil gaat is dat de bron van het bewijs ter zitting moet worden gepresenteerd, hetgeen vaak inhoudt dat getuigen (en deskundigen) ter zitting worden gehoord en daar een verklaring afleggen (onmiddellijkheidsbeginsel).

9.1.2 Enkele organen binnen het Engelse strafrechtssysteem

Met betrekking tot het tappen van telefoon- en internetverkeer zijn in Engeland en Wales een aantal organisaties van belang. Hieronder volgt in alfabetische volgorde een korte omschrijving van de betreffende organen.

Crown Prosecution Service

Voor 1985 werden de meeste verdachten vervolgd door de politie, die zowel de rol van opsporings- als vervolgingsinstantie vervulde. Met de inwerkingtreding van de Prosecution of Offences Act 1985 is daar verandering in gekomen.[41] De politie bleef nog steeds de vervolgingsbeslissing nemen, maar droeg de zaak over aan de Crown Prosecution Service (CPS), zodra de politie besloot dat tot vervolging moest worden overgegaan. De CPS besliste vervolgens of de vervolging zou worden doorgezet of niet. Vanaf 2002 is daarin voor de CPS meer zeggenschap gekomen, toen naar aanleiding van de Lord Justice Auld's Review of the Criminal Courts 2002 de CPS geleidelijk aan steeds vaker is gaan bepalen wanneer wel of niet tot vervolging van strafbare feiten moet worden overgegaan.[42]
Zelfstandige bevoegdheden in de voorbereidingsfase (*preparatory phase*) van het strafproces zoals het opleggen van boetes of het op een andere wijze rechtstreeks aanspreken van de verdachte heeft de CPS niet. Er moet altijd via de politie of een gerecht gehandeld worden (Lewis, 2006, p. 154). Ook kan de CPS in specifieke strafzaken de politie niet aansturen in het doen van onderzoek.[43] Wel kan de CPS de politie verzoeken meer onderzoek te

41 Anders dan in Nederland waar het Openbaar Ministerie (OM) het vervolgingsmonopolie heeft, zijn er in Engeland (& Wales) meerdere instanties bevoegd tot het vervolgen van strafbare feiten. Naast de CPS was dat tot voorkort ook de Revenue and Customs Prosecution Office (RCPO). De RCPO was een non-departementaal openbaar lichaam gecreëerd onder de Commissioners for Revenue and Customs Act 2005 als een onafhankelijk orgaan voor de vervolging van strafbare feiten in Engeland, Wales en Noord-Ierland in zaken die voorheen tot de bevoegdheid van de Inland Revenue en HM Customs and Excise (de voorloper van Her Majesty's Revenue & Customs) behoorden. Op 1 januari 2010 is de RCPO samengevoegd met de CPS, waarbinnen een nieuwe Revenue and Customs Division is gevormd.

42 Zie de Criminal Justice Act 2003, zie nader Lewis (2006, p. 154-155).

43 Zoals dat wel in Nederland het geval is waar het OM, of beter gezegd, de officier van justitie (OvJ), juridisch leiding geeft aan een opsporingsonderzoek van de politie.

verrichten indien de CPS het aangeleverde bewijs in een bepaalde zaak (nog) onvoldoende vindt (Lewis, 2006, p. 159).
Daar staat echter tegenover dat de CPS richtlijnen opstelt en publiceert met betrekking tot hoe bewijs ter zitting moet worden gepresenteerd, bijvoorbeeld: met betrekking tot de visuele identificatie van een verdachte, over het gebruik van wetenschappelijk bewijs, hoe bekennende verklaringen moeten worden verkregen en over transcripties van bewijs. Overigens is het zo dat opbrengsten van het aftappen van telefoon en internet (in het Engels omschreven als *intercept*) ter zitting niet kunnen worden gebruikt als bewijsmiddel (bijvoorbeeld in de vorm van een tapverslag). In paragraaf 9.2.4 wordt hier nader op ingegaan.
De CPS is verdeeld in 13 verschillende districten in Engeland en Wales. Elk district wordt geleid door een Chief Crown Prosecutor (CCP) die verantwoordelijk is voor kwaliteit van de geleverde diensten van de CPS in het betreffende district.[44] Verder bestaan er binnen de CPS twee gespecialiseerde casework teams – de Central Fraude Group en de Serious Crime Group – die de vervolging van alle zaken die afkomstig zijn van de Serious Organised Crime Agency (SOCA), UK Borders Agency en Her Majesty's Revenue and Customs (HMRC) behandelen.[45] De CPS doet de procesvoering in strafzaken, maar ter zitting (*trial phase*) wordt de vervolgende overheid veelal vertegenwoordigd door een advocaat (prosecuting barrister of een sollicitor). Als sprake is van een minder ernstig delict wordt de strafzaak aangebracht bij de Magistrates' Court en berecht door (leken)rechters. Zwaardere delicten worden berecht door de Crown Court met een rechter en een jury (Holdsworth, 2006, p. 15).[46] In dat laatste geval heeft de jury een doorslaggevende stem in de beoordeling van het (toegelaten) bewijsmateriaal.

Her Majesty's Revenue and Customs
De Britse belastingdienst Her Majesty's Revenue and Customs (HMRC) in haar huidige vorm is een jonge organisatie die is opgericht op basis van de Commissioners for Revenue and Customs Act 2005 (CRCA 2005). Dit na een fusie tussen de Inland Revenue en HM Customs and Excise Departments.[47] Naast het innen van belastingen houdt HMRC zich bezig met rechtshandhavingstaken en het opsporen van zogenaamde Serious Organised Fiscal Crime. Opsporingsambtenaren van HMRC hebben ruime bevoegdheden voor het toepassen van dwangmiddelen zoals aanhouding, binnentreding, huiszoeking en het detineren van personen die verdacht worden van strafbare feiten genoemd in de Customs and Excise Acts.[48] Bij de vervolging van strafbare feiten wordt samengewerkt met de politie en de Revenue and Customs Division van de CPS.

Police
De meeste (vermeende) strafbare feiten worden in Engeland en Wales onderzocht door de politie. De politie in Engeland en Wales verschilt qua organisatie en bevoegdheden sterk met de politie in Nederland en andere Europese landen. Hoewel de politie onder de verantwoordelijkheid van de Home Secretary valt, heeft deze geen directe juridische mogelijkheden om de politie te vertellen wat ze moet doen. Wel kan de Home Secretary de politiekorpsen via zogenaamde Home Office Circulairs aansturen. Dit maakt de Engelse politie als geheel tot een vrij onafhankelijke organisatie. Binnen Engeland en Wales bestaan 43 locale politiekorpsen. Elk politiekorps wordt op basis van de Police Act 1996 en de Police Reform Act 2002, geleid door een Chief Constable, een locale Police Authority en de Home Office. Deze driekoppige leiding is verantwoordelijk voor het algemene politie- en het opsporingsbeleid (Stelfox, 2009, p. 178-180; Spencer, 2002, p. 150).

44 Aan het einde van maart 2010 werkten bij de CPS in totaal 8.316 mensen. Ongeveer 35% daarvan is gekwalificeerd prosecutor. Zie http://www.cps.gov.uk/.
45 Her Majesty's Revenue and Customs (HMRC) en de Serious Organised Crime Agency (SOCA) worden hieronder behandeld.
46 Zie ook paragraaf 9.1.3.
47 De O'Donnell review of the Revenue Departments, gepubliseerd in maart 2004 adviseerde een fusie tussen de Inland Revenue en HM Customs and Excise om te komen tot HM Revenue and Customs. Dit nieuwe departement is op 18 april 2005 in het leven geroepen.
48 Zie Section 138 Customs and Excise Management Act 1979 (c. 2).

Anders dan in bijvoorbeeld Nederland kent de Engelse politie geen specifieke afdelingen die belast zijn met bijvoorbeeld opsporingsonderzoek naar strafbare feiten, zoals de recherche in Nederland. In het opsporingsonderzoek heeft de Engelse politie een zeer zelfstandige rol. Er is geen openbaar aanklager noch een onderzoeksrechter die de politie feitelijk of juridisch aanstuurt. Tot enkele jaren terug besliste de politie ook zelf over de vervolging van de verdachte. Dat is inmiddels veranderd door de steeds nadrukkelijkere rol die de CPS heeft gekregen met betrekking tot de vervolgingsbeslissing in strafzaken. Wel heeft de politie de bevoegdheid om zaken te seponeren, waarschuwingen (C*autions*) uit te delen eventueel gepaard met voorwaarden (C*onditional Cautions*) danwel boetes op te leggen aan de verdachte (zoals *Fixed Penalty Notices* en *Penalty Notices for Disorder*).[49] In al deze gevallen wordt een zaak dan niet voorgelegd aan de (straf)rechter.[50]
In 1984 zijn de opsporingsbevoegdheden van de politie verruimd met de inwerkingtreding van de Police and Criminal Evidence Act (PACE 1984). Zo was het voor invoering van de PACE 1984 voor de politie niet mogelijk om een verdachte aan te houden voor verhoor (*arrest*), zonder dat er voldoende bewijs was om een aanklacht in te dienen. Dat is sinds 1984 wel mogelijk. Verder is met de invoering van de PACE 1984 het op audio-band opnemen van de verhoren van de verdachte verplicht gesteld. Daar is in 2001, met de invoering van de Criminal Justice and Police Act, de mogelijkheid bijgekomen om de verhoren van de verdachte met video op te nemen, indien de Home Secretary dat wenselijk acht.

Serious Organised Crime Agency
De Serious Organised Crime Agency (SOCA) is een non-departementaal openbaar lichaam en valt onder de verantwoordelijkheid van de Home Office.[51] De belangrijkste functies van SOCA zijn neergelegd in de Serious Organised Crime and Police Act 2005 (SOCAP 2005). Volgens Section 93.4 van de Police Act 1997 vallen verschillende soorten gedragingen onder de term zware criminaliteit (serious crime). Dat kan zijn het gebruik van geweld, crimineel substantieel financieel gewin, de uitoefening van een gemeenschappelijk crimineel doel, maar het kan ook betrekking hebben op een delict, begaan door een persoon ouder dan 21 jaar, waarop een gevangenisstraf van 3 jaar of meer is gesteld. De betrokkenheid van de SOCA is dan gericht op onder andere het voorkomen, opsporen en bijdragen aan de vermindering van deze zware (georganiseerde) criminaliteit, zoals drugsdelicten, mensensmokkel en mensenhandel, wapenhandel, fraude, computercriminaliteit en het witwassen van geld te bestrijden en op te sporen. In dat kader is de SOCA bevoegd om telefoon en internetverkeer te onderscheppen. Anders dan de politie, die is opgedeeld in regionale korpsen, is de SOCA één organisatie die werkzaam is in het gehele Verenigd Koninkrijk.[52] SOCA opereert echter niet alleen, maar ondersteunt en werkt samen met andere opsporingsdiensten binnen de strafrechtspleging, zoals de politie, HMRC en de United Kingdom Border Agency (UKBA). Hiervoor is een platform in het leven geroepen, genaamd de Organised Crime Partnership Board, om de coördinatie tussen de UKBA, HMRC en de Association of Chief Police Officers zo optimaal mogelijk te maken.
SOCA-functionarissen kunnen beschikken over de (gecombineerde) bevoegdheden van politie, douane en immigratie-officieren. SOCA is verdeeld in drie zogenaamde core business groepen: Strategy and Prevention, Operational Capability en Capability and Service Delivery.[53] Elke groep wordt geleid door een uitvoerend directeur en is gespecialiseerd in

49 *Fixed Penalty Notices* zijn boetes voor verkeersovertredingen en fout parkeren. *Penalty Notices for Disorder*, geïntroduceerd bij de inwerkingtreding van de *Criminal Justice and Police Act 2001*, zijn boetes die de politie direct kan opleggen en bedoeld om verstoring van de openbare orde aan te pakken. Zie ook Lewis (2006, p. 168).
50 In de jaren 90 is er een wettelijke grondslag gekomen voor het uitdelen van (C*onditional*) *Cautions* door de Engelse politie. Daarvoor deed de politie dit puur op basis van de ruime discretionaire bevoegdheid met betrekking tot de vervolgingsbeslissing (Lewis, 2006, p. 167).
51 Zie http://www.soca.gov.uk/. SOCA wordt gefinancierd door, en rapporteert aan de Home Secretary en staat onder leiding van een bestuur met een meerderheid van niet-uitvoerende leden. Bij de SOCA werken (momenteel) rond 3.700 mensen (voltijds dienstverband), die opereren vanuit bijna 50 vestigingen in het Verenigd Koninkrijk en nog eens 40 vestigingen in het buitenland.
52 Aldus een respondent van de SOCA.
53 Zie http://www.soca.gov.uk/.

specifieke aspecten van het werk. In de praktijk komen medewerkers van alle drie de groepen samen in multidisciplinaire teams om bepaalde problemen aan te pakken of operationele taken uit te voeren.

9.1.3 Fasen in het strafproces

In het Engelse strafproces zijn drie opeenvolgende fasen te onderscheiden. De voorbereidingsfase (*Preparatory phase*) die start bij de opsporing en eindigt bij de vervolgingsbeslissing, de tussenfase (*Intermediate phase*) die loopt van de vervolgingsbeslissing tot de aanvang van het rechtsgeding en tenslotte de strafzitting (*Trial phase*).

Preparatory phase
De opsporing van (vermeend) strafbare feiten is de taak van de politie. Daarnaast zijn er evenals in Nederland ook bijzondere opsporingsdiensten, zoals HMRC, die zich richten op de opsporing van speciale soorten delicten, zoals belastingfraude. In de opsporing opereert de politie grotendeels zelfstandig. De politie wordt niet aangestuurd door de openbaar aanklager zoals dat formeel in Nederland wel het geval is. Bij de opsporing van ernstige misdrijven maakt de politie of een bijzondere opsporingsdienst gebruik van dwangmiddelen, zoals huiszoeking, voorarrest en de telefoontap.
Wanneer de opsporing zijn einde nadert, moet worden beslist over de vervolgstap. Afhankelijk van de mate van succes van de opsporing kan dat betekenen dat de zaak wordt overgedragen aan de CPS die sinds 2002 beslist over de vervolgingsvraag en de eventuele strafeis.[54] Een tweede mogelijkheid is dat de zaak wordt geseponeerd (take no further action, 'NFO') door de politie of een bijzondere opsporingsdienst. Voor de politie is er geen mogelijkheid om voorwaardelijk te seponeren, dat wil zeggen, een afspraak met de verdachte maken over bijvoorbeeld het betalen van een geldboete waardoor de zaak niet verder wordt vervolgd. Een aantal bijzondere opsporingsdiensten zoals de HMRC hebben deze mogelijkheid tot voorwaardelijk seponeren echter wel.[55] Ten slotte heeft de politie wel de mogelijkheid om een verdachte een formele waarschuwing (*Caustion*) te geven of, in het geval van lichtere verkeersdelicten, een zogenaamde *fixed penalty notice*. Bij een veroordeling kan de rechter bij de hoogte van de straf wel rekening houden met een eerdere waarschuwing(en) gegeven door de politie.
Indien de CPS de strafzaak heeft overgenomen en een beslissing neemt over het al dan vervolgen van de verdachte, worden de richtlijnen van de Code of Practice for Crown Prosecutors gevolgd.[56] Wanneer wordt besloten de vervolging niet voort te zetten wordt doorgaans een notice of discontinuance gestuurd naar het gerecht waar de zaak anders zou hebben gediend (Section 23 Prosecution of Offences Act 1985 (POA 1985)).[57] De verdachte heeft overigens het recht om voortzetting van de vervolging te verlangen (Section 23.7 POA 1985). De CPS heeft ook nog andere mogelijkheden om een vervolging te stoppen, zoals het niet produceren van bewijsmateriaal ter zitting of de rechter vragen uit te spreken dat de vervolging moet worden gestaakt (Spencer, 2002, p. 170-171).

Intermediate phase
Zoals hierboven aangegeven loopt de tussenfase van de vervolgingsbeslissing tot de aanvang van het rechtsgeding. Als voor (verdere) vervolging wordt gekozen eindigt formeel gesproken de opsporing. Bovendien verandert de status van de verdachte van suspect naar defendant. De autoriteiten zijn dan in beginsel niet langer gerechtigd om de verdachte nog te ondervragen (Spencer, 2002, p. 175).

54 Zie ook de vorige paragraaf over de Crown Prosecution Service (CPS).
55 Zie de Customs and Excise Management Act 1979, Section 138 e.v.
56 Zie http://www.cps.gov.uk/publications/code_for_crown_prosecutors/.
57 Bij een zogenaamd summary offence of een either-way offence die bij de Magistrates' Court wordt aangebracht kan dit tot aan het moment dat het bewijs in de strafzaak op de zitting wordt gepresenteerd (zie Sections 23(2) en 23A POA 1985). Bij een zaak die voor de Crown Court dient, heeft de CPS de mogelijkheid om (toch) niet verder te vervolgen tot aan het moment dat de zaak *has been sent for trial*.

Belangrijk in deze fase is de zogenaamde 'mode of trial', waarin wordt gekozen voor welk gerecht de strafzaak moet worden aangebracht. Het Engelse recht verdeelt hierbij delicten in lichter strafbare feiten (*Summary Offences*) die worden aangebracht bij de Magistrates' Court, zwaardere strafbare feiten (*Indictable Offences*) die worden berecht door de Crown Court en *Either-way Offences*, die of door de Magistrates' Court of de Crown Court worden berecht (Spencer, 2002, p. 171). Ook worden in deze fase door de rechter beslissingen genomen over voorarrest of bail voor de verdachte.
Oorspronkelijk ging het Engelse recht er van uit dat geen van beide procespartijen (de vervolgende instantie en de verdediging) de bewijsmiddelen voor aanvang van de trial phase hoefde prijs te geven, waardoor de tegenpartij ter zitting kon worden overvallen met bepaalde bewijsstukken. In de jaren tachtig van de vorige eeuw is aan die wijze van procesvoering een einde gekomen (Spencer, 2002, p. 175-177). Mede op basis van artikel 6 EVRM moet de vervolgende autoriteit (CPS) thans al het verzamelde bewijsmateriaal waar de vervolging op gefundeerd is onthullen aan de verdediging (disclosure of evidence). Ook niet gebruikt materiaal (bijvoorbeeld afgetapte telefoongesprekken) dat ontlastend is voor de verdachte moet worden onthuld (exculpatory material). In het Engelse recht[58] is dit geregeld in de Criminal Procedure and Investigations Act 1996 (CPIA 1996). Doorgaans lijkt de intermediate phase het aangewezen moment voor disclosure of evidence.[59] De disclosure blijkt evenwel geen absoluut recht te zijn. Zo heeft the House of Lords bepaald dat dergelijk exculpatory material "can be withheld by virtue of Public Interest Immunity (PII) if there is an important countervailing public interest, non-disclosure is strictly necessary to protect this interest, and any difficulty caused to the defence can be sufficiently counterbalanced to ensure a fair trial".[60] Deze omstandigheden kunnen zich voordoen bij het aftappen van telefoon- en internetverkeer.

Trial phase
Uiteindelijk kan een strafzaak worden aangebracht bij de Crown Court of bij de Magistrates' Court.[61] Tussen de beide gerechten bestaan een aantal verschillen in de behandeling van een strafzaak. Zo wordt in het geval van een 'not guilty plea' de zaak in een Crown Court behandeld ten overstaande van een jury. De Magistrates' Court bestaat, door de bank genomen, uit lekenrechters, zowel bij een guilty als bij een not guilty plea (Spencer, 2002, p. 178). Verder is de behandeling van de strafzaak bij een Magistrates' Court minder formeel dan bij de Crown Court en zijn er minder momenten in de procedure ingebouwd voor de beide procespartijen om hun zaak te bepleiten dan bij de Crown Court.

9.2 De telefoon- en internettap in de praktijk

Zoals hierboven aangeven vindt de opsporing van (vermeende) strafbare feiten plaats in de eerste fase (*preparatory phase*) van het strafproces. In deze paragraaf staat het gebruik van de telefoon- en internettap tijdens de opsporing centraal. Naast de regelgeving wordt hier de praktijk van het aftappen belicht, zoals dat uit rapportages en interviews naar voren is gekomen. De bespreking is chronologisch van opzet.
De interceptie (*interception*) van communicatie (telefoon- en internetverkeer) wordt in het Verenigd Koninkrijk geregeld in de Regulation of Investigatory Powers Act 2000 (RIPA 2000). In hoofdstuk 23 van de RIPA 2000 worden de bevoegdheden en verplichtingen rond het onderscheppen en afluisteren van alle vormen van communicatie, waaronder internet- en telecommunicatie, vastgelegd. Daarnaast geeft de Home Office in een Code of Practice betreffende Interception of Communications nadere procedures en regels die moeten worden

58 In Schotland is een ander systeem van toepassing, zie Privy Council Review of Intercept as Evidence 2008, p. 42-43.
59 Vergelijk Spencer (2002, p. 175-177).
60 Zie *RvH: RvC* (2004) 2 AC 134, (2004) HRLR20; zie ook Hopkins, 2009*b*, p. 80. Formulering in hoofdtekst is afkomstig van de Privy Council Review of Intercept as Evidence 2008, p. 42-43.
61 Zie Jehle (2006, p. 13) voor een vereenvoudigde schematische weergave van het strafrechtssysteem van Engeland en Wales.

gevolgd voordat een interceptie van communicatie kan worden uitgevoerd (Section 1.1 van genoemde Code of Practice).

9.2.1 Het tapbevel en het autorisatieproces

Een tapbevel wordt in Engeland en Wales niet toegekend door een onafhankelijke instantie zoals een rechter(-commissaris), maar door een Secretary of State. De werkzaamheden en beslissingen van de Home Office, de Secretary of State en de instanties die de intercepties aanvragen en uitvoeren, worden gecontroleerd door de Interception of Communications Commissioner. Dit is een hoge rechter die voor de uitvoering van deze controletaken is aangesteld door de Prime Minister (Section 57 RIPA 2000). Elk jaar rapporteert de Commissioner aan het Britse parlement over de wijze waarop met de wettelijke bevoegdheden in de praktijk wordt omgegaan door de politie en door andere bevoegde instanties.[62] Ook kan een burger naar het zogenaamde Investigatory Powers Tribunal (IPT) om te klagen over (vermeend onrechtmatig) overheidshandelen, zoals bijvoorbeeld onrechtmatig aftappen van telefoongesprekken.[63]
Alvorens een tapbevel voor ondertekening wordt aangeboden aan een Secretary of State doorloopt een tapaanvraag een aantal stadia in een autorisatieproces (Interception of Communications Commissioner, 2011, p. 10). Hieronder wordt nader op die stadia ingegaan.[64]
De instantie die de tapaanvraag indient, doet zelf een eerste proportionaliteits- en subsidiariteitstoets. In dit verband werd door een respondent van de Home Office (vanuit het gezichtpunt van een opsporingsambtenaar) het volgende naar voren gebracht:

> "We have to satisfy the Home Secretary, who signs the warrants that we are not just doing this because it's easy for the investigators to have intercept. It is because we have tried other things, we have tried everything we can to get to the point where we have gathered evidence or opportunities to gather evidence and it is not working, we are not getting the evidence. But we also have to show that using intercept will actually help us gain evidence in another format." – Home Office

Verder stelt deze respondent dat een tapaanvraag soms binnen de hiërarchische kolom een aantal keer op en neer gaat, voordat de aanvraag op het bureau van de Home Secretary belandt.

62 De Commissioner heeft in 2009 en in 2010 de volgende instanties die betrokken zijn bij de interceptie van telefoon- en internetverkeer bezocht: Secret Service, Secret Intelligence Service (SIS), Government Communications Headquarters (GCHQ), SOCA, Metropolitan Police Counter Terrorism Command, Police Service of Northern Ireland, Northern Ireland Office, HMRC, Foreign and Commonwealth Office (FCO), Home Office, Scottisch Government en Ministry of Defence. Zie Interception of Communications Commissioner, 2010, p. 2 en Interception of Communications Commissioner, 2011, p. 11. Alleen in 2009 heeft de Commissioner ook nog de Strahclyde Police bezocht.

63 Zie nader paragraaf 8.3.

64 Het instellen van een Covert Human Intelligence Source (CHIS) is, evenals bij het autorisatieproces bij de telefoon- of internettap, gebaseerd op de RIPA 2000. De autorisatie beambte (*authorising officer*) is bij de inzet van een CHIS evenwel (in beginsel) *niet* de Secretary of State (zie Section 5.1 e.v. van de Covert Human Intelligence Sources Code of Practice), maar een beambte lager in de organisatie. Bij Intrusive Surveillance (IS), bijvoorbeeld afluisterapparatuur, blijkt de Secretary of State de autorisatie af te geven als het gaat om aanvragen door de Intelligence Services of bijvoorbeeld het Ministerie van Defensie. In andere gevallen wordt de autorisatie gedaan door een *senior authorising officer* of door bijvoorbeeld een daartoe aangewezen aangewezen deputy of the police, SOCA of HMRC (vergelijk Section 32(6) and 34(6) RIPA 2000). Zie Section 6.1 e.v. van de Revised Code of Practice inzake Covert Surveillance and Property Interference. Opmerkelijk is dat voor al deze drie heimelijke opsporingsmethoden verschillende autorisatieregimes bestaan, waarbij de procedure rond de aanvraag van een telefoon- of internettap het zwaarst is opgetuigd. Hiermee lijkt een bepaalde rangorde te zijn gegeven aan de mate van inbreuk op de persoonlijke levenssfeer van een burger. Op de CHIS en de IS wordt hieronder, onder het kopje *Intrusive Surveillance en Covert Human Intelligence Sources*, verder ingegaan.

> "I think the process that the warrant application has to go through from the investigator to get from the intercept up to it actually going from the agency to the Home Secretary. That is such a regular process and the people who are putting these applications through are at a very senior level, they know what standard they have to get before it leaves the agency. And it's likely to perhaps go up the chain and come back down once or twice, more likely to do that than to go to the Home Office and come back." – Home Office

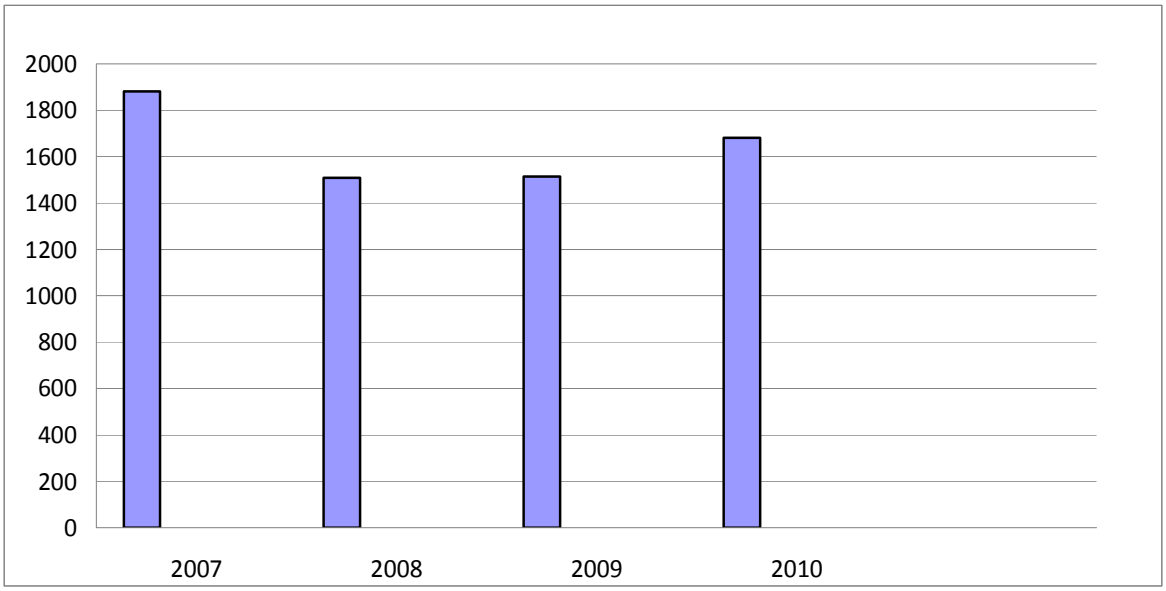
Vervolgens wordt de aanvraag doorgestuurd naar het verantwoordelijke ministerie (Sponsor Government Department). De SOCA, HMRC, de Security Service en een gedeelte van de Metropolitan Police, moeten hun tapaanvraag sturen naar de Home Office. Daar worden de aanvragen getoetst aan de criteria van de RIPA 2000.[65]
Een tapbevel kan alleen worden afgegeven indien het valt binnen een of meerdere van de volgende drie doelen: de belangen van nationale veiligheid, voorkoming of opsporen van zware criminaliteit en het veilig stellen van het economisch welzijn van het Verenigd Koninkrijk (Section 5.3 RIPA 2000).[66] Daarnaast wordt ook gekeken of sprake is van een 'justifiable interference with an individual's right under Article 8 of the European Convention of Human Rights (the right to privacy) if it is necessary and proportionate for the interception to take place' (Section 2.4 Code of Practice).[67] In paragraaf 9.3 wordt nader ingegaan op inbreuken op en waarborgen van het recht op privacy.
Een tapbevel betreft steeds één persoon of één woning (premises) (Section 8.1 RIPA 2000). De af te luisteren persoon hoeft overigens niet altijd een verdachte te zijn. In het geval dat het gaat om de nationale veiligheid blijkt het ook vaak personen te betreffen die nimmer voor een rechter zullen verschijnen. Bij de afweging voor het verlenen van een tapbevel wordt gekeken of de betreffende persoon een significante rol heeft binnen een bepaalde (criminele) organisatie of dat hij individueel handelt. Vervolgens wordt gekeken in hoeverre een tap de privacy van derden niet te veel binnendringt (collateral intrusion).[68]
Indien aan de bovenstaande criteria is voldaan wordt de aanvraag, voorzien van (eventuele) opmerkingen van een hogere ambtenaar (senior official)[69] over mogelijke risico's en juridische aspecten, voorgelegd aan de betreffende Secretary of State. Zoals hierboven reeds is aangegeven is dat, bij de behandeling van de aanvragen door de Home Office, doorgaans de Home Secretary.
Uiteindelijk komt de aanvraag bij de Secretary of State. Alvorens te tekenen kan deze verzoeken om meer informatie. Indien tevreden met de beoordeling van de aanvraag door zijn ambtenaren, ondertekent hij een tapbevel voor een periode van drie maanden. Daarna, afhankelijk van het doel waarvoor de tap wordt ingezet kan een bevel drie maanden (bij zware criminaliteit) of zes maanden (bij nationale veiligheid of economisch welzijn) worden verlengd (Section 9 RIPA 2000 en Section 2.11 Code of Practice). Ook in dat geval ondertekent de betreffende Secretary of State.[70] Met betrekking tot het toekennen van tapbevelen wijst de Commissioner in 2009 op het volgende:

> "Outright and final refusal of an application is comparatively rare, because the requesting agencies and the senior officials in the Secretary of State's Department scrutinise the applications with care before they are submitted for approval. However, the Secretary of State may refuse to grant the warrant if he or she considers, for example, that the strict requirements of necessity and proportionality are not met. The agencies are well aware that the Secretary of State does not act as a 'rubber stamp'" (Interception of Communications Commissioner, 2010, p. 3).

65 Aldus blijkt uit het interview met een respondent van de Home Office.
66 Onder zware criminaliteit (*serious crime*) moet onder andere worden verstaan: in- en uitvervoer van drugs, fraude, mensenhandel, vuurwapendelicten, geweld, computercriminaliteit en kidnapping (zie RIPA 2000).
67 Overigens kan een tapbevel worden gebruikt voor zowel het telefoon- en internetverkeer als voor opgeslagen communicatie, zie Section 2.14 van de Code of Practice.
68 *Idem*.
69 Een dergelijke senior official van de Home Office is ook geïnterviewd.
70 Aldus een respondent van de Home Office.

In Grafiek 1 is voor de periode van 2007 tot en met 2010 een overzicht gegeven van het aantal uitgegeven tapbevelen afkomstig van de Home Secretary.

Grafiek 1 Aantallen uitgegeven tapbevelen



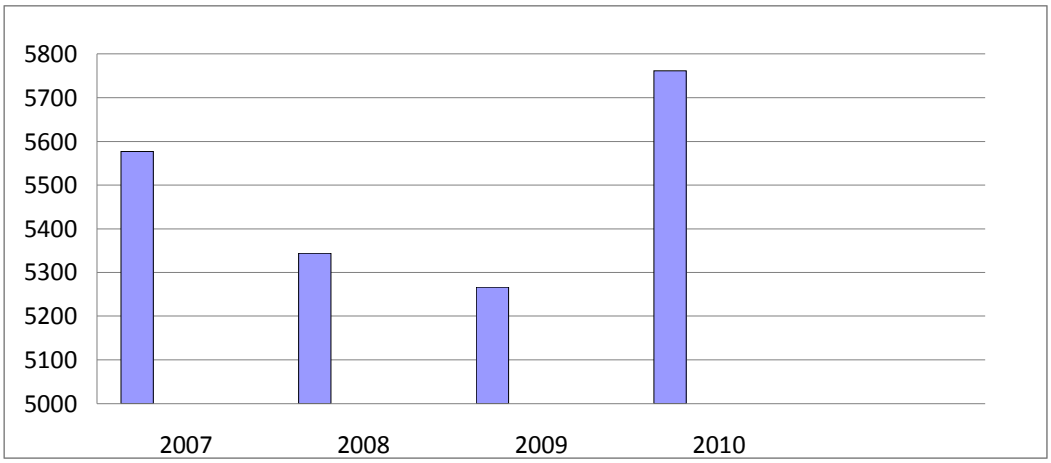
Bronnen: Reports of the Interception of Communications Commissioner 2007 t/m 2010

In 2007 betrof het aantal uitgegeven tapbevelen 1.881. Het jaar daarop (2008) was dat aantal gedaald tot 1.505. Daarna is de uitgifte van tapbevelen gestegen van 1.514 (2009) naar 1.682 in 2010. De stijging van 1.514 (2009) naar 1.682 (2010) bedraagt ruim 10%. Deze laatste stijging wordt verklaard door een groei in het aantal gevallen van zware criminaliteit en bedreigingen van de nationale veiligheid van het Verenigd Koninkrijk (Interception of Communications Commissioner, 2011, p. 18). In het algemeen valt het geringe aantal tapbevelen dat in de periode 2007-2010 jaarlijks wordt afgegeven in het oog. Hierbij moet worden opgemerkt dat het bevelen betreft op personen, en niet op nummers. Aanvragen voor aanpassingen (modifications) in een bestaand tapbevel, die bijvoorbeeld moeten worden doorgevoerd omdat de getapte persoon van nummer of toestel wisselt, hoeven niet altijd langs de Secretaty of State, maar kunnen in sommige gevallen door een senior official (van de Home Office) worden beoordeeld (Section 10 RIPA 2000).[71] Wijzigingen hebben overigens geen invloed op lengte van de taptermijn (Section 2.12 Code of Practice).

Grafiek 2 toont het totaal aantal aanpassingen op van kracht zijnde tapbevelen voor de periode 2007 tot en met 2010.

[71] Aldus ook een respondent van de Home Office.

Grafiek 2 Aantallen aanpassingen op van kracht zijnde tapbevelen



Bronnen: Reports of the Interception of Communications Commissioner 2007 t/m 2010

In 2007 zijn in totaal 5.577 aanpassingen gepleegd op bestaande tapbevelen. Dat is in 2008 teruggelopen tot 5.344 en die trend is doorgezet in 2009 toen 5.267 aanpassingen zijn gedaan. In 2010 zijn het aantal aanpassingen 5.761 geweest hetgeen een toename ten opzichte van het jaar ervoor is van ruim 9%. Een verklaring voor de recente stijging in aantallen aanpassingen wordt niet gegeven door de Commissioner, maar deze stijging komt overeen met de stijging die te zien was in het aantal afgegeven tapbevelen in de genoemde periode en die werd toegeschreven aan de groei in het aantal gevallen van zware criminaliteit en bedreigingen van de nationale veiligheid van het Verenigd Koninkrijk in deze periode.

Intrusive Surveillance en Covert Human Intelligence Sources
Naast de telefoon- en internettap bestaan er andere heimelijke opsporingsmethoden, die als mogelijke alternatieven (kunnen) dienen voor de inzet van met name de telefoontap. Één daarvan is de zogenaamde Intrusive Surveillance (IS). Hieronder kan volgens de Revised Code of Practice (RCoP) inzake Covert Surveillance and Property Interference[72] ook afluisterapparatuur worden verstaan. In Section 2.11 van RCoP staat IS omschreven als een "covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a *surveillance device* [*cursivering toegevoegd*]."[73] Daarnaast zijn er de Covert Human Intelligence Sources (CHIS). Een CHIS is iemand die een persoonlijke of andersoortige relatie aangaat met een persoon met als doel, zonder dat laatst genoemde persoon dat weet, het verkrijgen of openbaar maken van informatie of het voor een andere persoon toegankelijk maken van informatie.[74] Een undercovertraject voldoet alleen aan deze omschrijving indien er sprake is van een min of

[72] De Revised Code of Practice inzake Covert Surveillance and Property Interference is gebaseerd op Section 71 van de RIPA 2000.

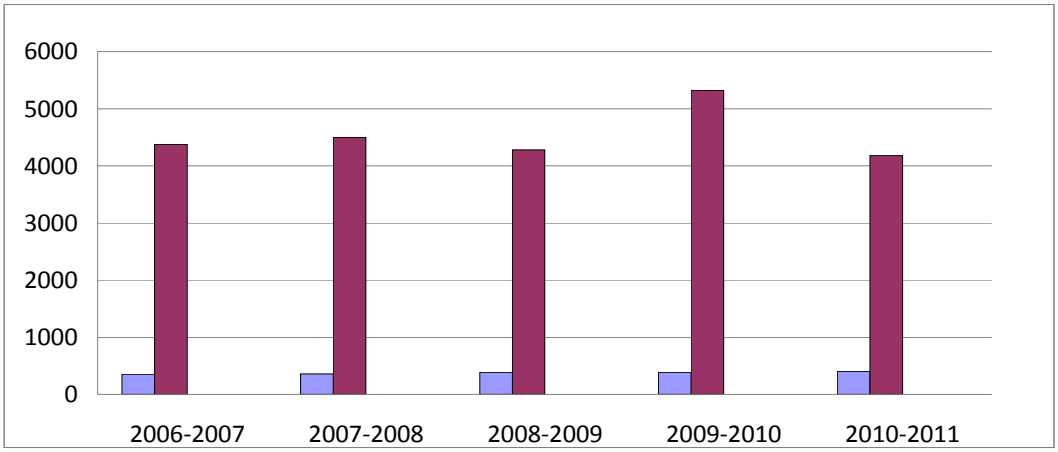
[73] In Section 2.12 wordt daar aan toegevoegd: "The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained. In addition, surveillance under the ambit of the 2010 Order is to be treated as intrusive surveillance. Accordingly, it is not necessary to consider whether or not intrusive surveillance is likely to result in the obtaining of *private information*."

[74] Zie Covert Human Intelligence Sources Code of Practice (CHIS CoP), Section 2.1 waar staat dat een CHIS iemand is die: "(a) establishes or maintains a personal or other relationship with *a person* [*cursivering toegevoegd*] for the covert purpose of facilitating the doing of anything falling within paragraph b) or c); (b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or (c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship." Ook deze CoP is gebaseerd op Section 71 van de RIPA 2000. Zie ook Section 26.8 RIPA 2000. Uit de tekst blijkt dat de subjecten waar een undercovertraject zich op richt niet noodzakelijkerwijs steeds een verdachte hoeft te zijn.

meer bestendige relatie tussen de undercover agent en een burger.[75] Dit betekent dat bijvoorbeeld een eenmalige pseudo-koop of het eenmalig inzetten van een lokmiddel niet valt onder de werking van de RIPA 2000 of de CHIS CoP. De resultaten van het inzetten van IS en van CHIS kunnen als bewijs in een strafzaak worden gebruikt.[76]
Hoewel de RIPA 2000 de mogelijkheid biedt om CHIS te gebruiken voor het voorkomen en opsporen van alle strafbare feiten (zie Section 29.3 sub *b* RIPA 2000), blijken CHIS doorgaans alleen te worden ingezet wanneer het gaat om *serious crime* (Kruisbergen & De Jong, 2010, p. 108).[77] Undercovertrajecten worden in Engeland klaarblijkelijk als een relatief zwaar middel beschouwd, waardoor in de regel eerst gekeken wordt of met de inzet van lichtere opsporingsmiddelen kan worden volstaan (Kruisbergen & De Jong, 2010, p. 108.).[78] Een uitzondering op deze werkwijze wordt gemaakt door de SOCA die al in een vroeg stadium undercovertrajecten toepast om informatie te verkrijgen over de organisatie en werkwijze van criminele groepen (Kruisbergen & De Jong, 2010, p. 108).

Jaarlijks worden cijfers omtrent (ondermeer) geautoriseerde IS en ingezette CHIS gepubliceerd door de Chief Surveillance Commissioner. Hieronder in Grafiek 3 worden de cijfers over de periode 2006 tot en met 2011 weergegeven.

Grafiek 3 Aantallen geautoriseerde IS (*grijs*) en ingezette CHIS (*zwart*)



Bronnen: Annual Reports of the Chief Surveillance Commissioner voor 2006-2007, 2007-2008, 2008-2009, 2009-2010 en 2010-2011.

In het tijdsvak 1 april 2006 tot en met 31 maart 2007 waren 4.373 CHIS ingezet (recruited) door law enforcement agencies en 350 IS geautoriseerd. De periode erna (april 2007 tot en met maart 2008) betreft het 4.498 ingezette CHIS en 355 IS. Van 1 april 2008 tot en met 31 maart 2009 gaat het om 4.278 ingezette CHIS en 384 geautoriseerde IS. In de periode van 1 april 2009 tot en met 31 maart 2010 zijn 5.320 CHIS ingesteld en 384 IS. Uit deze cijfers valt te concluderen dat het aantal ingestelde CHIS ver uitsteekt boven de aantallen IS in dezelfde periode. Bovendien blijkt het aantal ingezette CHIS ook beduidend hoger te liggen dan het aantal afgegeven tapbevelen van rond dezelfde periode (vergelijk Grafiek 1). De

75 Bij undercovertrajecten in Engeland (en Wales) kunnen zowel undercoveragenten als burger infiltranten worden ingezet (zie Section 4.2 CHIS CoP).

76 Zie Section 9.1 van de Revised Code of Practice inzake Covert Surveillance and Property (IS) en Section 8.7 van de Covert Human Intelligence Sources Code of Practice (CHIS).

77 Onder *serious crime* (zie ook hierboven) moet onder andere worden verstaan: in- en uitvervoer van drugs, fraude, mensenhandel, vuurwapendelicten, geweld, computercriminaliteit en kidnapping (zie RIPA 2000).

78 Zo wordt bijvoorbeeld in een beleidsdocument van de lokale overheid van London aangegeven dat de Greater London Authority (GLA) "envisages that it will use both covert directed surveillance and covert human intelligence sources only in the most exceptional circumstances. Investigations requiring the use of covert directed surveillance or covert human intelligence sources may only be undertaken by officers of the Internal Audit Division or by specialist investigators engaged by the Authority." Zie (Section 8) http://legacy.london.gov.uk/about/corp-gov/docs/ripa-policy.pdf.

aantallen IS (waaronder afluisterapparatuur) blijft evenwel achter bij de aantallen telefoon- en internettaps. Hieruit volgt dat van de drie heimelijke opsporingsmethoden, de telefoon- en internettap, IS en CHIS, de laatst genoemde volgens de statistieken verreweg het meest gebruikt is in de afgelopen jaren. Dat is, gezien de zwaarte van het opsporingsmiddel, een opmerkelijke uitkomst.

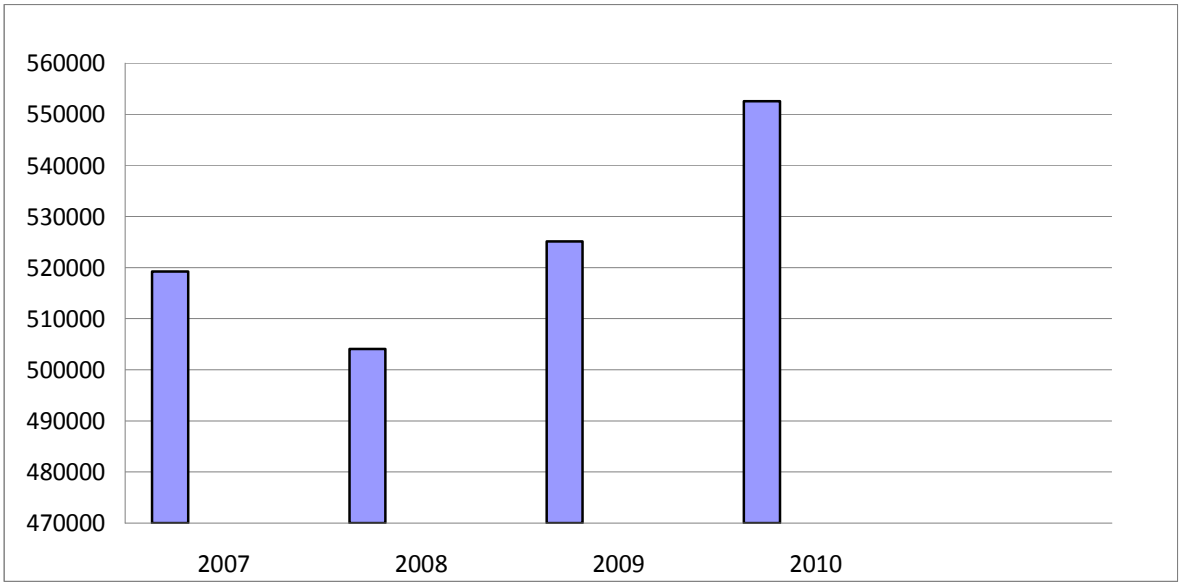
9.2.2 Verzoeken om gebruik te maken van abonnee- en verkeergegevens

Naast het gebruik van de inhoud van telefoongesprekken of van het gebruik van internet, kunnen ook de gegevens *over* het telefoon- en internetverkeer van belang zijn voor de opsporing van strafbare feiten. Deze gegevens worden aangeduid als abonnee- (*subscriber data*)[79] en verkeersgegevens (*traffic data*). Onder verkeersgegevens vallen onder andere de gebruikersgegevens, datum en tijdstip van de verbinding en locatiegegevens tijdens de verbinding. Een groot aantal instanties binnen het Verenigd Koninkrijk is bevoegd deze gegevens te verwerven en te gebruiken (zie hoofdstuk II Deel I van de RIPA 2000).[80] Daartoe wenden zij zich tot de Communication Service Providers (CSP) die een rechtmatig verzoek van een dergelijke aanvrager moet inwilligen. Onder de aanvragers behoren de 43 politiekorpsen in Engeland en Wales, SOCA en HMRC.[81]
Ook het gebruik van abonnee- en verkeergegevens is een inbreuk op iemands persoonlijke levenssfeer en zal daarom moeten voldoen aan de eisen gesteld in artikel 8 lid 2 EVRM.[82] Om hieraan te voldoen zijn in de RIPA en de Code of Practice regels gesteld over de verwerving van verkeersgegevens, het soort gegevens dat bemachtigd mag worden, welke personen binnen de aangewezen instanties gebruik mogen maken van de bevoegdheden tot het verwerven van deze gegevens en welke personen feitelijk de gegevens verwerven.

In Grafiek 4 is voor de periode van 2007 tot en met 2010 een overzicht gegeven van het aantal autorisaties voor met name het gebruik van abonnee- en verkeergegevens afkomstig van de Home Secretary.

79 Te vergelijken met CIOT-bevragingen in Nederland.
80 Section 21 e.v. RIPA 2000.
81 Naast de in de hoofdtekst genoemde instanties betreft het 8 politiekorpsen in Schotland, de Police Service of Northern Ireland, de British Transport Police, Port of Liverpool Police, Port of Dover Police, Royal Military Police, Royal Air Force Police, Ministery of Defence Police, Royal Navy Police, Civil Nuclear Constabulart, Scottish Crime and Drug Enforcement Agency (SCDEA), Untited Kingdom Border Agency (UKBA), Child Exploitation & Online Protection Centre (CEOP). Zie Interception of Communications Commissioner, 2011, p. 33.
82 Zie nader paragraaf 9.3.

Grafiek 4 Aantallen verzoeken om gebruik te maken van met name abonnee- en verkeersgegevens



Bronnen: Reports of the Interception of Communications Commissioner 2007 t/m 2010

In 2010 zijn in totaal 552.550 verzoeken gedaan om gebruik te maken van gegevens. Deze verzoeken komen vooral voor rekening van inlichtingendiensten, politiekorpsen en andere instanties binnen de strafrechtspleging (Interception of Communications Commissioner, 2011, p. 31).[83] Het aantal verzoeken in 2008 betrof 504.073 en in 2009 was dat 525.130. Een stijging over genoemde jaren heen van ongeveer 5%. In 2007 bedroeg het aantal verzoeken 519.260.
Tweederde van de 552.550 aanvragen over 2010 betrof informatieverzoeken over abonneegegevens (*subscriber data*), vooral met de bedoeling om de eigenaren van mobiele telefoons te traceren (zie Section 21.4 sub *c* RIPA). Ruim een kwart van de aanvragen had betrekking op verkeersgegevens (*traffic data*; zie Section 21.4 sub *a* RIPA 2000). Verder betrof 6% gegevens die gebruikt worden door personen onder andere werkzaam bij telecommunicatie diensten (*service use data*; zie Section 21.4 sub *b* RIPA 2000) en 3% tenslotte, had betrekking op een combinatie van de drie bovengenoemde (Interception of Communications Commissioner, 2011, p. 32).[84]
Een verklaring voor de stijging vanaf 2008 weet de Commissioner niet te geven, maar hij wijst wel op de groei in mogelijkheden binnen de communicatietechnologie (Interception of Communications Commissioner, 2011, p. 31). Opvallend is het grote contrast in aantallen aanvragen voor het gebruik van verkeersgegevens (*traffic data*) en de hoeveelheid tapbevelen die is uitgegeven en van kracht is (zie Grafiek 1). Met betrekking tot de aanvraag van verkeersgegevens stelt de Commissioner:

> "The statistics show that certain police forces have increased their demands for communications data and I believe that this is due, in part, to the fact that there is an increasing awareness amongst investigators of the type of communications data that is available and how communications data can [be] used as [a] powerful investigative tool." (Interception of Communications Commissioner, 2011, p. 31)[85]

83 Doordat ook de verzoeken van de *inlichtingendiensten* in Grafiek 4 zijn meegenomen wordt het beeld wel vertekend.
84 Chart 2: Percentage of Communications Data Requests by Type.
85 Overigens is onduidelijk of de Communications Commissioner met de term 'communication data' alleen maar doelt op 'traffic data', of dat 'communication data' ook 'subscriber data' (abonneegegevens) omvat. Hier is gekozen voor de uitleg dat met communication data alleen traffic data wordt bedoeld.

Daarnaast zijn er meer dan 400 locale overheden (*local authorities*), verdeeld over het gehele Verenigd Koninkrijk, bevoegd om bepaalde verkeersgegevens te verwerven. Het gaat dan om abonneegegevens of berichtgegevens.[86] In 2010 waren er 1.809 aanvragen van locale overheden waarvan 95% betrekking had op abonneegegevens (naam en adres) de andere 5% op service use data. Locale overheden vragen vooral abonneegegevens om de onbekende verdachten te kunnen identificeren.[87]

9.2.3 Het gebruik van de tap

In de beschrijving van de gang van zaken tijdens de interceptie van telefoon- en internetverkeer wordt uitgegaan van de werkwijze van de SOCA en HMRC, zoals die voornamelijk uit de interviews naar voren is gekomen. Daar waar de werkwijze tussen de beide instanties uiteenloopt wordt dat aangegeven.
Er bestaan binnen Engeland en Wales 3 verschillende aftapfaciliteiten. Eén onder de auspiciën van de SOCA, een tweede onder die van HMRC en de derde (een kleinere) onder het gezag van de Metropolitan Police (MET).

> "The facilities are available to police forces throughout the United Kingdom. Most of the police cases which have facilities submit their authorisations through SOCA. There are some from the Metropolitan Police who work with HMRC and they submit the paperwork through HMRC. But that's a small part of it. And then the Metropolitan Police has a small Section which deals with some (…) very limited serious crime (…)." – Home Office

De SOCA is betrokken bij afluisteren van telefoonverkeer zodra het zware criminaliteit (*serious crime*) betreft. Zoals hierboven al is aangegeven valt onder zware criminaliteit ondermeer: in- en uitvervoer van drugs, fraude, mensenhandel, vuurwapendelicten, geweld, computercriminaliteit en kidnapping. Met betrekking tot het laatst genoemde delict ondersteunt de SOCA de politie door het afluisteren van telefoongesprekken.[88] Naast het zelf afluisteren van telefoonverkeer ondersteunt de SOCA een aantal andere instanties, waaronder de politie, bij het aftappen van telefoonverkeer. Dit betekent dat politiemensen door de SOCA worden getraind in het afluisteren van telefoonverkeer.[89]
Als Britse belastingdienst heeft HMRC een afdeling die is belast met de opsporing van fiscale delicten. Binnen HMRC bestaan 8 verschillende interceptie agencies. Daarnaast zijn er operationele teams in het veld belast met de opsporing en het verzamelen van bewijs. Een casemanager[90] (of zijn/haar deputy) van een dergelijk operationeel team fungeert als een contactpersoon als het gaat om inlichtingen verkregen uit aftappen van telefoonverkeer. Deze persoon is als het ware een intermediair tussen het operationele team en degenen die het aftappen verzorgen.[91]
Op twee verschillende manieren wordt er afgetapt, namelijk in real time en via een transcriptie faciliteit. Bij de tweede mogelijkheid wordt bijvoorbeeld als volgt te werk gegaan:

> "Some of the interceptors are trained investigators. (…) when before SOCA was set up, all intercept for the police service was done by the National Criminal Intelligence Service or NCIS and they employed civilian transcribers who would listen to the calls, as far as I'm

86 Zie ook Interception of Communications Commissioner, 2011, p. 40.
87 *Idem*, p. 41.
88 Aldus een respondent van de SOCA.
89 Aldus een respondent van de SOCA.
90 Een respondent van de Home Office geeft aan dat voor elke strafzaak een casemanager wordt aangesteld.
91 Volgens een respondent van de Home Office zijn degenen die de interceptie doen, eerst werkzaam geweest als opsporingsambtenaren in het veld. Werken in een interceptieteam is een vooruitgang in iemands carrière. "They have operational experience, they know what actually becomes an evidential opportunity to go out and gain evidence which parallels, what is actually happening in the intercept facility."

> aware, and they would transcribe it, write it out or type it out and that would than go to authorised persons within the investigative capability, who would assess the calls and than react to that. (…) SOCA still does some of that, but they also do some the way HMRC does. Because the inherited staff from NCIS and from HMRC's predecessor Customs and Excise." – Home Office

De laatst genoemde mogelijkheid sluit echter niet altijd goed aan bij de werkzaamheden van het team dat in het veld opereert. Dit omdat via een transcriptie faciliteit eerst sprake is van overschrijving van informatie alvorens die kan worden uitgereikt aan het team werkzaam in het veld. Bovendien, zo blijkt, hebben degenen die de transcriptie uitvoeren niet altijd de kennis en ervaring om te beoordelen hoe belangrijk bepaalde informatie kan zijn.

Voordat wordt besloten om het aftappen van telefoon- of internetverkeer als opsporingsmethode in te zetten in een zaak, is er volgens de respondenten van de SOCA en HMRC, al gebruik gemaakt van andere opsporingsmethoden. Met andere woorden, de telefoon- of internettap is een van de laatste opsporingsmethoden die in een strafzaak wordt ingezet. Een van de eerste methoden die wordt ingezet in de opsporing door SOCA of HMRC is het opvragen van verkeersgegevens. Hiermee wordt dit opsporingsmiddel klaarblijkelijk losgekoppeld van de telefoon- en internettap. Opsporingsambtenaren proberen uit de gegevens te halen welk communicatieapparaten en -methoden de betrokkene gebruikt. Daarnaast wordt geprobeerd om uit de verkeersgegevens een beeld van de life style van de betrokkene (verdachte) te destilleren. Een respondent van HMRC geeft in dit verband aan:

> "Now the reality is, I think investigators would almost like it to be more of a first result service. But frankly we don't have the resources or all the legal framework that allows us to do it that way." - HMRC

Het gebruik van verkeersgegevens om een beeld te schetsen van de betrokkene is volgens de respondent van de HMRC belangrijk omdat anders het aftappen van de telefoon (of het internet) weinig nut blijkt te hebben.[92] Anders dan bij de uitkomsten van het aftappen van telefoonverkeer kunnen verkeersgegevens in een strafzaak wel worden gebruikt als bewijs.[93] Volgens één van de respondenten, werkzaam bij HMRC is het feit dat de tap niet frequent wordt ingezet als opsporingsmethode geen direct gevolg van het feit dat de resultaten uit de tap niet gebruikt mogen worden als bewijs. Eerder is volgens hem het tegendeel het geval. Als de tap voor het bewijs gebruikt zou worden zou er volgens hem zoveel werk gemoeid zijn met het uitluitseren en uitwerken van de resultaten van de tap. Dit zou volgens hem eerder tot een minder frequent, dan tot een frequenter gebruik van de tap leiden. De oorzaak voor het feit dat de tap in Engeland en Wales relatief weinig wordt ingezet, is volgens hem vooral een gevolg van de strenge proportionaliteits- en subsidiariteitseisen die aan dit opsporingsmiddel worden gesteld, hetgeen ertoe leidt dat het middel alleen bij de meest ernstige misdrijven kan worden ingezet.
Deze respondent geeft aan:

> "It's not really used, it's not used a lot because it's not used as evidence. Quite the contrary. We'd use it less if it was used as evidence because we couldn't manage all the legal framework around the management of investigative material. Would make it almost prohibitive for us to use intercept to the same degree that we currently use it. So it's not because of we can't use it as evidence, so we don't as a last result. It's purely on the basis that the legal framework says that it must fulfil these tests and so consequently we use intercept in our most serious investigations." - HMRC

92 In zijn eigen woorden: "that's almost one of the first things that ought to happen."
93 In Grafiek 4, paragraaf 9.2.2, worden de aantallen verzoeken om gebruik te maken van verkeersgegevens genoemd. Deze cijfers zijn beduidend hoger de aantallen afgegeven tapbevelen over dezelfde periode (zie Grafiek 1).

Uit de hierboven gepresenteerde cijfers blijkt dat aftappen van telecommunicatie in Engeland en Wales niet vaak als opsporingsmiddel wordt ingezet. Niettemin blijkt uit de rapportage van de Privy Council dat de SOCA dat het gebruik van telefoon- en internettap samen met het gebruik van verkeersgegevens als "the single most powerful tool for responding to serious and organised crime" wordt gezien (Privy Council Review of Intercept as Evidence, 2008, p. 11). De redenen die hiervoor worden gegeven zijn de volgende:

- It carries very low risk of putting police officers in danger or warning the suspect of police interest in him;
- It is flexible and uniquely easy to put in place quickly;
- It is less costly and less intrusive than for example covert entry, surveillance or eavesdropping;
- It can help ensure the safety of law enforcement personnel; and
- It can provide excellent intelligence of criminals' plans, allowing law enforcement to prevent serious crimes from occurring as well as to collect evidence of crimes being committed.

(Privy Council Review of Intercept as Evidence, 2008, p. 11)

Toch blijkt uit de beschikbare cijfers (Grafieken 1, 2 en 3), dat van de telefoon- en internettap veel minder gebruikt wordt gemaakt dan van CHIS. Echter, bekeken vanuit de context van de rapportage van de Privy Council, die erover gaat om de directe resultaten van de telefoon- en internettap als bewijsmiddel ter zitting te kunnen gebruiken (zie nader paragraaf 9.2.4), zal mogelijk vooral de kwalitatieve inzet van de telefoontap worden bedoeld. en dus niet zozeer de kwantitatieve inzet, en dan met name bij de aanpak van zware en georganiseerde criminaliteit. Opvallend is dat respondenten van de SOCA, HMRC en de Home Office de inzet van informanten niet zien als een werkbaar alternatief voor het aftappen van telecommunicatie. Zij bevestigen de redenen die in de rapportage van de Privy Council worden genoemd.

> "When you are dealing with a lot of cases it's not really that practical. But if (…) you are looking at longer term operations perhaps to try to investigate somebody who is very clever, who keeps themselves remote from the day to day affairs of a business, and only deals with the people they trust. If you really want to get to that person you might have to think about that. (…) also it is expensive on (the) long term if the cases that you are investigating are sufficiently serious, for example some of the tax cases that are investigated run into tens hundreds of millions of pounds. So the investment in a case like that, if it's the only way that you are going to get the evidence, it would be justified. Similarly, in large scale heroine trafficking or cocaine trafficking, if it is feasible to deploy an undercover officer, because organizations like that are very distrusting of newcomers. Then it becomes quite expensive to do that. So it is expensive but they do have a use. But they wouldn't be used as often as intercept or bugging would be, because there is not as many of them. High risks attached to it as well."- Home Office. [94]

De telefoontap aanvullend inzetten naast andere opsporingsmiddelen, zoals het gebruik van informanten, lijkt wel een beproefde methode te zijn.

> "So the operational team will reach a point where they'll say, ok we have done all this, we need to get a bit further forward with it. They will come to these covert areas and say how can you help. Now we may look at that and say well actually the most effective way of us helping is intercept. Or it might be we say, actually the most effective way for the minute is, you need to go and develop all of this communications data or we, there is an opportunity here or we might deploy an undercover officer. So we might consider all of

[94] In deze context moet niettemin worden gewezen op de bevinding dat de SOCA reeds in een vroeg stadium undercovertrajecten toepast om informatie te verkrijgen over de organisatie en werkwijze van criminele groepen (zie paragraaf 9.2.1).

> those different things and interception will be one part of it. But most often actually the intercept is probably at that stage as effective and more effective and might help us place our undercover officer or identify an opportunity for recruiting an informant and or may say where we need to deploy a covert audio device. So it helps us work out where we can use some of these other techniques that rely a lot on different resources and limited resources and helps us really target those in the right areas." - HMRC

Daarnaast heeft aftappen van telecommunicatie ook een meerwaarde als het gaat om het vergaren van informatie, hetgeen ook, zoals hierboven weergegeven, door de Privy Council is geconstateerd.

> "So to say that's kind of the most effective way and obviously in the meantime of doing that we are learning about what the organization hierarchy is, who is important in the organization, what the modus operandi is for the organization, so how do they work how do they make the crime happen, what they are planning. What they are doing with the money, where they are putting their money, where they are getting the supply, if it's a commodity that they are dealing with such as drugs or in our case goods, where did they get those from. (…) All of these different aspects (…) is what we will get out of (it). Particularly is what we can get out of the intercept. And in the meantime the operational team are dealing with helping their positioning things, so that they can collect evidence that actually shows that those things are happening. Because obviously the intercept, all of the stuff that we learned in the intercept, won't come just from a series of phone calls. It comes from having an overall picture of the whole of the organization. So we use it as an intelligence tool to help us understand what the organizations look like." - HMRC

De internettap
De regelgeving met betrekking tot de telefoontap (RIPA 2000) is ook van toepassing op de internettap. Ook voor de internettap geldt dat de opbrengsten niet mogen worden gebruikt als bewijs in een strafzaak. Wel is het mogelijk om informatie die op de computer bewaard is als bewijs te gebruiken. In die zin heeft de internettap een toegevoegde waarde. Het gebruik van de internettap blijkt een gevoelig punt te zijn, met name op het gebied van de mogelijkheden, waarover geen verdere informatie wordt gegeven. Wel blijkt uit de interviews dat er door opsporingsambtenaren niet veel gebruik wordt gemaakt van de internettap. Dit geldt des te meer indien de telefoontap ter beschikking staat.

9.2.4 Het gebruik van telecommunicatiedata als bewijs

Tot op heden kunnen opbrengsten van het aftappen van internet en de telefoon (*intercept*) niet als bewijsmiddel ter zitting worden gebruikt.[95] Om te kijken of hier verandering in aangebracht kan worden, heeft de Britse regering in 2007 een commissie (Privy Council) in het leven geroepen met als taak:

> "to advice on whether a regime to allow the use of intercepted material in court can be devised that facilitates bringing cases to trial while meeting the overriding imperative to safeguard national security." (Privy Council Review of Intercept as Evidence, 2008, p. 4)

Deze commissie heeft als belangrijkste aanbeveling gedaan dat intercept in beginsel als bewijsmiddel ter zitting moet worden geïntroduceerd, dat voldoet aan de eisen van artikel 6

[95] Dit verbod geldt overigens alleen voor materiaal dat op basis van een Brits tapbevel is onderschept. Indien het materiaal betreft dat in het buitenland, bijvoorbeeld in Nederland, naar Nederlandse maatstaven rechtmatig is afgetapt; of het aftappen is gebeurd met toestemming van een van de betrokkenen (vgl. *Liberty tegen het Verenigd Koninkrijk*, EHRM 1 juli 2008 (http://www.echr.coe.int/ECHR/EN/Header/Case-Law/), of het telefoongesprek is opgenomen met een (verborgen) microfoon die niet (rechtstreeks) is verbonden aan de telefoon, dan mag het materiaal wel ter zitting worden gebruikt als bewijs. Zie in dit verband Privy Council Review of Intercept as Evidence, 2008, p. 9.

en 8 van het EVRM (Privy Council Review of Intercept as Evidence, 2008, p. 48-49).[96] In dit verband wijst de Privy Council onder ander op een aantal voordelen van het huidig gebruik van intercept als een opsporingsmiddel:

"There is uniquely close and valuable cooperation between UK intelligence and law enforcement agencies;
- Law enforcement agencies (primarily SOCA) use intercept to gather complex intelligence pictures sometimes over many years, whilst in other instances they use intercept to move swiftly, particularly when life is at risk;
- GCHQ [Government Communications Headquarters] and Security Service provide extensive operational and (critically) technical support to law enforcement operations;
- The UK has a particularly large and sophisticated intercept capability, which is used flexibly and efficiently."

(Privy Council Review of Intercept as Evidence, 2008, p. 49)

9.3 Waarborgen bij het gebruik van heimelijke opsporingsmiddelen

9.3.1 Inbreuk op het recht op privacy

Door gebruik te maken van de telefoon- en internettap wordt een inbreuk gemaakt op iemands persoonlijke levenssfeer. Ook bij het gebruik van Intrusive Surveillance (IS) en Covert Human Intelligence Sources (CHIS) wordt inbreuk gemaakt op de persoonlijke levenssfeer van een burger. Het recht op privacy is een grondrecht dat onder andere wordt gewaarborgd door het EVRM. Een rechtmatige inbreuk maken op dat grondrecht door het openbaar gezag is niet uitgesloten, maar moet wel voldoen aan de eisen die in artikel 8 lid 2 EVRM worden gesteld.[97]
Nu is het EVRM niet rechtstreeks geldend recht in het Verenigd Koninkrijk, maar door de gelijktijdige inwerkingtreding van de RIPA 2000 met de Human Rights Act 1998 (HRA), zijn de mensenrechten van het EVRM geïncorporeerd in het Britse recht. Hierdoor kan in alle Engelse gerechten een beroep gedaan worden op de grondrechten neergelegd in het EVRM (Colvin & Cooper, 2009, p. 4).
De rechtspraak van het Europese Hof voor de Rechten van de Mens (EHRM) betreffende artikel 8 lid 2 EVRM richt zich vooral op de voorwaarden *in accordance with the law* en *necessary in a democratic society* (Krabbe, 2004, p. 161). Dat de inbreuk 'in accordance with the law' moet zijn betekent ondermeer dat de bevoegdheid tot tappen moet berusten op nationaal recht. Voor het Engelse recht is het van belang dat het EHRM de term 'Law' ruim interpreteert, zodat zowel geschreven als ongeschreven recht hieronder valt.[98] De voorwaarde 'in accordance with the law' heeft ook te maken met de kwaliteit van het nationale recht (*the quality of the law*). Zo moet het nationale recht in overeenstemming zijn met de rule of law, "which is expressly mentioned in the preamble to the Concention."[99] Het EHRM kenmerkt artikel 8 lid 2 EVRM als een autonome rechtsbron en heeft twee criteria ontwikkeld om het overheidsoptreden binnen het eigen nationaal rechtsstelsel te beoordelen (Krabbe, 2004, p. 163-164). Het betreft hier de toegankelijkheid van het nationale recht (*accessability*) en de voorzienbaarheid (*foreseeability*) van het recht.
Dat het recht toegankelijk moet zijn houdt in dat het voor een burger mogelijk moet zijn om te bepalen welke regels van toepassing zijn. Als dat ongeschreven recht betreft, zoals dat in

96 Zie ook *Liberty tegen het Verenigd Koninkrijk*, EHRM 1 juli 2008 (http://www.echr.coe.int/ECHR/EN/Header/Case-Law/).
97 De inbreuk moet zijn in accordance with the law, in the interests of among other the prevention of disorder or crime or the rights and freedoms of others en necessary in a democratic society. Zie ook hoofdstuk 11, Tappen in Duitsland, paragraaf 11.3.
98 Zie *Chappell tegen het Verenigd Koninkrijk*, EHRM 30 maart 1989 en later ook *Kruslin tegen Frankrijk*, EHRM 24 april 1990. Beide uitspraken zijn te vinden op http://www.echr.coe.int/ECHR/EN/Header/Case-Law/.
99 Zie *Malone tegen het Verenigd Koninkrijk*, EHRM 2 augustus 1984, te vinden op http://www.echr.coe.int/ECHR/EN/Header/Case-Law/.

Engeland en Wales zich soms voordoet, hoeft dat geen problemen op te leveren als de kennisneming van dat recht, bijvoorbeeld richtlijnen over afluisteren, eenvoudig is.[100] Met de inwerkingtreding van de RIPA 2000 zijn de regelingen van de telefoon- en internettap, de bovengenoemde CHIS en het gebruik van surveillance inmiddels gecodificeerd (Hopkins, 2009*a*, p. 33). In de zaak *Kennedy tegen het Verenigd Koninkrijk* (18 mei 2010) toetst het EHRM de RIPA 2000 aan artikel 8 lid 2 EVRM. Het Europese Hof komt uiteindelijk tot de conclusie dat er geen sprake is van (enige) tekortkomingen in het RIPA regime:

> "In the circumstances, the Court considers that the domestic law on interception of internal communications together with the clarifications brought by the publication of the Code indicate with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of intercept material collected. The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the surveillance regime. On the contrary, the various reports of the Commissioner have highlighted the diligence with which the authorities implement RIPA and correct any technical or human errors which accidentally occur (see paragraphs 62, 67, 71 and 73 above). Having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, insofar as they may have been applied to the applicant in the circumstances outlined in the present case, are justified under Article 8 § 2."[101]

De andere voorwaarde over de voorzienbaarheid van het recht brengt met zich mee dat de norm voldoende duidelijk moet zijn geformuleerd in regelingen, zodat een burger zijn gedrag daarop kan afstemmen (Krabbe, 2004, p. 166). Bij de regeling over aftappen levert dit problemen op. De bedoeling van de opsporingsmethode van de telefoon- en internettap is immers dat betrokken burgers juist niet op de hoogte geraken van de hantering van de maatregel. Indien voldaan aan strikte voorwaarden blijkt het EHRM akkoord te gaan met een verminderde voorzienbaarheid voor de burger.[102] Krabbe (2004) formuleert het bezwaar als volgt:

> "De democratische rechtstaat kan in het hart getroffen worden door ondemocratische, immers oncontroleerbare en steeds verfijndere technische onderzoeksmethoden. Indien autoriteiten bevoegdheden in het geheim kunnen uitoefenen, bestaat volgens het Hof een evident gevaar voor willekeurig optreden door overheidsinstanties." (Krabbe, 2004, p. 167)

Het EHRM beoordeelt de kwaliteit van het recht in het kader van de voorzienbaarheid met betrekking tot het aftappen van telefoongesprekken aan de hand van een zestal voorwaarden (ook genoemd in Deel I, hoofdstuk 3, paragraaf 3.3.1)

> "(iv) The Kruslin and Huvig judgments mention the following minimum safeguards that should be set out in the statute in order to avoid abuses of power: a definition of the categories of people liable to have their telephones tapped by *judicial order* [*cursivering toegevoegd*], the nature of the offences which may give rise to such an order, a limit on the duration of telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations, the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the

100 Zie o.a. *Sunday Times tegen het Verenigd Koninkrijk*, EHRM 26 april 1979, *Khan tegen het Verenigd Koninkrijk*, EHRM 12 mei 2000, *P.G. and J.H. tegen het Verenigd Koninkrijk*, EHRM, 25 september 2001, *Armstrong tegen het Verenigd Koninkrijk*, EHRM 16 juli 2002, *Allan tegen het Verenigd Koninkrijk*, EHRM 5 november 2002. Al deze uitspraken zijn te vinden op http://www.echr.coe.int/ECHR/EN/Header/Case-Law/.

101 *Kennedy tegen het Verenigd Koninkrijk*, EHRM 18 mei 2010, r.o. 169 (te vinden op http://www.echr.coe.int/ECHR/EN/Header/Case-Law/).

102 Vergelijk o.a. de zaak *Klass tegen Duitsland*, EHRM 6 september 1978 (te vinden op http://www.echr.coe.int/ECHR/EN/Header/Case-Law/).

> defence and the circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court (loc. cit. p. 24, § 35, and p. 56, § 34, respectively)."[103]

Hieruit blijkt onder andere dat het EHRM een voorkeur heeft voor een *rechterlijke toetsing* van de machtiging tot het aftappen van burgers. Zoals hierboven in paragraaf 9.1 beschreven, is dat niet de procedure die in Engeland en Wales wordt gevolgd. In het autorisatieproces wordt geen rechter betrokken, maar is het de Secretary of State die het tapbevel ondertekent.[104] Hiermee lijkt de regeling in strijd te komen met het Europese recht. Recent heeft het EHRM in *Kennedy tegen het Verenigd Koninkrijk* (18 mei 2010) evenwel anders beslist:

> "The Court recalls that it has previously indicated that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, *it is in principle desirable to entrust supervisory control to a judge* (see Klass and Others, cited above, § 56) [*cursivering toegevoegd*]. In the present case, the Court highlights the extensive jurisdiction of the IPT[105] to examine any complaint of unlawful interception. Unlike in many other domestic systems (see, for example, the G 10 Law discussed in the context of Klass and Others and Weber and Saravia, both cited above), any person who suspects that his communications have been or are being intercepted may apply to the IPT (see paragraph 76 above). The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasizes that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers (see paragraph 75 above). In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant (see paragraph 78 above). In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid (see paragraph 80 above). The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see paragraph 89 above)."[106]

Daar waar misbruik in individuele gevallen relatief eenvoudig is en de gevolgen schadelijk kunnen zijn voor de democratische samenleving als geheel, geeft het EHRM in beginsel de voorkeur aan een rechterlijke controle op het autorisatieproces van een telefoon- of internettap. Niettemin geeft de Engelse procedure, waarbij met name de rol van de Investigatory Powers Tribunal (IPT) naar voren wordt gehaald, voor het EHRM voldoende waarborgen om toch te voldoen aan de voorwaarden gesteld aan een regeling omtrent het aftappen van telefoon- en internetverkeer.

103 Zie *Valenzuela Contreras tegen Spanje*, EHRM 30 juli 1998, r.o. 46 en eerder o.a. *Kruslin tegen Frankrijk*, EHRM 24 april 1990 en (uitspraken te vinden op http://www.echr.coe.int/ECHR/EN/Header/Case-Law/).

104 Zie in dit verband tevens *Kennedy tegen het Verenigd Koninkrijk*, EHRM 18 mei 2010, r.o. 163 (te vinden op http://www.echr.coe.int/ECHR/EN/Header/Case-Law/).

105 Investigatory Powers Tribunal, zie de volgende subparagraaf.

106 *Kennedy tegen het Verenigd Koninkrijk*, EHRM 18 mei 2010, r.o. 167 (te vinden op http://www.echr.coe.int/ECHR/EN/Header/Case-Law/).

9.3.2 Investigatory Powers Tribunal

Ter aanvulling op hetgeen door het EHRM in *Kennedy tegen het Verenigd Koninkrijk* (18 mei 2010) wordt gezegd over het Investigatory Powers Tribunal (IPT), kan nog het volgende naar voren worden gebracht. Het IPT is opgericht op grond van Section 65 RIPA 2000. Deze instantie is in het leven geroepen om burgers de mogelijkheid te geven zich te beklagen over handelingen verricht door organen die hun bevoegdheden ontlenen aan de RIPA 2000. Het betreft dan bijvoorbeeld klachten tegen het optreden van of namens de Inlichtingendiensten: the Security Service (MI5) en de Secret Intelligence Service (MI6) en de Government Communications Headquarters (GCHQ).[107] Er bestaat in Engeland en Wales geen verplichting tot notificatie aan betrokken personen over gebruikmaking van heimelijke opsporingsmiddelen, zoals de telefoontap.[108] Burgers die menen dat hun telefoon onrechtmatig is afgetapt door bijvoorbeeld de politie, zullen hierover hun beklag moeten doen bij het Tribunaal. Indien het Tribunaal dat nodig acht, kan het op basis van Section 57 sub 3 RIPA 2000 de Communications Commissioner verplichten mee te werken aan onderzoek naar bijvoorbeeld vermeend misbruik van de telefoontap door de politie.
In 2010 zijn er in totaal 164 nieuw klachten binnengekomen bij het Tribunaal. Het heeft in dat jaar 208 beklagzaken afgerond en 40 zaken doorgeschoven naar 2011. Een uitsplitsing naar soorten zaken, bijvoorbeeld met betrekking tot vermeend onrechtmatig gebruik van de telefoontap door overheidsinstanties is volgens de Communications Commissioner niet te maken (Interception of Communications Commissioner, 2011,p. 54).

9.4 Concluderend

De interceptie van communicatie (telefoon- en internetverkeer) wordt in het Verenigd Koninkrijk geregeld in de RIPA 2000. Een tapbevel wordt in Engeland en Wales niet toegekend door een onafhankelijke rechter, maar door een binnen de bestuurskolom actieve Secretary of State. De Interception of Communications Commissioner is als een onafhankelijk orgaan belast met het toezicht op het aanvragen en uitvoeren van tapbevelen. Individuele klachten over (onrechtmatig) aftappen kunnen worden ingediend bij het Investigatory Powers Tribunal (IPT). Anders dan in Nederland, kan de informatie die met de tap wordt verkregen in Engeland en Wales niet als bewijs worden gebruikt in een strafzaak.

Een algemeen beeld dat uit de tapstatistieken naar voren komt, is dat er in Engeland en Wales relatief weinig wordt getapt. Hierbij moet worden opgemerkt dat de beschikbare cijfers over aantallen tapbevelen moeilijk met de Nederlandse cijfers kunnen worden vergeleken. In Engeland en Wales worden tapbevelen namelijk afgegeven op personen en binnen één bevel kunnen verschillende telefoonnummers worden afgetapt. Er blijken in Engeland en Wales vaak eerst andere heimelijke opsporingsmiddelen ingezet te worden, voordat wordt overgegaan tot de inzet van de tap. De tap wordt in Engeland en Wales dus, veel meer dan in Nederland, gezien als een van de laatste opsporingsmethoden die in een strafzaak kunnen worden ingezet. Een van de eerste middelen die in de opsporing door de SOCA of HMRC wordt gebruikt, is het opvragen van verkeersgegevens. Met deze gegevens kan het opsporingsteam een beeld krijgen van het (tele)communicatie- of internetverkeer van een betrokkene alvorens wordt overgegaan tot de inzet van een telefoon- of internettap. Het grote aantal aanvragen voor het gebruik van verkeersgegevens in de periode 2008-2010 (dat is inclusief informatieverzoeken over abonneegegevens, oftewel *subscriber data*) is opvallend en staat in scherp contrasteert met het geringe aantal tapaanvragen dat in dezelfde periode is uitgegeven. Verder valt uit de cijfers af te leiden dat in de periode van 2006 tot en met 2010 veel vaker gebruik is gemaakt van de inzet van infiltranten (*Covert Human Intelligence Sources- CHIS*) dan van de telefoon- en/of internettap.

[107] Zie bijvoorbeeld Section 7 onder 1 sub *a* HRA 1998 en RIPA 2000 en Pt III Police Act 1997.
[108] De Public Prosecutors van de CPS, waarmee is gesproken, geven bovendien aan nimmer vrijwillig te notificeren.

De beschikbare gegevens laten zien dat het aantal tapbevelen dat in 2010 werd afgegeven met ruim 10% is gestegen ten opzichte van het jaar ervoor. Deze stijging kan volgens de Communications Commissioner worden toegeschreven aan de groei van het aantal gevallen van zware criminaliteit en bedreigingen van de nationale veiligheid van het Verenigd Koninkrijk, misdrijven waarbij de tap bijna standaard wordt ingezet. Daarnaast is er een beperkte groei te zien van ongeveer 5% van het aantal verzoeken om gebruik te kunnen maken van verkeersgegevens over de periode 2008-2010. Deze verzoeken komen voornamelijk van inlichtingendiensten, politiekorpsen en andere instanties binnen de strafrechtspleging. Een directe verklaring voor die stijging vanaf 2008 weet de Commissioner niet te geven.

In Engeland en Wales bestaan er drie verschillende aftapfaciliteiten, een van de SOCA, een van HMRC en een van de Metropolitan Police (MET). De werkwijze van de MET is niet onderzocht. De SOCA is betrokken bij afluisteren van telefoonverkeer zodra het zware criminaliteit (serious crime) betreft en HMRC als het bepaalde fiscale delicten betreft. Met name binnen SOCA wordt op twee verschillende manieren afgetapt, namelijk in real time en via een transcriptie faciliteit. Deze laatste mogelijkheid sluit echter niet altijd goed aan bij de werkzaamheden van het team dat in het veld opereert. Dit omdat via een transcriptie faciliteit de beschikbare informatie eerst moet worden uitgeschreven, alvorens deze kan worden uitgereikt aan het opsporingsteam. Bovendien, zo blijkt, hebben degenen die de transcriptie uitvoeren niet altijd de kennis en ervaring die nodig is om het belang van bepaalde informatie goed te kunnen beoordelen.
Hoewel de beschikbare tapcijfers laten zien dat de telefoontap niet frequent wordt gebruikt in de opsporingspraktijk, blijkt uit een rapportage van de Privy Council dat de SOCA het gebruik van de telefoon- en internettap – samen met het gebruik van verkeersgegevens – als belangrijkste opsporingsmiddel ziet als het gaat om de aanpak van zware en georganiseerde criminaliteit. Dit laatste moet waarschijnlijk worden opgevat als een kwalitatief argument, dat door de Privy Council naar voren wordt gebracht ter ondersteuning van de aanbeveling om de resultaten van de telefoon- en internettap te accepteren als bewijs in een strafzaak. Respondenten zien de inzet van de telefoontap in combinatie met andere opsporingsmiddelen, zoals het gebruik van informanten, als een vruchtbare opsporingsstrategie. Verder zien zij meerwaarde in het aftappen van telecommunicatie, omdat informatie uit de tap gebruikt kan worden om het opsporingsproces te sturen. Door middel van de tap kan kennis worden vergaard over de wijze waarop een vermeende criminele organisatie functioneert. Deze informatie kan worden gebruikt om gericht andere opsporingsmiddelen in te zetten waarmee de veronderstelde criminele activiteiten verder kunnen worden onderzocht en waarmee gericht bewijs kan worden vergaard.
Zoals gezegd kunnen de opbrengsten van de telefoon- en internettap in het Engelse strafrechtssysteem niet als bewijsmiddel ter zitting worden gebruikt. Het is daarentegen wel mogelijk om informatie die op de computer is bewaard te gebruiken als bewijs. Een door de regering geïnstalleerde commissie (de Privy Council) heeft als belangrijkste aanbeveling naar voren gebracht dat er een regel moet worden geïntroduceerd die het mogelijk maakt om de informatie die met de tap wordt verkregen in beginsel wel als bewijsmiddel ter zitting te accepteren.
Het gebruik van de telefoon- en internettap maakt een inbreuk op de persoonlijke levenssfeer van de mensen die aan dit middel worden onderworpen. Het recht op privacy is een grondrecht dat onder andere wordt gewaarborgd door het EVRM. Hoewel een rechtmatige inbreuk op dat grondrecht door het openbaar gezag niet wordt uitgesloten, moet het wel voldoen aan de eisen die in artikel 8 lid 2 EVRM worden gesteld. De rechtspraak van het EHRM met betrekking tot lid 2 concentreert zich met name op de voorwaarden *in accordance with the law* en *necessary in a democratic society*. In dit verband heeft het EHRM twee criteria ontwikkeld om het overheidsoptreden binnen het eigen nationaal rechtsstelsel te beoordelen. Het betreft hier de toegankelijkheid van het nationale recht (*accessability*) en de voorzienbaarheid (*foreseeability*) van het recht. In de zaak *Kennedy tegen het Verenigd Koninkrijk* (18 mei 2010) toetst het EHRM de RIPA 2000 aan artikel 8 lid 2 EVRM en stuit daarbij niet op enige tekortkoming. In de Engelse procedure biedt de Investigatory Powers Tribunal (IPT) de burgers de mogelijkheid om zich te beklagen over handelingen van het

bevoegd gezag, hetgeen voor het EHRM voldoende waarborgen geeft bij het gebruik van de tap.

10 Het gebruik van de tap in Zweden

Zweden is het tweede land waar het rechtsvergelijkend onderzoek naar het gebruik van telefoon- en internettap als opsporingsmethode zich op richt. Zweden is een parlementaire monarchie en is met 9.2 miljoen ingezetenen qua inwoners aantal het grootste Scandinavische land.[109] Tot halverwege de jaren zeventig van de vorige eeuw beschikte de koning formeel over wetgevende bevoegdheden, maar is daar in 1974 door een grondwetswijziging van ontheven. Overigens is er in het Zweedse bestel geen wet die de benaming Grondwet draagt. Met de constitutie wordt doorgaans gedoeld op vier aparte wetten, zijnde: het Instrument van Overheid (*Regeringsform*), de (troon)Opvolgingswet (*Successionsordning*), de Wet betreffende Persvrijheid (*Tryckfrihetsförordning*) en de (basis)Wet over Vrije Meningsuiting (*Yttrandefrihetsgrundlag*) (Carlson, 2009, p. 23 e.v.). De bron van de politieke macht ligt bij het parlement, dat in 1866 over twee kamers van afgevaardigden beschikte en vanaf 1971 over nog slechts één kamer. Het parlement (*Riksdag*) wordt elke vier jaar gekozen en bestaat uit 349 leden.[110] Een nieuw gekozen parlement wijst vervolgens een Minister-president aan die een regering vormt. De Raad voor Wetgeving (*Lagrådet*) adviseert de regering over voorgestelde wetgeving.[111] Zweden is lid van de Raad van Europa sinds de oprichting (5 mei 1949) en heeft het Europees Verdrag voor de Rechten van de Mens (EVRM) geratificeerd op 4 februari 1952.

Hieronder wordt in paragraaf 10.1 een schets gegeven van het Zweedse strafrechtssysteem. Daarbij komen die overheidsorganen die rechtreeks te maken hebben met de telefoon- en internettap aan bod, en worden de verschillend fasen van het strafproces kort beschreven. In de volgende paragraaf (10.2) wordt ingegaan op het gebruik van de telefoon- en internettap als opsporingsmethode. Daarbij starten we met een beschrijving van het autorisatieproces van de tapaanvraag. Vervolgens wordt ingegaan op de machtigingen voor het gebruik van verkeergegevens en daarna op het gebruik van de tap en telecommunicatie. Daarna komen in paragraaf 10.3 de waarborgen en het gebruik van heimelijke opsporingsmiddelen aan de orde. Het hoofdstuk wordt afgesloten in met een samenvatting op hoofdpunten (paragraaf 10.4).

10.1 Het Zweedse strafrechtssysteem

10.1.1 Karakteristieken

Het Zweedse rechtssysteem als geheel is sterk beïnvloed door het Duitse recht, maar tegenwoordig domineert vooral het Europees recht als invloed van buiten (Carlson, 2009, p. 36). Een belangrijk onderscheid dat binnen het Zweedse recht wordt gemaakt, is dat tussen publiek recht (*offentlig rätt*) en privaat recht (*privaträtt* of *civilrätt*).[112] Het Zweedse recht maakt deel uit van de zogeheten Scandinavische rechtsfamilie (*Nordic Legal family*) dat zich kenmerkt door een mix van gecodificeerd recht en case law (Carlson, 2009, p. 36 e.v.). Het neemt daarmee eigenlijk een tussenpositie in binnen de tweedeling van civil law en common law stelsels.[113]

109 Zie http://europa.eu/abc/european_countries/eu_members/sweden/index_en.htm.

110 Vijftien parlementaire commissies houden zich bezig met onderwerpen waarover het parlement zeggenschap heeft, zoals Justitie en Europese Unie aangelegenheden (zie o.a. www.riksdagen.se.templetes).

111 Zoals de Raad van State dat in Nederland doet.

112 Een onderscheid gebaseerd op een Romeins rechtelijke traditie, die ook in het Duitse en Nederlandse recht terug te vinden is. Zie ook Carlson (2009, p. 39).

113 Anders echter Zila (2006, p. 286) voor wat betreft het Zweedse straf(proces)recht. Dat kan volgens deze auteur gerekend worden tot de civil law familie (*Europees continentaal recht*). Opgemerkt moet worden dat voorzichtigheid is geboden met dergelijk algemene kwalificaties voor (nationale) rechtssystemen.

De civil law karakteristieken van het Zweedse rechtsstelsel hebben betrekking op de wijze waarop rechterlijke instanties hun rol binnen het systeem vervullen. Theoretisch uitgangspunt hierbij is dat de gerechten de bedoeling van de wetgever (*ratio legis*) moeten vaststellen en vertalen naar concrete zaken en zich niet moeten inlaten met het zelf creëren van recht.[114] Anderzijds zijn er conform het common law systeem binnen het Zweedse rechtssysteem geen volledige codificaties zoals een burgerlijk wetboek. Wel bestaan er codificaties (*balkar*) over specifieke onderwerpen, zoals het strafrecht (*straffrätt*) en gerechtelijke procedures (*procesrätt*). De belangrijkste bron van materieel strafrecht is het Zweedse Wetboek van Strafrecht (*Brottsbalken*). Daarbuiten bestaan er met betrekking tot een groot aantal strafrechtelijke onderwerpen zelfstandige regelingen, die worden aangeduid als *speciaal strafrecht* (Zila, 2006, p. 286). Een principiële verdeling van onderwerpen over het Wetboek van Strafrecht en het speciaal strafrecht lijkt er niet te zijn. Het onderscheid lijkt eerder gebaseerd te zijn op een legislatieve traditie (Zila, 2006, p. 286).
Het Zweedse straf- en burgerlijk procesrecht is gebaseerd op drie basis beginselen: mondelinge procesvoering, het beginsel van concentratie en het onmiddellijkheidsbeginsel (Lindblom, 2000, p. 212). Een mondelinge procesvoering lijkt voor zich te spreken, zo wordt het bewijs ter zitting mondeling gepresenteerd.[115] Daarop is in 2008 via een wijziging in de wet voor gerechtelijke procedures (*Rättegångsbalken*) een uitzondering gemaakt, nu het ook mogelijk is om te refereren naar bepaalde schriftelijke stukken in plaats van deze voor te (moeten) lezen (Carlson, 2009, p. 153). Het beginsel van concentratie betekent dat de zaak zo moet worden voorbereid dat het in één zitting kan worden behandeld (Lindblom, 2000, p. 212; Carlson, 2009, p. 148). Het onmiddellijkheidsbeginsel houdt in dat een rechtelijk oordeel alleen kan worden gebaseerd op hetgeen ter zitting naar voren is gebracht. Genoemde Wet voor Gerechtelijke Procedures (*Rättegångsbalken*) is de belangrijkste bron van strafprocesrecht in Zweden. Enkele specifieke aspecten van het Zweeds (straf)procesrecht verdienen nadere aandacht. Zo geldt de Rättegångsbalken (Rgb) zowel voor het strafproces als het civiele proces.[116] Alle rechters behandelen zowel civiele zaken als strafzaken. Ook bestaat er binnen de zittende magistratuur in Zweden geen specialisatie in strafkamers en civiele kamers, zoals we dat in Nederland kennen. Zweedse zittingsrechters zijn veel minder actief op zoek naar de materiële waarheid dan in Nederland. De beide procespartijen (openbaar aanklager en verdachte) presenteren zelf hun bewijs nadat zij hun pleidooi hebben gehouden (Lindblom, 2000, p. 212). In die zin sluit het Zweedse strafproces aan bij de common law traditie.

10.1.2 Enkele organen binnen het Zweedse strafrechtssysteem

De belangrijkste organen binnen de Zweedse strafrechtspleging zijn de zittende magistratuur (*Domstolsväsendet*), de vervolgingsautoriteit (*Åklagarmyndigheten*), de politie en de gevangenis en reclassering (*Kriminalvården*). Hoewel al deze instanties organisatorisch onder het ministerie van justitie (*Regeringskansliet*) vallen, kunnen ze in individuele gevallen niet worden aangestuurd door het ministerie van justitie (Zila, 2006, p. 285). Hieronder wordt verder ingegaan op twee van de bovengenoemde organisaties die rechtstreeks te maken hebben met het aftappen van telefoon- en internetverkeer. De Zweedse vervolgingsautoriteit (*Åklagarmyndigheten*) en de Rijkspolitie (*Rikskriminalpolisen*).

Åklagarmyndigheten
Åklagarmyndigheten is de Zweedse vervolgingsautoriteit (het openbaar ministerie). De openbaar aanklager bepaalt of een strafzaak zal worden vervolgd (*åtalsunderlåtelse*) of niet.[117] Naast de openbaar aanklager heeft in sommige gevallen ook het (vermeend) slachtoffer de mogelijkheid een vervolging in te stellen of die van de openbaar aanklager over te nemen. Dit blijkt in de praktijk echter weinig voor te komen (Zila, 2006, p. 290 e.v.).

[114] Op deze benaderingswijze is het nodige af te dingen. Het suggereert immers een tegenstelling die er noodzakelijkerwijze niet hoeft te zijn.
[115] Een meervoudige strafkamer bestaat uit één jurist en drie lekenrechters.
[116] Dit gaat in Zweden zelfs terug tot in de Middeleeuwen (Lindblom, 2000, p. 212 e.v.).
[117] Onder bepaalde omstandigheden kan een openbaar aanklager zelfs ter zitting besluiten de vervolging te staken (zie Hoofdstuk 20, artikel 7 Rgb).

Verder heeft de openbaar aanklager ook de mogelijkheid om een strafzaak zelf af te doen door een oordeel te geven over de strafrechtelijke aansprakelijkheid, eventueel gevolgd door een sanctie.[118]
De vervolgingsautoriteit heeft ook verantwoordelijkheden tijdens een opsporingsonderzoek. Hierbij is de openbaar aanklager gebonden aan het (formele) legaliteitsbeginsel. Indien er reden is om aan te nemen dat er een strafbaar feit is gepleegd, is de openbaar aanklager gebonden om een opsporingsonderzoek in te stellen. In geval van eenvoudige strafbare feiten (*enkel beskaffenhet*) wordt het onderzoek uitgevoerd door de politie, maar bij meer ingewikkelde zaken neemt de vervolgingsautoriteit de leiding in het opsporingsonderzoek.[119] De openbaar aanklager moet dat onderzoek objectief uitvoeren. Beslissingen in het opsporingsonderzoek die door de rechter worden genomen zoals voorarrest, cameratoezicht en aftappen van telefoon- en internetcommunicatie, komen aan de orde bij de meer ingewikkelde strafzaken. Het onderzoek hiernaar wordt geleid door een openbaar aanklager. Als de politie de opsporing zelfstandig uitvoert, heeft de openbaar aanklager geen juridische mogelijkheden de politie aan te sturen. Dit betekent dat indien de openbaar aanklager bepaalde maatregelen wil nemen in het opsporingsonderzoek, hij de leiding van het onderzoek moet overnemen (zie Hoofdstuk 23 artikel 3 Rgb). Het probleem is echter dat de openbaar aanklager doorgaans geen inzicht heeft in het onderzoek dat de politie zelfstandig uitvoert (Zila, 2006, p. 301).
In 2005 is de Åklagarmyndigheten (vervolgingsautoriteit) gereorganiseerd, waarbij de organisatie van drie naar twee organisatieniveaus is teruggegaan. Aan het hoofd staat de Aanklager-Generaal (*Riksåklagare*) en zijn Advies Commissie. Daaronder (2^{e} niveau) vallen 32 Lokale parketten, 4 Nationale parketten en 3 Internationale parketten.[120] Elk parket wordt weer aangestuurd door een Hoofd Openbaar aanklager (*chefåklagare*). Het aantal parketten bij elkaar opgeteld (39) is minder dan het aantal district rechtbanken (63). Verder zitten er in de organisatie van de Åklagarmyndigheten twee niveaus, terwijl de gerechten op drie niveaus zijn georganiseerd.

Rikskriminalpolisen
Evenals de Zweedse vervolgingsautoriteit, is ook de politie gebonden aan het (formele) legaliteitsbeginsel. Dit betekent dat indien er reden is om aan te nemen dat er een strafbaar feit is gepleegd, de politie een opsporingsonderzoek moet instellen.[121] Een dergelijk onderzoek kan in beginsel op drie manieren worden afgerond: de zaak wordt opgehelderd en overgedragen aan de openbaar aanklager voor verdere vervolging, het opsporingsonderzoek wordt gestaakt (Hoofdstuk 23 artikel 4 Rgb)[122] of het opsporingsonderzoek wordt overgenomen door de vervolgingsautoriteit (Zila, 2006, p. 296). Daarnaast heeft de politie evenals de openbaar aanklager de mogelijkheid om een oordeel uit te spreken over de strafrechtelijke aansprakelijkheid van de dader en eventueel een sanctie op te leggen (zie Hoofdstuk 48 Rgb) (Zila, 2006, p. 295 e.v.).
De organisatiestructuur van de Rijkspolitie bestaat, evenals die van de vervolgingsautoriteit, uit twee verschillende niveaus. Het laagste niveau omvat 21 politiekorpsen. Elk politiekorps beslist zelf over de eigen interne organisatie en om die reden kan de structuur enigszins verschillend zijn tussen de korpsen. Een van de onderdelen van elk politiekorps vormt de Regionale Recherche. Deze is verdeeld in verschillende eenheden, in de regel minstens vier, namelijk: een recherche eenheid, een drugseenheid, een eenheid voor economische delicten,

118 In vergelijkbare zin kennen wij in Nederland sinds kort de strafbeschikking.
119 De eindverantwoordelijkheid van de opsporing ligt altijd bij de openbaar aanklager, ook in geval de politie de opsporing zelfstandig uitvoert.
120 Zie http://www.aklagare.se. Anders Zila (2006, p. 287 e.v.), die spreekt over 43 OM-parketten (in plaats van in totaal 39).
121 Hierop bestaat één uitzondering, namelijk indien het een (vermeend) strafbaar feit betreft waarop slechts een boete is gesteld. Dan hoeft de politie het delict niet aan de openbaar aanklager te melden (*rapporteftergift*) (Carlson, 2009, p. 147).
122 De politie kan een onderzoek in een strafzaak niet staken vanwege het algemeen belang (public interest).

een technische ondersteuningseenheid en een openbare orde eenheid. De laatste kan weer worden onderverdeeld in (nog) kleinere politiediensten.[123]

10.1.3 Fasen in het strafproces

Anders dan in Nederland kent het Zweedse strafproces geen gerechtelijk vooronderzoek (Den Hartog, 2001, p. 330). Voorafgaande aan de strafzitting is in Zweden alleen de opsporingsfase. Na afloop van het opsporingsonderzoek beslist de openbaar aanklager of de strafzaak voor de rechter wordt gebracht (*åtalsunderlåtelse*). Het gerecht is vervolgens belast met het dagvaarden van de verdachte, nadat het daartoe een vordering van de openbaar aanklager heeft ontvangen (Den Hartog, 2001, p. 330).[124] De aanklager geeft het gerecht een overzicht van bewijsmiddelen die hij/zij ter zitting wil presenteren (Carlson, 2009, p. 152-153; Den Hartog, 2001, p. 330).
Vrijwel alle strafzaken worden in eerste instantie aangebracht bij een rechtbank (*Tingsrätterna*), waarvan Zweden er 63 telt. Hoger beroep kan worden ingesteld bij een van de zes gerechtshoven (*Hovrätterna*). Het arrest van een gerechtshof kan worden beoordeeld door de Zweedse Hoge Raad (*Högsta Domstolen*), maar alleen indien dit hoogste rechtscollege daar toestemming voor geeft. Dit geldt overigens voor beide procespartijen (zowel de aanklager als de verdediging).

10.2 De telefoon- en internettap in de praktijk

In hoofdstuk 23 Rgb is het opsporingsonderzoek (*förundersökning*) geregeld en in hoofdstuk 27 wordt aandacht besteed aan opsporingsmiddelen zoals aftappen van (tele)communicatie, gebruik van verkeersgegevens (de gegevens *over* het telefoon- en internetverkeer), videoregistratie en inbeslagname (van bewijsmateriaal).[125] Enkele bijzondere bepalingen betreffende het gebruik van zulke opsporingsmethoden staan in de Wet Maatregelen voor het Onderzoek naar Maatschappelijk Gevaarlijke Misdrijven (2008:854), de Wet Maatregelen ter Voorkoming van Bepaalde Gevaarlijke Misdrijven (2007:979), de Wet Procedures bij Gemeenten, Administratieve Instanties en Rechtbanken ten tijde van oorlog of oorlogsdreiging e.d. (1988:97) en de Wet Bijzondere Controle van Buitenlanders (1991:572). Het opnemen en afluisteren van vertrouwelijke communicatie (via bijvoorbeeld een microfoon of een bug op een toetsenbord), dus niet het aftappen van telefoon- en internetverkeer, is in Zweden thans nog geregeld door middel van een tijdelijke regeling. De vervolgingsautoriteit en de leiding van de Rijkspolitie hebben in een schrijven aan de regering (*Regeringens Skrivelse*) in 2010 verslag gedaan van de wijze waarop de regels betreffende het aftappen van telecommunicatie, het gebruik van verkeersgegevens van telefoongesprekken en de videoregistratie bij vooronderzoeken in strafzaken zijn toegepast in met name 2009 (*Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid fö rundersökning i brottmål under år 2009*).[126] Daarvan wordt in dit hoofdstuk gebruik gemaakt.

10.2.1 Het tapbevel en het autorisatieproces

Het aftappen van telecommunicatie mag alleen worden toegepast bij de verdenking van een strafbaar grondfeit waarop een gevangenisstraf van twee jaar of meer is gesteld. Dit betekent dat ook voor poging, voorbereiding of medeplichtigheid aan een dergelijk grondfeit, aftappen van telefoon- of internet mogelijk is. Het aftappen van telecommunicatie bij grondfeiten waarop minder dan twee jaar gevangenisstraf is gesteld, is alleen mogelijk

123 Het politiekorps van Stockholm is het grootste politiekorps in Zweden met ongeveer 6.700 medewerkers, waarvan 5.000 politieagenten. Zie verder http://www.polisen.se.
124 Zie schematisch weergegeven, Jehle (2006, p. 17).
125 De regeling van het opsporen en aftappen nader wordt besproken in paragraaf 10.2.3.
126 Hier verder aangeduid als: Regeringens Skrivelse 2010/11:66.

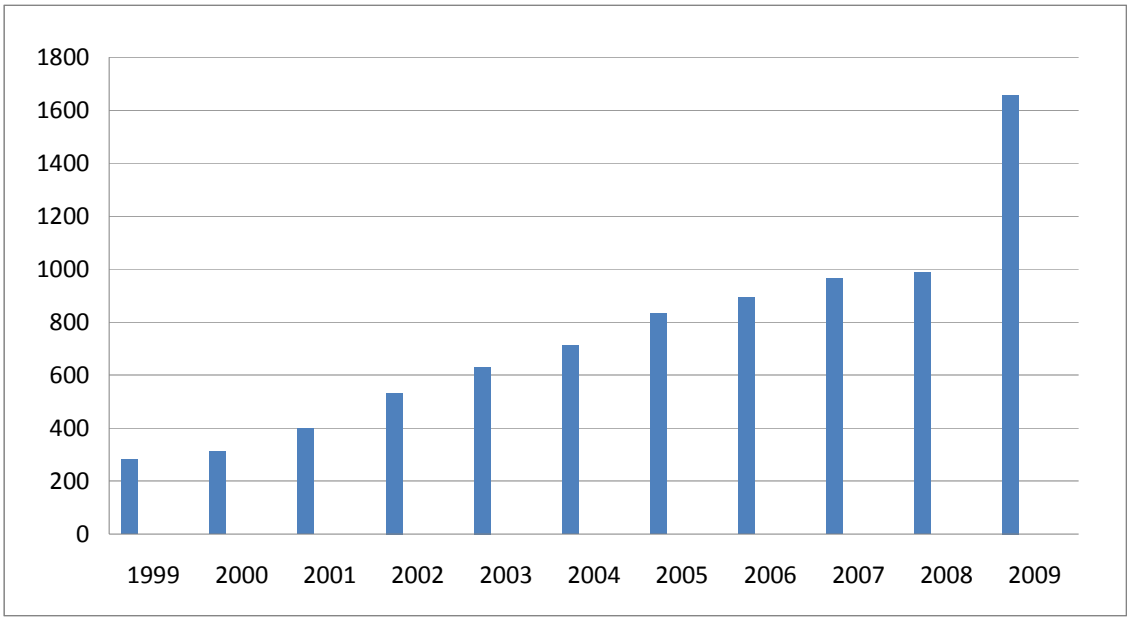
indien specifieke strafverzwarende omstandigheden zorgen dat de gevangenisstraf twee jaar of meer wordt (hoofdstuk 27 § 18 2e alinea Rgb).[127]
Verder is een voorwaarde voor het inzetten van de tap dat er een redelijk vermoeden van schuld bestaat tegen iemand. De maatregel dient verder van bijzonder belang te zijn voor het onderzoek (hoofdstuk 27 § 20 1e alinea Rgb). Het aftappen van telecommunicatie mag, behalve op telefoonnummers die in het bezit zijn van of gebruikt worden door de verdachte, ook uitgevoerd worden op nummers waarvan wordt aangenomen dat de verdachte er contact mee zal opnemen.
Voor het gebruik van opsporingsmiddelen, inclusief de telefoon- en internettap, gelden in Zweden drie algemene beginselen. Deze beginselen zijn het *doelbeginsel*, het *subsidiariteitsbeginsel* en het *proportionaliteitsbeginsel*.[128] Het doelbeginsel houdt in dat de bevoegdheid van een overheidsinstantie om een dwangmiddel als de telefoontap te gebruiken gekoppeld dient te zijn aan het doel waarvoor men heeft besloten het dwangmiddel in te zetten. Het subsidiariteitsbeginsel houdt in dat een instantie alleen een heimelijke opsporingsmethode mag gebruiken wanneer er duidelijk behoefte aan is *en* een minder ingrijpende maatregel niet voldoende is.[129] Het proportionaliteitsbeginsel, vastgelegd in hoofdstuk 27 § 1 (3e alinea) Rgb, houdt in dat een opsporings- of dwangmiddel uitsluitend mag worden ingezet als de redenen voor toepassing van dit middel opwegen tegen de inbreuk op de privacy of andere nadelen die het middel meebrengt voor de verdachte.
Indien de politie in een onderzoek de telefoontap wil gaan gebruiken, dan bespreekt de politie een dergelijke aanvraag (eerst) met de openbaar aanklager alvorens de aanvraag bij de rechtbank in te dienen.[130] Eén van de respondenten (een openbaar aanklager) vult dit aan door er op te wijzen dat, anders dan in Nederland, Zweden de figuur van de onderzoeksrechter niet kent. De openbaar aanklager beslist uiteindelijk of er voldoende reden is om een aanvraag voor een telefoontap te doen bij de rechtbank.
Een dergelijke aanvraag wordt volgens de geïnterviewde openbare aanklagers overigens alleen gedaan indien alle andere opsporingsmethoden geen mogelijkheden meer bieden om de zaak voor de politie verder te helpen (toepassing van het subsidiariteitsbeginsel).
Aanvragen voor het aftappen van telecommunicatie (tapbevelen), gebruik van verkeersgegevens van telecommunicatie en videoregistratie worden vervolgens getoetst door de rechtbank op verzoek van de openbaar aanklager, die een zodanig verzoek alleen zal doen indien daar voldoende grond voor is. Niettemin wordt een tapaanvraag soms door de rechter afgewezen. Een geïnterviewde openbare aanklager meldt dat indien een openbaar aanklager een afwijzing vreest, hij/zij de tapaanvraag voortijdig kan intrekken. Vervolgens kunnen verbeteringen of aanvullingen worden aangebracht en kan de aanvraag opnieuw worden ingediend.[131] Een tapbevel wordt door de rechter steeds afgegeven voor maximaal één maand. Een verlenging is mogelijk, maar een aanvraag daarvoor moet ook weer worden getoetst en toegewezen door de rechtbank. Ook een verlenging is maximaal één maand geldig.[132]
Om meer rechtszekerheidsgaranties te creëren bij de toetsing voor machtiging van gebruik van dwangmiddelen is in 2004 in Zweden de figuur van de Openbare Vertegenwoordiger *(Offentliga Ombud)* ingevoerd.[133] Deze Openbaar Vertegenwoordiger heeft de taak om de rechten en integriteitsbelangen van alle bij het aftappen betrokken individuen te bewaken en

127 Afluisteren via microphones (*bugging*) kan alleen als sprake is van een grondfeit waarop minimaal 4 jaar gevangenisstraf is gesteld. De reden dat voor bugging een zwaarder grondfeit is vereist dan voor het aftappen van een telefoon, wordt door een openbaar aanklager respondent de inbreuk op de persoonlijke levenssfeer genoemd (*integrity*).
128 Zie hoofdstuk 2 § 1 van het Regeringsform (Instrument van Overheid).
129 Daarmee lijkt dit beginsel sterk op het *subsidiariteitsbeginsel*.
130 Aldus een respondent die als Detective Inspector werkzaam is bij de Rikskriminalpolisen (Zweedse Politie).
131 Een nadeel dat kleeft aan het voortijdig intrekken en het vervolgens aanpassen van tapaanvragen, is dat er (veel) minder aanvragen door de rechtbank worden afgewezen. Dit kan tot het vertekende beeld leiden dat de rechter in Zweden (bijna) altijd een aanvraag direct goedkeurt.
132 Aldus (ook) een openbaar aanklager respondent. Een spoedtap, waarbij de Officier van Justitie in Nederland in eerste instantie over beslist, kent het Zweedse strafprocesrecht niet. Een openbaar aanklager zal altijd naar de rechter moeten voor de aanvraag van een tapbevel.
133 Zie nader over de Openbare Vertegenwoordiger (*Offentliga Ombud*) paragraaf 10.3.2.

kijkt daarbij ook naar de genoemde basisbeginselen voor het gebruik van dwangmiddelen (het subsidiariteitsbeginsel en het proportionaliteitsbeginsel). Een openbaar aanklager respondent legt uit dat bij de behandeling op de rechtbank van een tapaanvraag en een aanvraag voor het plaatsen van afluisterapparatuur (*bugging devices*), de Openbaar Vertegenwoordiger aanwezig is. Bij een tapaanvraag is de aanwezigheid van de Openbaar Vertegenwoordiger eventueel te omzeilen als de aanvraag snel wordt ingediend. In dat geval moet de Openbaar Vertegenwoordiger achteraf van de beslissing over de tapaanvraag op de hoogte worden gesteld. Bij de behandeling op de rechtbank van een aanvraag voor een zogenaamde *telephone surveillance*[134] hoeft de Openbaar Vertegenwoordiger niet aanwezig te zijn.

Grafiek 5 toont het totaal aantal (uitgegeven) tapbevelen voor de periode 1999 tot en met 2009. In Zweden kunnen er meerdere tapbevelen worden afgegeven op één persoon, en binnen elk bevel kunnen weer meerdere nummers of toestellen worden opgenomen.

Grafiek 5 Aantal tapbevelen



Bron: Regeringens Skrivelse 2010/11:66, p. 11

Uit het Regeringens Skrivelse (2010/11:66) blijkt dat de rechtbanken in 2009 in totaal 1.659 tapbevelen hebben afgegeven voor het aftappen van telecommunicatie betreffende in totaal 3.267 telefoonnummers.[135] In 2008, het jaar ervoor, waren dat er 990 en in 2007 betrof het 966 tapbevelen. Het totaal aantal tapbevelen steeg daarmee met circa 67% ten opzichte van het jaar ervoor (Regeringens Skrivelse 2010/11:66, p. 9). Volgens de respondenten van de Rijkspolitie en van de vervolgingsautoriteit is de nationale inzet tegen zware georganiseerde criminaliteit de voornaamste reden voor de grotere inzet van de tap als opsporingsmiddel. De gezamenlijke inzet van de overheidsinstanties tegen georganiseerde criminaliteit, die in 2009 van start ging, heeft geresulteerd in een stijging van het aantal opsporingsonderzoeken waarbij het aftappen van telecommunicatie is gebruikt (Regeringens Skrivelse 2010/11:66, p. 19). Voorts wordt er door deze respondenten op gewezen dat ook het aantal nummers per tapbevel fors stijgt vanwege de gestegen neiging in criminele kringen om frequent te wisselen van telefoon en telefoonnummer.

[134] Bij een 'telephone surveillance' kan bijvoorbeeld gedacht worden aan het in de gaten houden van een publieke telefoon in een telefooncel.

[135] Aangezien er meerdere machtigingen gegeven kunnen worden voor het afluisteren van dezelfde persoon, is het aantal machtigingen groter dan het aantal personen tegen wie het tapbevel is gericht.

Iedere machtiging voor het aftappen van telecommunicatie omvatte gemiddeld twee telefoonnummers. Het aftappen betrof in de meeste gevallen nummers die in het bezit waren van de verdachte.[136]
Van alle afgetapte nummers betrof 70% niet-geregistreerde telefoonkaarten in het bezit van de verdachte en 11% bleek betrekking te hebben op het mobiele telefoonabonnement of de vaste telefoon van de verdachte. Het resterende deel betrof abonnementen van een ander (3%) of andermans abonnement in de gemeenschappelijke woning (2%).
Vijf aanvragen tot machtiging voor het aftappen van telecommunicatie werden afgewezen. Dat is minder dan één procent van het totale aantal aanvragen.[137] Verder bleken bijna alle machtigingen voor het aftappen van telecommunicatie in 2009 te zijn uitgevoerd. Bij slechts 30 gevallen heeft men niet tot uitvoering over kunnen gaan. De redenen voor het niet uitvoeren van de machtiging bleken technische problemen, gebrek aan middelen of het feit dat de persoon op wie de machtiging betrekking had het land had verlaten dan wel was overleden (Regeringens Skrivelse 2010/11:66, p. 11).
Overigens moeten de bovenstaande cijfers volgens een respondent van de *Rikskriminalpolisen* enigszins gerelativeerd worden. Hij gaf aan dat de cijfers zoals geregistreerd in de Regeringens Skrivelse (2010/11:66) met betrekking tot het aantal tapbevelen niet geheel overeenkomt met het feitelijk aantal afgegeven tapbevelen, dat hoger blijkt te liggen. Klaarblijkelijk worden alleen taps op telefoonnummers geregistreerd.

Machtigingen voor alle heimelijke opsporingsmethoden
Ter vergelijking zijn er in 2009 in totaal 2.216 machtigingen gegeven voor *alle* heimelijke opsporingsmethoden bij in totaal 611 opsporingsonderzoeken. Dit betekent dat circa 75% van alle afgegeven machtigingen voor heimelijke opsporingsmethoden in dat jaar betrekking had op de telefoon- of internettap.[138] De andere 25% van alle machtigingen in 2009 betrof *andere heimelijke opsporingsmethoden*. Het totale aantal machtigingen steeg met circa 44% vergeleken met het jaar ervoor. Een directe verklaring voor deze stijging wordt niet gegeven, maar is wel af te leiden uit hetgeen in het Regeringens Skrivelse (2010/11:66) wordt gesteld over de nationale inzet tegen zware georganiseerde criminaliteit die in 2009 van start ging.[139]
Het totaal aantal machtigingen omvat 1.539 personen die verdacht waren van een misdrijf. Van de 611 opsporingsonderzoeken waren er 276 die betrekking hadden op één verdachte per onderzoek. De andere 335 opsporingsonderzoeken betroffen twee of meer verdachten. In totaal betrof het hier 1.263 verdachten, gemiddeld vier verdachten per onderzoek.[140] In een groot aantal vooronderzoeken werden meerdere machtigingen afgegeven voor de inzet van heimelijke opsporingsmethoden.
In 2009 werd tegen 303 verdachten een aanklacht ingediend. In 118 opsporingsonderzoeken was de openbare aanklager aan het einde van het jaar nog niet tot een besluit over al dan niet (verdere) vervolging gekomen. Eind 2009 waren er nog 107 lopende opsporingsonderzoeken.[141]

10.2.2 Machtigingen voor het gebruik van verkeersgegevens

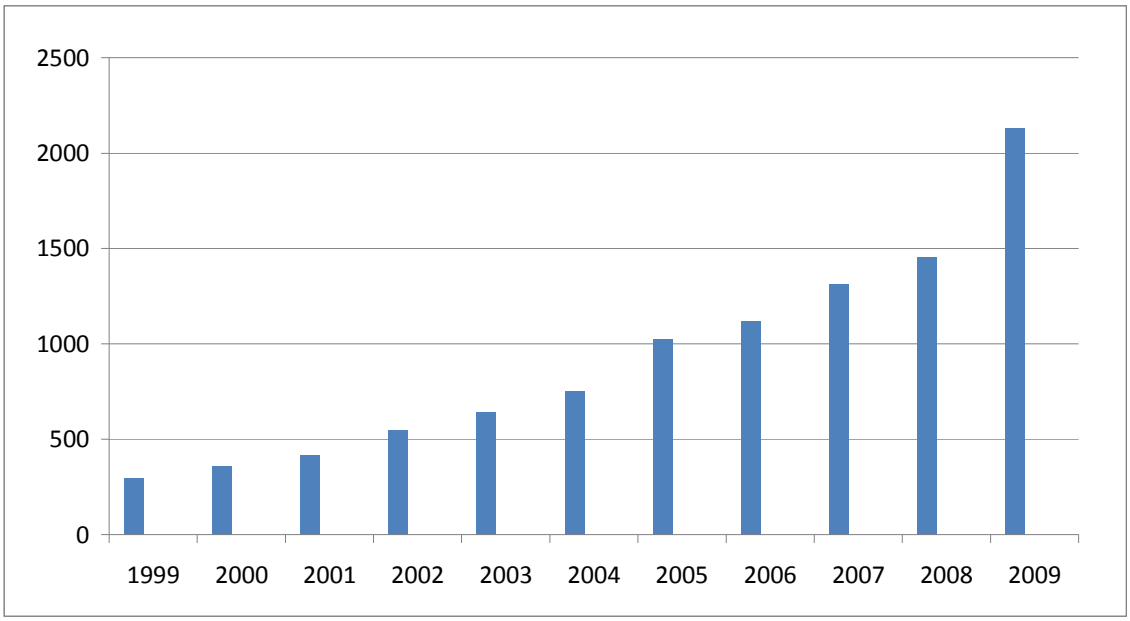
In Zweden houdt het gebruik van verkeersgegevens in dat gegevens die van en naar een bepaald telefoonnummer verstuurd worden, heimelijk worden binnengehaald, of dat voorkomen wordt dat zulke communicatie aankomt (hoofdstuk 27 § 19 1e alinea Rgb;

136 Uit het verslag van 2008 zou blijken dat amper 33% van de machtigingen van dat jaar betrekking had op telefoonnummers die in het bezit waren van een ander dan de verdachte, bijv. gemeenschappelijke huistelefoons of telefoonnummers die in het bezit waren van een werkgever. In 2009 daalde dit aandeel tot 20%. Zie Regeringens Skrivelse 2010/11:66, p. 10 (tevens refererend naar Regeringens Skrivelse 2009/10:66, p. 8).
137 Deze cijfers blijken op hetzelfde niveau te liggen als in het verslag van het voorgaande jaar (2008). Zie Regeringens Skrivelse 2010/11:66, p. 11.
138 Het totaal aantal machtigingen in 2009 minus het aantal tapbevelen in 2009 (zie Grafiek 6).
139 Zie hierboven in de hoofdtekst, gebaseerd op Regeringens Skrivelse 2010/11:66, p. 19.
140 *Idem*, p. 10.
141 De rest van de opsporingsonderzoeken waren op die datum reeds afgerond (Regeringens Skrivelse 2010/11:66, p. 10).

Regeringens Skrivelse 2010/11:66, p. 5). Er kunnen ook gegevens worden binnengehaald over e-mailadressen voor berichten die gestuurd worden (of zijn) van of naar het e-mailadres van de verdachte.[142]
Verkeersgegevens mogen in een opsporingsonderzoek alleen gebruikt worden bij een verdenking van een strafbaar grondfeit waarop 6 maanden of meer gevangenisstraf is gesteld. Ook voor poging, voorbereiding of medeplichtigheid aan een dergelijk grondfeit, mogen verkeersgegevens worden gebruikt (zie Hoofdstuk 27 § 19 2e alinea Rgb) zolang maar aan de 6 maanden eis wordt voldaan. Verder zijn dezelfde voorwaarden van toepassing als bij het aftappen van telefoon- en internetverkeer (Regeringens Skrivelse 2010/11:66, p. 6).

Grafiek 6 toont het aantal machtigingen voor het binnenhalen van verkeersgegevens voor de periode 1999 tot en met 2009. Deze machtigingen zijn inclusief de machtigingen die gecombineerd waren met het aftappen van telecommunicatie.

Grafiek 6 Aantal machtigingen voor het binnenhalen van verkeersgegevens



Bron: Regeringens Skrivelse 2010/11:66, p. 14

In 2009 zijn 2.134 machtigingen gegeven voor het binnenhalen van verkeersgegevens. Het aantal machtigingen voor het gebruik van verkeersgegevens steeg in 2009 met 47% ten opzichte 2008, toen er 1.455 machtigingen zijn afgegeven (Regeringens Skrivelse 2010/11:66, p. 13). In 2007 zijn in totaal 1.315 machtigingen afgegeven.
In het Regeringens Skrivelse (2010/11:66) wordt aangegeven dat opsporingsinstanties het noodzakelijk achten toegang te krijgen tot verkeersgegevens in verband met het aftappen van telecommunicatie, omdat deze gegevens inzicht bieden in de wijze waarop de tap doelmatig kan worden ingezet. Alle tapbevelen werden daarom gecombineerd met machtigingen voor het gebruik van verkeersgegevens. De aangegeven stijging hangt vooral samen met het aantal machtigingen voor het aftappen van telecommunicatie (Regeringens Skrivelse 2010/11:66, p. 13). De stijging van machtigingen voor uitsluitend het gebruik van verkeersgegevens bedroeg namelijk 2% in 2009 ten opzichte van het jaar ervoor. Het gemiddeld aantal dagen waarin verkeergegevens worden binnengehaald daalde echter met 35% (Regeringens Skrivelse 2010/11:66, p. 15).
In 2009 werd er in 11 gevallen een machtiging afgegeven voor het gebruik van verkeersgegevens na een internationaal rechtshulpverzoek in strafzaken. Verder werden er 6

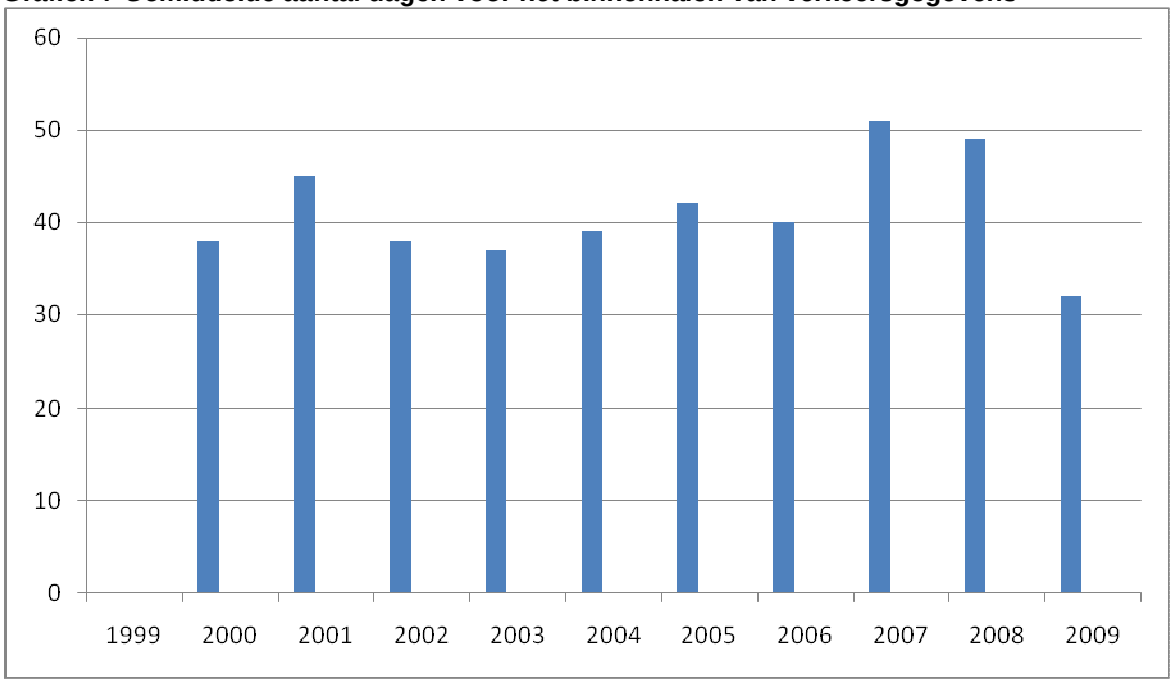
[142] Dit opsporingsmiddel geeft geen toegang tot de inhoud van de uitgewisselde telecommunicatie (Regeringens Skrivelse 2010/11:66, p. 6).

verzoeken tot machtigingen voor het gebruik van verkeersgegevens afgewezen (Regeringens Skrivelse 2010/11:66, p. 13).

Type strafbare feiten
Van de machtigingen voor uitsluitend het gebruik van verkeersgegevens in 2009 betrof 58% vermogensdelicten (zoals gekwalificeerde diefstal en zware oplichting), 22% geweldsdelicten (zoals moord, verkrachting en mensenhandel), 13% zware drugs- of smokkeldelicten, 2% economische delicten en 3% overige delicten (zoals zware brandstichting en zware strafbare feiten met betrekking tot vuurwapens) (Regeringens Skrivelse 2010/11:66, p. 14-15).

Gemiddelde tijd gebruik verkeersgegevens
Het gemiddeld aantal dagen waarop in 2009 verkeergegevens werden binnengehaald bedroeg 32 dagen. In 2008 bedroeg dat 49 dagen en in 2007 ging het om 51 dagen. In Grafiek 7 wordt de gemiddelde tijd van het binnenhalen van verkeersgegevens weergegeven voor de periode lopend van 2000 tot en met 2009. De cijfers zijn afgerond op hele dagen.

Grafiek 7 Gemiddelde aantal dagen voor het binnenhalen van verkeersgegevens



Bron: Regeringens Skrivelse 2010/11:66, p. 15

Er is voor 238 opsporingsonderzoeken een machtiging gegeven tot uitsluitend het gebruik van verkeersgegevens. Volgens het Regeringens Skrivelse (2010/11:66) is het gebruik ervan in 159 opsporingsonderzoeken nuttig geweest. Onder nuttig wordt verstaan dat de gegevens zijn gebruikt bij verhoren (54%), als bewijs bij de behandeling ter terechtzitting (38%), of hebben geleid tot vrijheidsontneming (8%).

10.2.3 Het gebruik van de tap

In Zweden mogen de volgende vormen van communicatie worden afgetapt: geluid, tekst, beeld, gegevens of verdere informatie die wordt doorgegeven met behulp van radio of door geluid of elektromagnetische golven die gebruik maken van een speciaal doorvoor bestemde geleider (hoofdstuk 6 § 19 van de Wet [2003:389] elektronische communicatie). De bepaling omvat telefonisch- en faxverkeer, e-mailverkeer, overdracht van datafiles door middel van FTP (File Transfer Protocol), als ook de overdracht vanaf websites, nieuwsgroepen en chatkanalen. Het aftappen van communicatie houdt in dat communicatie die doorgegeven wordt, of is, van en naar een telefoonnummer, een IP-adres, een code of een andere

telefonisch adres, heimelijk wordt afgetapt of opgenomen met een technisch hulpmiddel voor de weergave van de inhoud van de communicatie (zie hoofdstuk 27 § 18 1e alinea Rgb).[143] Verdachten van strafbare feiten en andere personen waar onderzoek naar wordt gedaan tijdens het opsporingsonderzoek, blijken volgens het Regeringens Skrivelse (2010/11:66) veelvuldig gebruik te maken van mobiele telefoons. De betreffende personen wisselen vaak van telefoon, telefoonnumers en telefoonkaarten. De betrokken Zweedse overheidsinstanties stellen dat de stijging van het aantal tapbevelen in 2009 ten dele moet worden toegeschreven aan de gestegen neiging binnen criminele kringen om te wisselen van telefoon en telefoonnummer.
Wat verder blijkt uit informatie van de respondenten is dat in de criminele kringen waarvan de telefoongesprekken worden afgeluisterd, tegenwoordig weinig informatie wordt uitgewisseld via de telefoon. Wanneer er binnen die kringen problemen rijzen, volgt er vaak wel telefonisch overleg tussen de personen die worden afgetapt.[144] Dat gebeurt dan in de zin van: "can we meet, we need to talk". Door gebruik te maken van de telefoontap in combinatie met afluisterapparatuur weet de politie dan vaak (al wel) wie de afgetapte persoon wil ontmoeten of waar de ontmoeting zal plaatsvinden.[145] Hoewel de inzet van afluisterapparatuur in de opsporing van strafbare feiten binnen Zweden steeds gebruikelijker blijkt te worden, blijft het in de praktijk toch veel tijd en menskracht vergen om het apparaat op de gewenste plek te installeren.[146]
De voornaamste reden voor de stijging van het aantal telefoontaps is echter de nationale inzet tegen zware georganiseerde criminaliteit, zo wordt duidelijk uit het Regeringens Skrivelse (2010/11:66). In dergelijke grote zaken werken de openbaar aanklager en de politie nauw samen volgens een respondent van het openbaar ministerie.
De gemiddelde aftaptijd in 2009 bedroeg 31 dagen en in 2008 was dat 47 dagen (Regeringens Skrivelse 2010/11:66, p. 12). Hoewel het aantal tapbevelen voor het aftappen van telecommunicatie in 2009 met 67% is gestegen, is de gemiddelde aftaptijd gerekend in dagen met 34% gedaald. De stijging van de totale aftaptijd gerekend in aantallen uren is 10% in 2009 (Regeringens Skrivelse 2010/11:66, p. 12).
Toch blijkt dat er tot nog toe in Zweden in relatief weinig zaken gebruik wordt gemaakt van heimelijke opsporingsmethoden, zoals de telefoontap (Regeringens Skrivelse 2010/11:66, p. 19). Een klein aantal omvangrijke opsporingsonderzoeken kan grote invloed hebben op de jaarcijfers. In het Regeringens Skrivelse (2010/11:66) wordt in dit verband als voorbeeld aangehaald een zaak waarin de afluistertijd vijf maanden bedroeg betrekking had op 29 verdachten, bijna 150 telefoons en 200 telefoonnummers (Regeringens Skrivelse 2010/11:66, p. 19). Door een respondent van het openbaar ministerie wordt gesteld dat opsporingsonderzoeken waarbij gebruik wordt gemaakt van telefoontaps soms wel kunnen oplopen tot 3 jaar. Hoewel dit uitzonderlijk lang is, blijkt dat binnen de internationale afdeling(en) van de Zweedse vervolgingsautoriteit telefoontaps vaker voor langere tijd worden gebruikt dan in nationale afdelingen van de Zweedse vervolgingsautoriteit. Dit komt omdat in de bestrijding van de georganiseerde criminaliteit, waar de internationale afdeling(en) zich op richt(en), het moeilijk blijkt te zijn om anders dan via telefoontaps en andere heimelijke opsporingsmiddelen, voldoende bewijsmateriaal te verzamelen om deze verdachten succesvol te kunnen vervolgen.

Type misdrijven
Van de tapbevelen die in 2008 werden afgegeven betrof 61% zware drugsdelicten, zware smokkeldelicten of allebei (Regeringens Skrivelse 2010/11:66, p. 11-12). Van de tapbevelen afgegeven in het jaar 2009 betrof 70% zware drugsdelicten of zware smokkeldelicten, 14% geweldsdelicten, 11% vermogensdelicten, 2% economische delicten en 3% overige delicten (Regeringens Skrivelse 2010/11:66, p. 11-12).

143 Aftappen kan, met bepaalde beperkingen, ook plaatsvinden buiten een openbaar toegankelijk telenetwerk, bijv. binnen een groter bedrijfsnetwerk.
144 Aldus Respondent C (openbaar aanklager).
145 Aldus Respondent C (openbaar aanklager).
146 Zo stelt Respondent D (openbaar aanklager). Ook blijkt de techniek van het afluisteren niet altijd optimaal, of kan geen gelegenheid worden gevonden om het afluisterapparaat te plaatsen.

Volgens het Regeringens Skrivelse 2010/11:66 is de toepassing van heimelijke opsporingsmiddelen nuttig geweest indien het (minimaal) heeft geleid tot gebruikmaking van voorarrest of andere dwangmiddelen of als de verzamelde gegevens zijn gebruikt bij verhoren. In 64% van de vooronderzoeken is doelmatig gebruik gemaakt van de heimelijke opsporingsmethoden (in boven genoemde zin). Opgesplitst naar de ingezette middelen was het aftappen van telecommunicatie van belang in 54% van de opsporingsonderzoeken, gebruik van verkeersgegevens (van telecommunicatie) in 67% en videoregistratie (camera-observatie) in 17%. Volgens de Zweedse regering laten deze cijfers zien dat de onderzochte heimelijke opsporingsmiddelen een zeer belangrijke functie vervullen bij het onderzoek naar strafbare feiten (Regeringens Skrivelse 2010/11:66, p. 22).

De internettap
De regelgeving met betrekking tot de telefoontap geldt ook voor de internettap. Respondenten van de politie (waaronder een Detective Superintendent, hoofd van een telefoontap-eenheid van de Rikskriminalpolisen (Zweedse Politie)) geven aan dat de internettap niet vaak wordt ingezet. De belangrijkste reden daavoor is dat het moeilijk is om uit de grote hoeveelheid informatie die met een internettap wordt binnengehaald de relevante informatie te filteren. Het scheiden van voor de opsporing relevante en niet-relevante informatie is volgens de politierespondenten een moeilijk proces. Daarnaast blijken er ook technische problemen, zoals het niet altijd kunnen beschikken over de meest recente software, aan het gebruik van de internettap in de weg te staan.

10.3 Waarborgen bij het gebruik van heimelijke opsporingsmiddelen

10.3.1 Inbreuk op het recht op privacy

In hoofdstuk 2 van het Instrument van Overheid (*Regeringsform*) zijn voorschriften opgenomen over de fundamentele vrijheden en rechten. Hierin komt naar voren dat iedere burger tegenover de overheid beschermd moet worden tegen huisvredebreuk en soortgelijke inbreuken, tegen het onderzoek van brieven en andere vertrouwelijke postverzendingen en tegen het aftappen of opnemen van telefoongesprekken of andere vertrouwelijke mededelingen (§ 6). Deze fundamentele vrijheden en rechten mogen uitsluitend beperkt worden door de wet en alleen om tegemoet te komen aan doelen die aanvaardbaar zijn in een democratische maatschappij. De beperkingen mogen nooit verder gaan dan noodzakelijk is of een bedreiging vormen voor de vrijheid van meningsvorming (§ 12).
Daarnaast wordt in artikel 8 lid 1 EVRM bepaald dat een ieder recht heeft op eerbiediging van het privé- en gezinsleven, huis en correspondentie. Zoals gezegd wordt in lid 2 van genoemde bepaling aangegeven dat onder bepaalde voorwaarden het openbaar gezag inbreuk kan maken op de hoofdregel van lid 1. Die inbreuk moet dan zijn: *in accordance with the law, in the interests of among other the prevention of disorder or crime or the rights and freedoms of others* en *necessary in a democratic society*. Elke Lidstaat heeft hierbij enige interpretatieruimte (*margin of appreciation*).
Via de Wet betreffende het Europees Verdrag tot Bescherming van de Rechten van de Mens en de fundamentele vrijheden (1994:1219) is het Europese Verdrag sinds 1 januari 1995 in het Zweedse recht opgenomen.[147] Zo is in hoofdstuk 2 § 23 van het Instrument van Overheid voorgeschreven dat een wet of ander voorschrift niet in strijd mag zijn met de verplichtingen die Zweden heeft op grond van het Europees Verdrag. Het recht op bescherming van het privé- en gezinsleven omvat ook de bescherming tegen diverse vormen van aftappen van telecommunicatie. Opsporingsmiddelen die een aantasting met zich brengen van de private sfeer, die volgens artikel 8 EVRM beschermd dient te worden, kunnen volgens het Europees Verdrag alleen geaccepteerd worden als ze ondersteund worden door de wet en onder de uitzonderingen vallen die worden aangegeven in artikel 8 lid 2 EVRM. De bepalingen over het aftappen van telecommunicatie, het binnenhalen van

[147] Zweden is lid van de Raad van Europa sinds de oprichting (5 mei 1949) en heeft het Europees Verdrag voor de Rechten van de Mens (EVRM) geratificeerd op 4 februari 1952.

verkeergegevens en videoregistratie, vormen een voor de criminaliteitsbestrijding noodzakelijke uitzondering op de bescherming tegen inbreuk op het privéleven en de correspondentie van het individu.
Met name de voorwaarden *accordance with the law* en *necessary in a democratic society* worden als toetsingsgronden door het Europees Hof voor de rechten van de mens (EHRM) gebruikt om nadere invulling te geven aan artikel 8 lid 2 EVRM (Krabbe, 2004, p. 161). In de voorwaarde 'necessary in a democratic society' ligt een proportionaliteitstoets besloten waaraan het EHRM redelijk strak de hand houdt (Bleichrodt et al., 2011, p. 145). Deze toets houdt ondermeer in dat de intensiteit van de inbreuk wordt afgewogen tegen de beperking (op het recht op privacy) die daarmee wordt gediend (Bleichrodt et al., 2011, p. 145). Zo is de Zweedse regering van mening dat het aantal afgeluisterde uren van grotere betekenis is voor de mate waarin inbreuk is gemaakt op de integriteit, dan het aantal machtigingen of het aantal nummers dat wordt getapt. Met name geldt dit in gevallen waarin een nieuw tapbevel gericht is tegen dezelfde persoon die herhaaldelijk van telefoon wisselt (Regeringens Skrivelse 2010/11:66, p. 20). Vandaar dat de intensiteit van het tappen in Zweden nadrukkelijk wordt meegenomen in de overwegingen.

10.3.2 Openbaar Vertegenwoordiger (Offentliga Ombud)

Op 1 oktober 2004 is er een systeem ingevoerd voor Openbaar Vertegenwoordigers betreffende het afluisteren van telecommunicatie en heimelijke cameraobservatie. Het doel was om verdere rechtszekerheidsgaranties te creëren bij de toetsing voor een machtiging.[148] De Openbaar Vertegenwoordiger is de tegenhanger van de openbaar aanklager bij zittingen voor de rechtbank en heeft als taak om de rechten en integriteitbelangen van individuen in het algemeen te bewaken. Hij/zij dient alle aspecten naar voren te brengen, waaronder ook de bescherming van de integriteit van derden. De Openbaar Vertegenwoordiger dient er ook op toe te zien dat de basisbeginselen voor het gebruik van dwangmiddelen (inclusief het gebruik van het aftappen van telefoon- en internetcommunicatie) worden toegepast, dat wil zeggen het doelbeginsel, het subsidiariteitsbeginsel en het proportionaliteitsbeginsel.[149] De Openbaar Vertegenwoordiger dient toegang te hebben tot al het materiaal dat de basis vormt voor toetsing door de rechtbank. Hij heeft de mogelijkheid zich in de zaak uit te spreken en het recht om tegen de beslissing van de rechtbank in hoger beroep te gaan.

10.3.3 Veiligheid- en Iintegriteitbeschermingscommissie

Per 1 januari 2008 is er in Zweden een nieuwe overheidsinstantie opgericht, de Veiligheid- en Integriteitbeschermingscommissie (*Säkerhets- och Integritetsskyddsnämnden)*. Deze commissie ziet toe op onder andere het gebruik van heimelijke opsporingsmiddelen door misdaadbestrijdende overheidsinstanties en daarmee verband houdende activiteiten. Het toezicht van de commissie omvat ook het werkterrein van de veiligheidspolitie. De commissie dient ook op verzoek van individuen bijvoorbeeld te controleren of het individu is blootgesteld aan heimelijke opsporingsmiddelen en of dit gebeurd is in overeenstemming met de wet. In dit verband wordt door een van de resondenten (openbaar aanklager) naar voren gebracht dat iedere burger in Zweden naar de Veiligheid- en Integriteitbeschermingscommissie kan gaan met het verzoek om na te gaan of er tegen hem of haar heimelijke opsporingsmiddelen zijn toegepast. Politie en justitie moeten meewerken aan een door deze commissie ingesteld onderzoek. Deze commissie toetst echter alleen de (on)rechtmatigheid van het overheidsoptreden. De aanvrager (burger) wordt ook alleen daarover geïnformeerd. Indien de aanvrager bijvoorbeeld wel onderworpen is geweest aan een telefoontap, maar de inzet van de tap in de ogen van de commissie rechtmatig is toegepast, zal de aanvrager alleen te horen krijgen dat er jegens hem of haar geen sprake is geweest van onrechtmatig overheidsoptreden. Indien uit het onderzoek van de Veiligheid- en Integriteitbeschermingscommissie echter blijkt dat de telefoontap in strijd met de regels is

[148] Wetsvoorstel 2002/03:74, commissieverslag 2003/04:JuU12, zie o.a. Regeringens Skrivelse 2003/04:14.
[149] Zie hiervoor, paragraaf 10.2.1.

ingezet, dan wordt de aanvrager daarover wel geïnformeerd en gewezen op de mogelijkheid van een schadevergoeding.

10.3.4 Notificatie

Op 1 januari 2008 zijn er verdere rechtszekerheidsgaranties ingevoerd voor het gebruik van heimelijke opsporingsmiddelen.[150] Verdachten of voormalig verdachten van strafbare feiten, waarvan een telefoonnummer bij de politie of het openbaar ministerie bekend is, moeten achteraf op de hoogte worden gesteld van het feit dat ze aan een heimelijk opsporingsmiddel zijn onderworpen.[151] Indien het vooronderzoek niet geschaad wordt, moet hiervan melding worden gemaakt uiterlijk een maand na afronding van het onderzoek. Melding dient echter uitgesteld te worden als de gegevens vallen onder de bepalingen van de Wet Openbaarheid en Geheimhouding (2009:400). Het is aan de openbaar aanklager om te bepalen of sprake is van omstandigheden die aan het notificeren in de weg staan. Volgens een geïnterviewde openbaar aanklager wordt er in ieder geval bij de opsporing van georganiseerde criminaliteit in de meeste gevallen niet genotificeerd, om toekomstig onderzoek niet in gevaar te brengen.[152] Indien men vanwege geheimhouding binnen een jaar na afronding van het opsporingsonderzoek geen melding heeft kunnen doen, dan mag het bericht achterwege blijven.

In de praktijk is het volgens een geïnterviewde openbaar aanklager soms moeilijk om de identificerende gegevens te achterhalen van personen die zijn afgeluisterd, omdat de afgetapte telefoonnummers niet, of onder valse namen, geregistreerd staan. In die gevallen blijft notificatie (noodgedwongen) achterwege. Als de verdachte vervolgd wordt, komt in de behandeling ter zitting meestal wel naar voren dat er gebruik is gemaakt van een (of meerdere) telefoontap(s). In sommige gevallen wordt een verdachte echter niet vervolgd wegens gebrek aan bewijs. In dat geval kan de openbaar aanklager er volgens de respondent voor kiezen om toch te notificeren. Over de notificatieregeling is deze respondent van mening dat het veel administratief werk met zich meebrengt, hetgeen ten koste gaat van ander werk.

Onder deze notificatieplicht vallen geen onderzoeken naar misdrijven die vallen binnen de competentie van de veiligheidspolitie (*Säkerhetspolisens*), dat wil zeggen misdrijven tegen de nationale veiligheid, sabotage en terroristische misdrijven.

10.4 Concluderend

Het Zweedse strafproces kent geen gerechtelijk vooronderzoek, slechts een opsporingsonderzoek waarbij de openbaar aanklager na afloop beslist of de strafzaak voor de rechter wordt gebracht of niet. Het aftappen van telefoon- en internetverkeer wordt uitgevoerd tijdens het opsporingsonderzoek. Voor het gebruik van de telefoon- en internettap, gelden in Zweden drie algemene beginselen, het *doelbeginsel*, het *subsidiariteitsbeginsel* en het *proportionaliteitsbeginsel*. Het doelbeginsel houdt in dat er een koppeling is tussen de bevoegdheid om een opsporingsmiddel zoals de telefoontap in te zetten en het doel waarvoor men dit middel wil gebruiken. Het subsidiariteitsbeginsel houdt in dat een instantie alleen een tap mag gebruiken wanneer er behoefte aan is en tevens een minder ingrijpende maatregel niet afdoende is, waarmee het *subsidiariteitsbeginsel* wordt omschreven. Het proportionaliteitsbeginsel ten slotte, houdt in dat een tap alleen mag worden ingezet indien de redenen voor toepassing ervan opwegen tegen de inbreuk op de

[150] Wetsvoorstel 2006/07:133, commissieverslag 2007/08:JuU3, zie o.a. Regeringens Skrivelse 2007/08:11.

[151] Op dit moment is nog niet duidelijk of ook voor de nieuwe wet geldt dat auteurs van de onderschepte internet- en telefoonberichten achteraf op de hoogte moeten worden gesteld van het aftappen.

[152] Met notificeren wordt de betrokkene er immers van op de hoogte gesteld dat hij/zij door de politie wordt gevolgd. Dat kan toekomstig opsporingsonderzoek van die persoon bemoeilijken.

privacy en tegen andere nadelen die de inzet van het middel met zich mee brengt. In Zweden mag, de tap zowel worden ingezet op nummers die gebruikt worden door de verdachte als op nummers waarvan vermoed wordt dat de verdachte er contact mee zal opnemen.
Er blijkt in Zweden weinig gebruik gemaakt te worden van de telefoon- en internettap. Een klein aantal omvangrijke opsporingsonderzoeken kan daardoor grote invloed hebben op de jaarcijfers, zo blijkt uit het Regeringens Skrivelse (2010/11:66). Uit de vraaggesprekken komt naar voren dat de internationale afdeling(en) van de Zweedse vervolgingsautoriteit vaker voor langere tijd gebruik maken van de telefoon- en internettap dan de nationale afdelingen van de Zweedse vervolgingsautoriteit. Dit komt vooral doordat het bij de bestrijding van de georganiseerde criminaliteit – waar de internationale afdeling(en) zich vooral op richten – moeilijk is om buiten het gebruik van de telefoon- en internettap, voldoende bewijsmateriaal te verzamelen.
Wat betreft de verhouding tussen verschillende heimelijke opsporingsmiddelen, zoals tappen, infiltreren en opnemen vertrouwelijke communicatie blijkt de tap het vaakst ingezet te worden. Bij de aanpal van zware criminaliteit is er echter vaak sprake van een combinatie van heimelijke opsporingsmethoden. Respondenten geven aan dat afluisterapparatuur (bugging) een heimelijk opsporingsmiddel is dat over de hele breedte complementair is aan de telefoontap en goed in combinatie met de tap kan worden ingezet.
Uit het Regeringens Skrivelse (2010/11:66) blijkt dat het totaal aantal tapbevelen in 2009 met circa 67% is gestegen ten opzichte van het jaar ervoor. Als verklaring voor deze stijging wordt gewezen op de nationale inzet tegen zware georganiseerde criminaliteit die in 2009 van start ging. Dit heeft geresulteerd in een stijging van het aantal opsporingsonderzoeken waarbij het aftappen van telecommunicatie wordt gebruikt. Ook het aantal machtigingen afgegeven voor het binnenhalen van verkeersgegevens is in 2009 met 47% gestegen ten opzichte van 2008. Deze laatste stijging hangt samen met het aantal machtigingen voor het aftappen van telecommunicatie. De gemiddelde aftaptijd gerekend in dagen daalde in 2009 met 34% ten opzichte van het jaar ervoor. Ook het gemiddeld aantal dagen waarin verkeergegevens werden binnengehaald daalde in 2009 met 35% vergeleken met het jaar ervoor. Uit de Zweedse statistieken komt naar voren dat het aftappen van telecommunicatie een belangrijke functie vervult in het opsporingsproces. De inzet van de tap bleek in 54% van de gevallen een bijdrage te leveren aan het onderzoek. Verkeersgegevens van telecommunicatie leverden in 67% van de gevallen zinvolle opsporingsinformatie op.
In Zweden wordt de intensiteit van het tappen nadrukkelijk wordt meegenomen in de overwegingen. Verder blijkt er in het Zweedse strafrechtssysteem relatief veel aandacht besteed te worden aan het creëren van waarborgen rond het aftappen van telefoon- en internetverkeer. Hierbij valt met name de figuur van de Openbaar Vertegenwoordiger op, die aan het begin van de procedure (min of meer in abstracto) moet waken over de rechten en integriteitbelangen van individuen, waaronder ook de bescherming van de integriteit van derden.

11 Het gebruik van de tap in Duitsland

Duitsland is het derde land waar het landenvergelijkend onderzoek inzake het gebruik van de telefoon- en internettap als opsporingsmethode, zich op richt. Het is het buurland van Nederland en het land heeft 82 miljoen inwoners.[153] In 1990 is het land herenigd waarbij de Duitse Democratische Republiek feitelijk is opgegaan in de Bondsrepubliek Duitsland.[154] De staatsmacht is in Duitsland niet gecentraliseerd. Het land is een federale democratische en constitutionele republiek (*Bundesrepublik*) en bestaat naast de centrale staat (*Zentralstaat*) uit zestien deelstaten (*Länder*). Elke deelstaat is eigenlijk een ministaat met een eigen constitutie (*Landesverfassung*), een parlement (*Landtag*) en een regering (*Landesregierung*). Behalve Berlijn en Sleeswijk-Holstein hebben alle deelstaten ook een eigen Constitutioneel Hof (*Verfassungsgerichtshof*) (Fisher, 2009, p. 15). Belangrijke federale organen (*oberste Bundesorgane*) zijn het parlement (*Bundestag*), de Federale Raad (*Bundesrat*)[155], de president, de regering (*Bundesregierung*) en het Federale Constitutionele Hof (*Bundesverfassungsgericht; BVerfG*) (Fisher, 2009, p. 11). De Federale Constitutie (*Grundgesetz; GG*) dateert van 23 mei 1949 en heeft in artikel 23 GG opgenomen dat het recht van de Europese Unie voorrang heeft op Duits recht. Het land is sinds 13 juli 1950 lid van de Raad van Europa en heeft het Europees Verdrag voor de Rechten van de Mens (EVRM) geratificeerd op 5 december 1952.[156]

In het navolgende wordt allereerst in paragraaf 11.1 kort ingegaan op enkele algemene trekken van het Duitse strafrechtsysteem. Ook worden hier de overheidsorganen die te maken hebben met de telefoon- en internettap als opsporingsmiddel beschreven. In de daaropvolgende paragraaf (11.2) komt de praktijk van de telefoon- en internettap aan de orde. Hierin wordt het autorisatieproces, het gebruik van verkeersgegevens, het gebruik van de telefoon- en de internettap en afluisterapparatuur beschreven. In de volgende paragraaf (11.3) staan de waarborgen bij het gebruik van heimelijke opsporingsmiddelen centraal. Het hoofdstuk wordt afgesloten met een samenvatting van de belangrijkste punten in paragraaf 11.4.

11.1 Het Duitse strafrechtssysteem

11.1.1 Karakteristieken

Het Duitse rechtssysteem kenmerkt zich onder andere door een onderscheid in Publiek (*öffentliches Recht*) en Privaat recht.[157] Belangrijke rechtsgebieden binnen het Duitse publiekrecht zijn het strafrecht en het strafprocesrecht. In het Duitse wetboek van strafrecht (*Strafgesetzbuch; StGB*), dat dateert van 15 mei 1871 is het legaliteitsbeginsel[158] vastgelegd in § 1 StGB (en in artikel 103(*ii*) GG). In Duitsland bestaat een sterke binding van de wetgever en de magistratuur aan de (formele) wet (*Bindung an das Gesetz*), om het risico

153 Zie http://europa.eu/abc/european_countries/eu_members/germany/index_en.htm.
154 In het vervolg wordt hier gesproken van Duitsland.
155 Een belangrijke taak van de Federale Raad is het behartigen van de belangen van de deelstaten vis-à-vis de federale staat en indirect vis-à-vis de Europese Unie. Zie www.bundesrat.de.
156 Toen nog gescheiden van de Duitse Democratische Republiek (DDR), maar onder dezelfde naam als heden: Bondsrepubliek Duitsland (BRD) 1949-1990.
157 *Idem*, p. 27 e.v. Een onderscheid dat wij in Nederland ook kennen.
158 Het legaliteitsbeginsel beoogt de wettelijke (en volgens Corstens ook de democratische) grondslag van de strafrechtspleging te verzekeren (Corstens, 2008, p. 15). Ook in Nederland is het legaliteitsbeginsel verankerd in de wet (zie artikel 1 Sv [strafvorderlijk legaliteitsbeginsel] en artikel 1 Sr en artikel 16 GW [materieelrechtelijk legaliteitsbeginsel]). Ook op supranationaalniveau is het materieelrechtelijk legaliteitsbeginsel vastgelegd, namelijk in artikel 7 lid 1 EVRM en artikel 15 lid 1 IVBP.

op rechtsonzekerheid zo klein mogelijk te houden (Fisher, 2009, p. 243-244; Krey, 2009a, p. 34).

Het strafprocesrecht wordt geregeld op federaal niveau, in het wetboek van strafvordering (*Strafprozeßordnung; StPO*).[159] Aanvullend daarop wordt in de Duitse wet betreffende de rechterlijke macht (*Gerichtsverfassungsgesetz; GVG*) het functioneren en de jurisdictie van de strafgerechten geregeld. Het Duitse strafprocesrecht is oorspronkelijk een *inquisitor* procesrecht,[160] maar heden ten dage bevat het strafprocesrecht elementen van zowel het *accusator* als het *inquisitor* systeem.[161]

Verder wordt in het Duitse publiekrecht een onderscheid gemaakt tussen het *Polizeirecht* (ook wel *Ordnungsrecht* of *Sicherheitsrecht* genoemd) enerzijds en het *Straf(prozeß)recht* anderzijds.[162] Het onderscheid komt voort uit het Duitse materiële politiebegrip (Bleichrodt et al., 2011, p. 77 e.v.). Daaruit volgt dat het afwenden van gevaar (*Gefahrenabwehr*) onder andere een taak is van de politie. Ook andere bestuurlijke organen kunnen met Gefahrenabwehr belast zijn, maar dan is geen sprake van Polizeirecht (Bleichrodt et al., 2011, p. 77 e.v.). Over de verhouding tussen de beide rechtsgebieden kan worden opgemerkt dat het straf(proces)recht begint daar waar het overheidsoptreden ter afwending van gevaar van herhaling ophoudt (Bleichrodt et al., 2011, p. 79). Echter elk overheidsoptreden waarbij inbreuk wordt gemaakt op de grondrechten van burgers moet zijn gebaseerd op een voorziening in de wet die de grondslag voor het overheidsingrijpen ook in concreto regelt (Bleichrodt et al., 2011, p. 82). Genoemd ingrijpen moet in proportionaliteit staan tot de grondwetsinbreuk, hetgeen door de rechter moet worden getoetst. Dat geldt zowel voor het concrete optreden als voor de wettelijke regeling als zodanig.

11.1.2 Enkele organen binnen het Duitse strafrechtssysteem

Het politierecht wordt geregeld op het niveau van de deelstaten.[163] Hierop zijn echter twee uitzonderingen van toepassing. Ten eerste het Federale Bureau voor Strafrechtelijk Onderzoek (*Bundeskriminalamt*) en ten tweede de federale politie (*Bundespolizei*). Beide federale organisaties zijn onttrokken aan de verantwoordelijkheid van de deelstaten.

Hieronder wordt kort ingegaan op een aantal organen binnen het Duitse (straf)rechtssysteem die zich in het kader van opsporing van (vermeend) strafbare feiten bezighouden met het aftappen van internet en telefoons. Dit betreft de Duitse vervolgingsautoriteit, de politie van de deelstaten, de federale politie (Bundespolizei) en het Bundeskriminalamt.

159 Het Duitse wetboek van Strafvordering dateert van 1 februari 1877.

160 Bij een inquisitor strafproces moet worden gedacht aan een systeem waarbij de focus is gericht op de *vervolging van een (vermeend) strafbaar feit*. De verdachte is hierin een object van onderzoek. Presentatieregels voor het bewijs ontbreken (grotendeels) en op de strafzitting wordt gebruik gemaakt van een dossier waarin schriftelijke bewijsstukken zitten die door de vervolgende instantie zijn vergaard in eerdere fasen van het onderzoek. Daarbij zijn de procedureregels gecodificeerd in een wetboek. Een puur inquisitor strafproces is een theoretisch model dat in de praktijk niet wordt toegepast.

161 Aldus Fisher, 2009, p. 262. Het voert te ver om binnen het bestek van deze bijdrage de ontwikkeling op dit punt van het Duitse strafprocesrecht nader in te gaan. Wel kan kort worden aangegeven wat onder een accusator/adversarial strafproces moet worden verstaan. De termen *accusator* en *adversarial* worden doorgaans als synoniemen gebruikt. Kenmerkend voor deze procesvorm is dat het gericht is op *conflictoplossing*. Hierbij geldt dat de beide procespartijen (de openbaar aanklager en de verdachte) gelijkwaardig zijn en een actieve rol spelen in het proces. De taak van de rechter is om er op toe te zien dat de presentatieregels voor bewijs worden nageleefd en dat de jury wordt geïnformeerd over haar taken. Echter, ook hier geldt dat een puur accusator/adversarial strafproces een theoretisch model is dat in de praktijk niet als zodanig voorkomt.

162 Zie voor een vereenvoudigd schema van het Duitse strafrechtssysteem, Jehle (2006, p. 18).

163 Meer hierover onder het kopje 'Politie van de deelstaten en de Bundespolizei'.

Staatsanwaltschaft (*Anklagebehörde*)
Op basis van § 141 van het *Gerichtsverfassungsgesetz* (GVG) is aan elk gerecht in Duitsland een vervolgingsautoriteit (*Anklagebehörde*) verbonden die het vervolgingsmonopolie (*Anklagemonopol*) heeft. *De* vervolgingsautoriteit bestaat niet in Duitsland. Elke deelstaat heeft een eigen *Staatsanwaltschaft* die op het hoogste niveau wordt aangestuurd door een minister van justitie van de deelstaat.[164] Deze (politieke) persoon kan alle Staatsanwälte van de deelstaat instructies geven (zie § 146 GVG). De Staatsanwaltschaft is een hiërarchische organisatie, met op het hoogste ambtelijke niveau een Advocaat-Generaal die is verbonden aan een gerechtshof (*Oberlandesgericht*) in de deelstaat (Fisher, 2009, p. 264; Krey, 2009a, p. 74-78; Juy-Birmann, 2002, p. 298-299). De deelstaten hebben richtlijnen inzake de organisatie en de werking van de Staatsanwaltschaft (*Anordnungen über Organisation und Dienstbetrieb der Staatsanwaltschaft*). Daarnaast bestaat er een federale vervolgingsautoriteit, met een vergelijkbare structuur. Aan het hoofd van deze organisatie staat de federale minister van justitie, met daaronder de federale Advocaat-Generaal (*Generalbundesanwalt*) die verbonden is aan het *Bundesgerichtshof*.[165]

In beginsel worden de taken van de openbaar aanklager uitgeoefend door de Staatsanwalt, zijnde de openbaar aanklager van de betreffende deelstaat (zie artikel 30 en 83 GG en §§ 141 GVG). De *Generalbundesanwaltschaft* treedt op in cassatie- en bij klachtzaken voor het Bundesgerichtshof en in geval een strafzaak in eerste instantie moet worden aangebracht bij het Oberlandesgericht.

Politie van de deelstaten en de Bundespolizei
Het onderscheid dat wordt gemaakt tussen het Polizeirecht en het Straf(prozeβ)recht heeft ook invloed op de wijze waarop de politie in Duitsland is georganiseerd en wordt bestuurd.[166] Met betrekking tot de openbare orde hebben de deelstaten hun eigen politieregelingen en bevoegdheden.[167] Hoewel het gevaar bestaat dat de regelingen van de verschillende deelstaten sterk uiteen lopen, blijkt dat niet het geval te zijn. Hetzelfde geldt ten aanzien van de inrichting van de bevoegdheden van de politie van de deelstaten,[168] die is onderverdeeld in geuniformde politie (*Polizeipräsidien),* recherche (*Landeskriminalamt*) en de waterpolitie (Krey, 2009a, p. 96). Zowel de Polizeipräsidien als de Landeskriminalamt hebben opsporingsbevoegdheden met betrekking tot (vermeend) strafbare feiten (zie § 84 van de *Polizei- und Ordnungsbehördengesetz*). Toch richt de recherche zich op de opsporing van zwaardere vergrijpen en is zij het aanspreekpunt voor de Staatanwalt.

Proactief optreden van de politie, in de zin dat van een verdenking van een strafbaar feit (nog) geen sprake is, wordt gerekend tot de taak van het afwenden van gevaar (*Gefahrenabwehr*) (Krey, 2009a, p. 92 e.v.).[169] De vraag in hoeverre dergelijke proactieve maatregelen van de politie vallen onder het bereik van het federale strafprocesrecht, is in Duitsland aanleiding geweest tot een langdurige discussie.[170] In 2005 heeft het

[164] Staatsanwälte hebben niet de onafhankelijke positie die rechters bezitten, zie onder andere Juy-Birmann, 2002, p. 298-299. In Frankfurt (am Main) (deelstaat Hessen) bestaat de Staatsanwaltschaft uit 300 medewerkers waaronder een zogenaamde *Leitender Oberstaatsanwalt*, een *Stellvertretender Leitender Oberstaatsanwalt*, negentien *Oberstaatsanwältinnen/anwälte*, 88 *Staatsanwältinnen/anwälte*, negentien *Rechtspfleger/innen* en zeven *Gerichtshelfer/innen*. Zie http://www.sta-frankfurt.justiz.hessen.de.

[165] Zie o.a. Krey (2009*a*, p. 74-78). Verder is het mogelijk voor een burger om in bepaalde gevallen een strafvervolging in te stellen (*Privatklage*) (Fisher, 2009, p. 264).

[166] Vergelijk Bleichrodt et al. (2011, p. 78 e.v.).

[167] *Idem*, p. 78-79.

[168] *Idem*, p. 80-81. Bleichrodt, Mevis en Volker (2011) wijzen in dit kader op het bestaan van een *Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und die Länder*.

[169] Voorbeelden die deze auteur noemt in zijn boek zijn, observatie en/of aandachttrekkende aanwezigheid van de politie op plaatsen waar (wetende uit hun ervaring) strafbare feiten kunnen worden gepleegd (zie p. 94).

[170] Onder dit proactief handelen, valt ook onderzoek (bijvoorbeeld telefoontaps) waarvan de resultaten gebruikt kunnen worden in de (mogelijke) vervolging van toekomstige strafbare feiten (Krey, 2009a, p. 94 e.v.).

Bundesverfassungsgericht deze vraag in positieve zin beantwoord, waardoor er voor de deelstaten geen wetgevende taak is weggelegd op dit specifieke gebied.[171]

De Bundespolizei heeft als primaire taak zich te richten op het afwenden van gevaar (Gefahrenabwehr). Daaronder worden de douane, de spoorwegenpolitie en de beveiliging van vliegverkeer (geregeld in het *Bundespolizeigesetz*) gerekend. Pas in tweede instantie heeft de Bundespolizei enkele bevoegdheden op het gebied van opsporing van strafbare feiten en dan met name met betrekking tot delicten zoals smokkel (Fisher, 2009, p. 267; Krey, 2009a, p. 103).

Bundeskriminalamt
De *Bundeskriminalamt* (BKA) is als agentschap onderdeel van het Federale Ministerie van Binnenlandse Zaken.[172] Het BKA heeft taken en verantwoordelijkheden op het gebied van criminaliteitsbestrijding en strafvordering op basis van de Wet voor het Federale Bureau voor Strafrechtelijk Onderzoek (*Bundeskriminalamtgesetz*)[173] en werkt vanuit die optiek samen met de Bundespolizei en de politie van de afzonderlijke deelstaten. Het BKA fungeert enerzijds als een informatie- en communicatiecentrum voor de (gehele) Duitse politie, waarmee de organisatie zowel de politie van de afzonderlijke deelstaten als de Bundespolizei ondersteunt in de preventie en de opsporing van deelstaat of land overschrijdende criminaliteit. Anderzijds initieert het BKA zelf de opsporing naar internationale misdrijven op basis van eigen bevoegdheden om strafrechtelijk onderzoek te verrichten in bijvoorbeeld gevallen van internationale (georganiseerde) mensenhandel, handel in wapens, munitie, explosieven of drugs en terrorisme (zie § 129*a* en 129*b* StGB). Daarnaast zal het BKA het opsporingsonderzoek verrichten indien daartoe vanwege het belang van de zaak speciaal opdracht is gegeven door een Staatsanwalt.[174]

11.1.3 Fasen in het strafproces

Het strafproces (*Strafverfahren*) is verdeeld in drie opeenvolgende hoofdfasen:[175]

a) het vooronderzoek / opsporingsonderzoek (*Vorverfahren*);
b) de fase waarin wordt besloten al dan niet tot vervolging over te gaan (*Zwischenverfahren*);
c) het onderzoek ter zitting (*Haubtverfahren/Hauptverhandlung*).

De Staatsanwalt kan een vooronderzoek of opsporingsonderzoek (*Vorverfahren*) in persoon uitvoeren, door verdachten, getuigen en experts te (ver)horen (§§ 161, 161*a* en 163*a* StPO). Daarnaast kan de Staatsanwalt de politie onderzoek laten doen (§§ 161 StPO en 152 GVG). Tenslotte kan de Staatsanwalt op grond van § 162 StPO een onderzoeksrechter (*Ermittlungsrichter*) verzoeken om bepaalde onderzoekshandelingen uit te voeren.[176] Hiertoe zal een Staatsanwalt overgaan indien het opsporingsonderzoek raakt aan de grondrechten

171 Het Federale Constitutionele Hof (BVerfG) stelde dat "(d)er Niedersächsische Gesetzgeber habe teilweise seine Gesetzgebungskompetenz überschritten. Da der Bundesgesetzgeber die Verfolgung von Straftaten durch Maßnahmen der Telekommunikationsüberwachung in der Strafprozessordnung abschließend geregelt habe, seien die Länder insoweit von der Gesetzgebung ausgeschlossen. Zudem sei die gesetzliche Ermächtigung insgesamt nicht hinreichend bestimmt und genüge nicht den Anforderungen des Verhältnismäßigkeitsgrundsatzes. Ferner fehlten im Gesetz Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung. Damit war die Verfassungsbeschwerde eines Richters, der sich durch die angegriffenen Regelungen in seinem Fernmeldegeheimnis verletzt sah, erfolgreich." BverfG Pressemitteiling Nr. 68/20065 vom 27 Juli 2005, Zum Urteil 27 Juli 2005 – 1 BvR 668/04 (www.bundesverfassungsgericht.de).

172 Zie http://www.bka.de. Het WODC onderhoudt contacten met het Bundeskriminalamt, dat voor het grootste deel is gevestigd in Wiesbaden (deelstaat Hessen).

173 ie nader Krey (2009a, p. 103).

174 Zie http://www.bka.de.

175 Vergelijk Juy-Birmann (2002, p.310-311).

176 Hierbij valt ondermeer te denken aan het (ver)horen van de verdachte of een getuige. Een valse verklaring afleggen tegenover een rechter is strafbaar, zo een verklaring afleggen tegenover een Staatsanwalt is dat niet (zie §§ 254 en 251 StPO en §§ 153 en 154 StGB).

van de verdachte of betrokkene. Dan kan alleen een rechter de betreffende opsporingsmethode bevelen. Dit is bijvoorbeeld het geval bij een arrestatiebevel en bij een *tapbevel* (zie § 100*b* StPO) (zie o.a. Krey, 2009a, p. 81.).

Hoewel de Staatsanwalt vanuit juridisch oogpunt leiding geeft aan het opsporingsonderzoek dat wordt uitgevoerd door de politie, is het feitelijk de politie die de touwtjes in handen heeft bij de uitvoering van het opsporingsonderzoek (Krey, 2009b, p. 13-14). Hiervoor worden drie redenen aangegeven. Allereerst kan de Staatsanwalt een dergelijk onderzoek niet werkelijk alleen (in persoon) uitvoeren, eenvoudigweg omdat hij de capaciteit daar niet voor heeft. Zo zijn er ongeveer 3.000 Staatsanwältinnen/anwälte werkzaam in Duitsland tegenover 250.000 politieambtenaren (Krey, 2009b, p. 14). Ten tweede staan de belangrijkste computersystemen bij de politie (Krey, 2009b, p. 14). Ten derde worden de meeste opsporingsonderzoeken uitgevoerd door de politie.[177] De Staatsanwalt is in de meeste gevallen niet betrokken bij het onderzoek totdat de politie het onderzoek heeft afgerond.[178] In zulke gevallen fungeert de Staatsanwalt alleen als een openbaar aanklager en niet als een leidinggevende in het opsporingsonderzoek.[179] Bij ernstige misdrijven (waaronder georganiseerde criminaliteit) ligt de situatie evenwel anders. Dan blijkt de Staatsanwalt wel een (dominante) rol te spelen in het opsporingsonderzoek (Krey, 2009b).[180]

Mocht de strafzaak voldoende feitelijke aanknopingspunten bieden (*zureichende tatsächliche Anhaltspunkte*) dan is de Staatsanwalt verplicht om een strafvervolging in te stellen.[181] Door middel van een dagvaarding (*Anklagegeschrift*) wordt de zaak vervolgens voor de rechter gebracht.[182] Het onderzoek ter zitting (*Haubtverfahren/Hauptverhandlung*) is bedoeld als de fase waarin het eigenlijke en volledige onderzoek (inclusief de bewijsvoering) naar het strafbare feit dient plaats te vinden.

11.2 Het gebruik van de telefoon- en internettap in de praktijk

In Duitsland kan niet voor de opsporing van elk strafbaar feit gebruik worden gemaakt van de telefoon- of internettap. De wet bepaalt dat dit slechts ten aanzien van bepaalde soorten zwaardere delicten (*schwere Straftat*) is toegestaan. In § 100*a* StPO wordt een uitputtende lijst gegeven van commune delicten (*Strafgesetzbuch*)[183] en bijzondere delicten, bijvoorbeeld uit de Asielprocedurewet (*Asylverfahrensgesetz*) of de Geneesmiddelenwet (*Arzneimittelgesetz*), waarvoor het gebruik van de telefoon- en internettap in aanmerking kan komen.[184] Naast de verdachte kan de tap ook gericht zijn tegen een derde waarvan het waarschijnlijk is dat deze in contact staat met de verdachte (*Information-Transmitter*).[185] Een telefoonlijn van een derde mag eveneens worden afgetapt als waarschijnlijk is dat deze

177 In Nederland lijkt dit overigens niet anders te zijn (zie Deel 1).
178 Vergelijk Spapens (2008); Elsner & Peters (2006, p. 224-225).
179 *Idem*.
180 Dit geldt ook voor de Staatsanwalt respondent die in het onderhavige onderzoek is geïnterviewd. Zie verder § 3.
181 Dit in tegenstelling tot bijvoorbeeld Nederland en Zweden, waar de openbaar aanklager een discretionaire bevoegdheid heeft om al dan niet te vervolgen (opportuniteitsbeginsel).
182 Lekenrechters (*Schöffen*) participeren bij de behandeling van strafzaken in eerste aanleg (zowel bij een *Amtsgericht* als bij een *Landgericht*).
183 Hieronder vallen bijvoorbeeld delicten als moord en doodslag (§§ 211 en 212 StGB), maar ook corruptie en omkoping (§§ 332 en 334 StGB).
184 De wet spreekt over "dass jemand als Täter oder Teilnehmer eine (…) schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat (…)." Waarmee wordt aangegeven dat ook deelnemingsvormen, poging en voorbereiding vallen onder het bereik van de regeling. Deze catalogus van strafbare feiten is na de introductie in 1968 meerdere malen uitgebreid met nieuwe strafbare feiten waarvoor de telefoon- en internettap gebruikt kan worden, zie nader Wörner, 2004, p. 88-89. Voor de letterlijke tekst van de regeling, zie http://dejure.org/gesetze/StPO/100a.html.
185 Zie o.a. *BGH* NJW 1994, 2904 ff., 2907; *Nack*, KK, § 100*a* StPO Rn. 27. Vergelijk Wörner (2004, p. 86 e.v.).

ook door de verdachte wordt gebruikt. Deze derde hoeft zich overigens niet bewust te zijn van het gebruik van de verdachte van de betreffende telefoonlijn (Wörner, 2004, p. 86 e.v.).

Verder moet sprake zijn van een (redelijke) verdenking gebaseerd op feiten dat een persoon een feit heeft gepleegd die staat op de lijst van § 100*a* StPO. Er hoeft geen specifieke verdenking te bestaan en de rechter die hierover oordeelt, heeft een grote discretionaire bevoegdheid, die slecht marginaal lijkt te kunnen worden getoetst.[186]

De regeling van § 100*a* StPO (telefoon- en internettap) moet worden gezien als een regeling alleen te gebruiken in laatste instantie. Met andere woorden, alleen indien andere minder ingrijpende opsporingsmiddelen inadequaat, onmogelijk of te moeilijk zijn om in de praktijk uit te voeren, mag gebruik worden gemaakt van de telefoon- of internettap. De genoemde onmogelijkheid slaat op de situatie dat er geen andere – minder ingrijpende – opsporingsmethoden zijn om de betreffende informatie te verkrijgen.[187] Te moeilijk om in de praktijk uitvoering aan te geven, houdt in dat er veel meer tijd en moeite gepaard zou moeten gaan met het op een andere wijze dan via een tap vergaren van de benodigde informatie (Wörner, 2004, p. 87-88). Hiermee lijkt een subsidiariteitstoets te zijn aangelegd voor het gebruik van de telefoon- of internettap. In elk geval moet apart worden gewogen voor welke opsporingsmethode moet worden gekozen (*subsidiariteitstoets*) en welke methode daarbij de minste inbreuk maakt op de (grond)rechten van de verdachte (*proportionaliteitstoets*).[188]

11.2.1 Het tapbevel en het autorisatieproces

Voor het aftappen van telefoons (*Telefonüberwachung*) tijdens het opsporingsonderzoek is in beginsel een rechterlijk bevel vooraf vereist. Alleen in spoedgevallen mag een Staatsanwalt dit dwangmiddel zonder die toestemming vooraf toepassen, onder de voorwaarde dat achteraf binnen 3 dagen rechterlijke autorisatie wordt gevraagd (§§ 100*a* en 100*b* StPO).[189] Indien daardoor binnen die drie dagen een verdachte in de zaak wordt aangehouden, is het niet langer nodig voor de Staatsanwalt om achteraf toestemming te vragen voor de telefoontap bij de rechter.[190]

Voorafgaande aan het toestemmingsverzoek van de Staatsanwalt aan de rechter, vindt er overleg plaats tussen de politie en de Staatsanwalt. Door een respondent van het BKA wordt in dit verband naar voren gebracht dat een van zijn taken als leidinggevende van een opsporingsteam is om te rapporteren aan de Staatsanwalt. Dit houdt onder meer in dat het doel van het opsporingsonderzoek wordt besproken en de te nemen stappen daarin. Verder wordt over de mogelijke inzet van opsporingsmethoden, zoals de telefoontap en surveillance gesproken.[191] Uit de interviews komt het beeld naar voren dat de Staatsanwalt in deze besprekingen een wat lijdelijke rol speelt. Indien de Staatsanwalt akkoord is met een tapaanvraag gaat deze hiermee naar de rechter. Een tapbevel kan worden afgegeven voor een termijn van uiterlijk 3 maanden (§ 100*b* II 4 StPO).

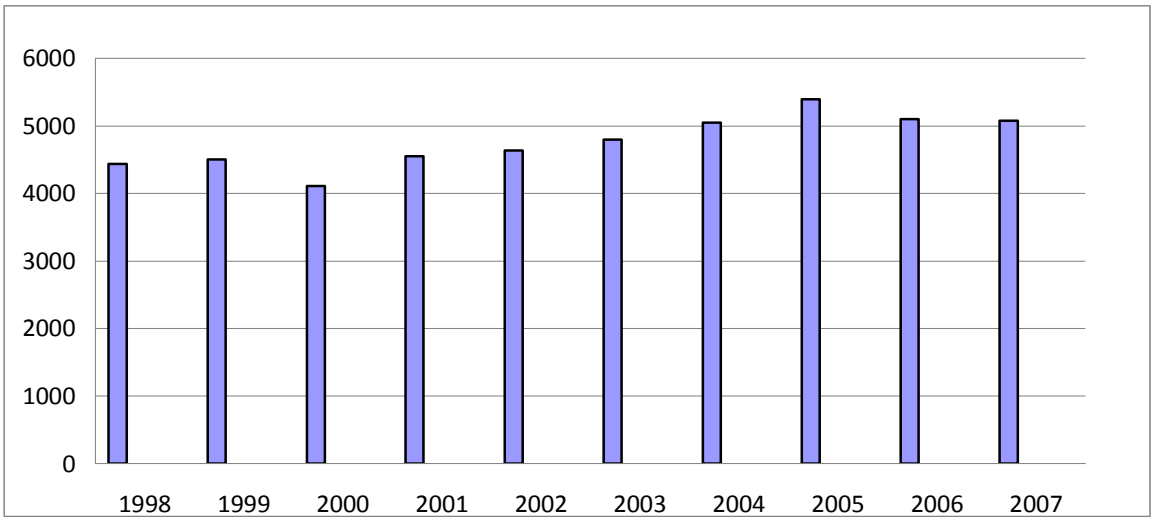
Gelijktijdig met de tapaanvraag wordt gevraagd om ook andere middelen in te mogen zetten in de bepaalde strafzaak. De respondent van de Staatsanwalt geeft aan gemiddeld 10 tapaanvragen per werkdag binnen te krijgen die vaak snel afgehandeld moeten worden. De werkrelatie die de Staatsanwalt opbouwt met de rechter is daarom belangrijk bij het efficiënt

186 Zie o.a. *BGH* NStZ 1995, 510 ff. (511). Zie ook Wörner (2004, p. 87).
187 De kosten van de opsporing mogen hierbij overigens geen rol spelen, zie nader Wörner (2004, p. 87-88).
188 Onder andere artikel 10 GG. De regeling laat de proportionaliteit ook terug komen in de keuze om de telefoon- en internettap als opsporingsmiddel (en dwangmiddel) te beperken tot bepaalde (zwaardere) strafbare feiten. Zie nader Wörner (2004, p. 87-88).
189 Vergelijk Juy-Birmann (2002, p. 320).
190 Aldus de Staatsanwalt.
191 Dat hoeft voor de BKA overigens niet altijd dezelfde Staatsanwalt(schaft) te zijn. Deze keuze het hangt (o.a.) af van de plaats van het (vermeend) delict of de woonplaats van de verdachte.

afhandelen van tapaanvragen. Zo geeft een respondent van de Staatsanwalt aan dat "one of the focus points of my particular work is to have an ongoing relationship with these judges so that the orders which I need from them, the permission, is [given] (…) very quickly. (…) The work carried out here relies heavily on wire tapping. If (…) the investigative judges delay or refuse the application for wire tapping, that can have serious consequences on the work carried out here."[192]
Een tapbevel kan vervolgens worden verlengd voor een periode van 3 maanden, steeds zolang nieuwe informatie de aanvraag kan onderbouwen. Soms wordt een verlenging door de rechter afgewezen, maar vaak gebeurt dat niet, omdat de politie een verlengingsaanvraag eerst doorspreekt met de betrokken Staatsanwalt die uiteindelijk ook beslist over het indienen van een dergelijk verlengingsverzoek.

Grafiek 8 toont het totaal aantal (uitgegeven) tapbevelen voor vaste telefoonlijnen in de periode 1998 tot en met 2007.[193]

Grafiek 8 Aantallen uitgegeven tapbevelen betreffende vaste telefoonlijnen[194]



Bron: Bundesnetzagentur Martkbeobachtung Telekommunikationsdienstemarkt, Jahresbericht 2008, p. 109.

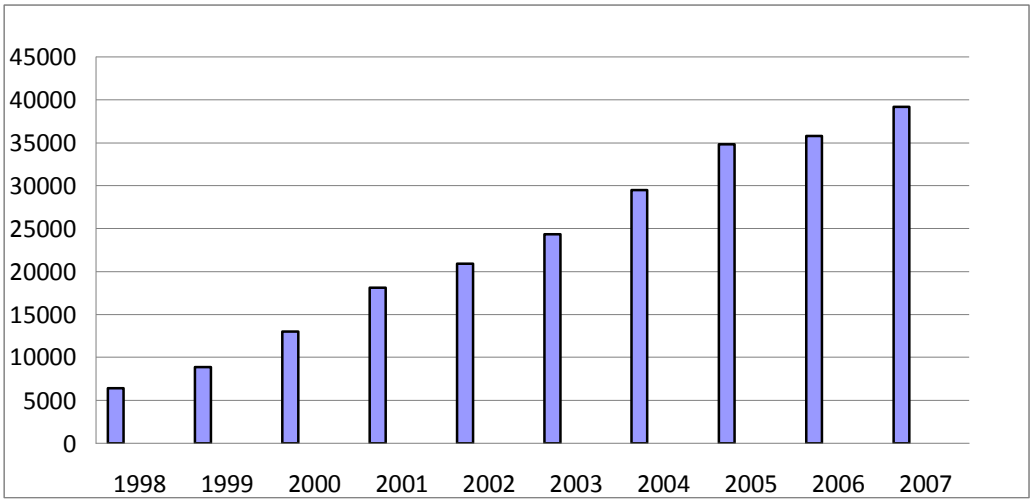
Uit Grafiek 8 blijkt dat in 2007 in totaal 5.078 tapbevelen zijn afgegeven met betrekking tot vaste telefoonlijnen in Duitsland. Het jaar ervoor 2006, was dat een fractie hoger, namelijk 5.099. In 2005 zijn er in de weergegeven periode de meeste tapbevelen afgegeven betreffende vaste telefoonlijnen, namelijk 5.398. Als het aantal tapbevelen van het begin van de periode in Grafiek 8 (1998) wordt afgezet tegen het aantal tapbevelen aan het eind van die periode (2007) dan blijkt sprake van een toename van het aantal tapbevelen van ruim 14%.

192 Aldus de Staatsanwalt.

193 Albrecht, Dorsch & Krüpe (2003) hebben onderzoek gedaan naar het gebruik van de telefoontap in een aantal verschillende landen, waaronder Duitsland. Uit cijfers van dat onderzoek blijkt dat in de periode van 1998-2000 in Duitsland per 100.000 inwoners (gemiddeld) 15 tapbevelen zijn afgegeven (zie p. 104, Grafiek 34). Uit hetzelfde onderzoek komt naar voren dat in dezelfde periode in Nederland 62 tapbevelen per 100.000 zijn afgegeven (zie ook Bokhorst, 2004).

194 In het Bundesnetzagentur Martkbeobachtung Telekommunikationsdienstemarkt, Jahresbericht 2008, p. 111 wordt de Grafiek aangeduid als: *Statistik der strafprozessualen Überwachungsmaßnahmen der Telekommunikation*. De Bundesnetzagentur is een regelgevende instantie voor elektriciteit, gas, telecommunicatie, post en spoorwegen markten. Het is een federale overheidsinstelling en onderdeel van het Duitse federale ministerie van Economie en Technologie (zie ook http://www.bundesnetzagentur.de). De BKA-data en de data van andere Politie-instanties worden jaarlijks naar de Bundesnetzagentur gestuurd.

Grafiek 9 Aantallen uitgegeven tapbevelen betreffende mobiele telefoons



Bron: Bundesnetzagentur Martkbeobachtung Telekommunikationsdienstemarkt, Jahresbericht 2008, p. 109.

Grafiek 9 geeft het totale aantal (uitgegeven) tapbevelen voor mobiele telefoons weer in de periode 1998 tot en met 2007. Hieruit komt een heel ander beeld naar voren. In 2007 bedroeg het totaal aantal tapbevelen voor mobiele telefoons 39.200. In 2006 bedroeg dat 35.816 tapbevelen en in 2005 waren dat er 34.855. Uit Grafiek 9 valt op te maken dat in de periode van 1998 tot en met 2007 het aantal uitgegeven tapbevelen exponentieel is gegroeid. Als het aantal tapbevelen aan het begin van de getoonde periode (1998), zijnde 6.391, wordt afgezet tegen het aantal tapbevelen aan het eind van die periode (2007), laat dit een toename van het aantal tapbevelen zien van ruim 600%. Een verklaring voor de grote toename van uitgegeven tapbevelen voor mobiele telefoons over de periode 1998-2007 is gelegen in de exponentiële groei in het gebruik van mobiele telefoons van de laatste jaren.[195] Voor personen die aan de tap worden onderworpen geldt dat ze doorgaans frequent wisselen van telefoonkaarten en van mobiele telefoons (zie hierover ook paragraaf 11.2.2).

Het gebruik van abonnee- en verkeersgegevens

Naast het aftappen van telefoon- en internetverbindingen kunnen ook abonnee- en verkeersgegevens voor opsporingsdoeleinden worden gebruikt. In de afgelopen jaren blijkt steeds meer gebruik te worden gemaakt van abonnee- (zie Grafiek 10, hieronder) en verkeersgegevens voor opsporingsdoeleinden. Het is niet alleen een aanvulling op de telefoontap, maar heeft zich in feite ontwikkeld tot een onafhankelijke opsporingsmethode. Deze opsporingsmethode (met name het opvragen en gebruiken van verkeersgegevens) vindt ook toepassing bij de opsporing van meer conventionele misdrijven, zoals diefstal (*Raub*), gewapende overval (*räuberische Erpressung*), drugsdelicten (*Rauschgiftdelikte*), fraude (*Betrug*) en levensdelicten (*Tötungsdelikte*).[196] Door een respondent van het BKA wordt naar voren gebracht dat verkeersgegevens in de opsporing worden gebruikt, en dat het gebruik hiervan zo interessant is omdat daarmee in kaart kan worden gebracht waar een persoon zich in een bepaalde periode bevindt (of bevonden heeft). Bij het opstarten van een

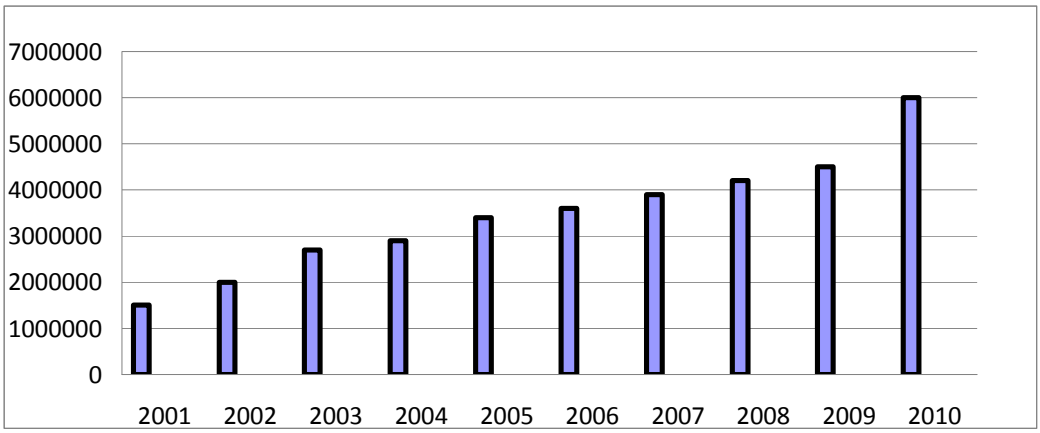
[195] Aldus de Bundesnetzagentur in het Jahresbericht 2008. Voor de groei in 2007 zelf, geeft de Bundesnetzagentur aan dit volledig toe te schrijven aan de sterke groei in het gebruik van mobiele telefoons.

[196] Zie Albrecht & Kilchling (2009), die aangeven dat "der Zugriff auf die Telekommunikations-Verkehrsdaten ist eine Ermittlungsmaßnahme, die erst seit einigen Jahren vermehrt zum Einsatz kommt. Sie ergänzt nicht nur das „klassische" Abhören, sondern entwickelt sich immer mehr zu einer eigenständigen Ermittlungsmethode, die sehr ökonomisch einsetzbar ist." Zie ook Grafe (2008, p. 134).

opsporingsonderzoek is er vaak (nog) weinig bekend over de verdachte en dan kunnen verkeersgegevens inzicht bieden in de handel en wandel van de verdachte. Daarom is het volgens deze respondent van het BKA goed om in het opsporingsproces daarmee te beginnen. Deze methode lijkt dus niet (langer) als een 'laatste' (red)middel gebruikt te worden, maar veeleer als een 'eerste' stap in het opsporingsproces.
Overigens moet ook voor een aanvraag bij een Telecom provider om gebruik te (kunnen) maken van verkeersgegevens eerst toestemming worden verleend door de rechter. Dit betekent dat de politie eerst de Staatsanwalt moet inschakelen die dan vervolgens de aanvraag indient bij de rechter.[197] De aanvraag moet overigens wel betrekking hebben op een strafbaar feit waarvoor deze methode gelegitimeerd is.

Grafiek 10 geeft het totaal aantal verzoeken om gebruik te maken van *abonnee*gegevens (naam en adres gekoppeld aan een telefoonnummer) over de periode 2001 tot en met 2010 weer. In 2010 zijn 250 verschillende autoriteiten gemachtigd om abonneegegevens op te vragen bij in totaal 135 verschillende telecommunicatiebedrijven.[198]

Grafiek 10 Aantallen verzoeken om gebruik te maken van abonneegegevens*[199]*



Bron: Bundesnetzagentur Martkbeobachtung Telekommunikationsdienstemarkt, Jahresbericht 2010, p. 125.

In 2010 bedroeg het totaal aantal verzoeken 6.000.000. Het jaar ervoor (2009) waren dat 4.500.000 verzoeken. In 2008 werden 4.200.000 verzoeken om gebruik te maken van gegevens gedaan en in 2007 was dat aantal 3.900.000. Uit Grafiek 10 valt op te maken dat in de periode van 2001 tot en met 2010 het aantal verzoeken exponentieel is gegroeid. Als het aantal verzoeken in 2001, zijnde 1.500.000, wordt afgezet tegen het aantal verzoeken in 2010 dan blijkt de toename uit te komen op 400%.
Uit de statistieken van de Bundesnetzagentur kunnen geen cijfers worden gehaald over de aantallen aanvragen over het gebruik van verkeersgegevens.[200] Door het Max-Planck-Institut für Ausländisches und Internationales Strafrecht (Max-Planck-Institut), is een schatting gemaakt van het gebruik van verkeersgegevens op grond van § 100*g*, § 100*h* StPO over de periode van 2002-2005 voor heel Duitsland (*Bundesweit*) (Albrecht, Grafe & Kilchling, 2008). Uit die schatting komt naar voren dat in 2002 het totaal aantal keren dat verkeersgegevens zijn opgevraagd wordt geschat op circa 10.200. Het jaar erop (2003) is de schatting dat dit aantal gestegen naar circa 15.200 en in 2004 naar circa 22.600. In 2005 is geschat dat het gebruik van opgevraagde verkeersgegevens is gestegen naar circa 40.700. De stijging in

197 Zie o.a. § 100*g* StPO.
198 Zie Bundesnetzagentur, Jahresbericht 2010, p. 124.
199 De Bundesnetzagentur spreekt over *Auskunftsersuchen von Sicherheitsbehörden* of over *information requests by security authorities*.
200 Albrecht & Kilchling (2009) stellen namelijk dat "mit den offiziellen Statistiken sind keine Aussagen über die Gesamtzahl der Beschlüsse oder der Abfragen zu unterschiedlichen Bereichen von Verkehrsdaten möglich. Damit lassen sich auch nicht die Entwicklungen in diesem Bereich beobachten."

2005 is fors, waarbij het geschatte aantal opgevraagde verkeersgegevens in dat jaar vergelijkbaar is met het totaal aantal tapbevelen in 2005.[201] De genoemde (geschatte) cijfers van het Max-Planck-Institut laten een exponentiële groei zien in het gebruik van verkeersgegevens in opsporingsonderzoeken over de periode 2002-2005, waarbij de indicatie is dat na 2005 meer verkeersgegevens worden opgevraagd dan telefoontapbevelen worden afgegeven. Het aanvragen van verkeersgegevens is zoals gezegd in Duitsland losgekoppeld van de tap, en wordt als zelfstandige methode ingezet, ook bij minder zware delicten.

11.2.2 Het gebruik van de telefoon- en de internettap en afluisterapparatuur

Het proces van opsporing waar een geïnterviewde respondent van het BKA zicht op heeft, betreffende zware en georganiseerde criminaliteit (onder andere mensenhandel), begint normaliter niet met een tapaanvraag. Gewoonlijk begint een opsporingsonderzoek naar aanleiding van binnengekomen informatie over een verdachte situatie of over een (bepaalde) persoon. Deze informatie wordt allereerst gecheckt en tevens wordt gezocht of er mogelijk (meer) relevante informatie bij de politie bekend is. Hierbij kunnen dus ook opgevraagde verkeersgegevens een rol spelen. Hiermee wordt getracht enigszins een beeld te krijgen van de gebeurtenis (bijvoorbeeld of er sprake is van een delict) en van de persoon in kwestie. Vervolgens wordt nagegaan of het BKA de aangewezen instantie is om het onderzoek te gaan verrichten. Indien dat het geval is, wordt een plan van aanpak gemaakt waarin beschreven staat hoe men het opsporingsonderzoek uit zal gaan voeren. Pas als alle informatiebronnen zijn benut (inclusief de buitenlandse) en het onderzoek niet verder komt, wordt, als de wettelijke regeling dat toelaat, een aanvraag gedaan voor een telefoontap.
Uit het beeld dat wordt geschetst van de bestrijding van de internationale drugshandel lijkt naar voren te komen dat al vrij snel bij aanvang van het onderzoek de opsporingsmiddelen zijn uitgeput, waardoor niets anders rest dan een telefoontap aan te vragen. Zo stelt de respondent van het BKA dat al in een vroeg stadium van een opsporingsonderzoek getapt wordt, omdat in die fase een (buitenlands) telefoonnummer vaak de enige informatie is waarover het BKA beschikt met betrekking tot een verdachte van (internationale) drugshandel. De respondent van de Staatsanwalt geeft aan dat er feitelijk geen zaken zijn waarin de telefoon niet wordt afgetapt: "we have no cases whatsoever in which wire tapping has not taken place, in our department."[202] Veelal wordt doormiddel van een telefoontap (soms een informant) een link gelegd naar een ander telefoonnummer, waarvoor een nieuwe tapaanvraag wordt gedaan.[203] De waarde van een telefoontap op een bepaald nummer blijkt evenwel vaak maar van korte duur. De respondent van de Staatsanwalt geeft aan dat voorheen "we looked at the [telephone] numbers, but of course you had these cards that could be changed and we followed a new strategy which was the IMEI's. But what is happening now is that the price of mobile phones is going down drastically and so they change their mobile phones like they used to do with their [telephone] cards."
De respondent van de Staatanwalt vervolgt door er op te wijzen dat binnen criminele kringen niemand zijn telefoon langer gebruikt dan een week. Dit betekent dat bij het aftappen van de telefoon goed moet worden opgelet of er een nieuw telefoonnummer wordt genoemd, dat vervolgens dan zal moeten worden afgetapt om de als politie bij te blijven. "That's why we are accused of listening in on conversations far too much. But we need to do this in order to establish the links (…)."[204]
De bovenstaande constateringen van de Staatsanwalt respondent over de trend, om in plaats van telefoonkaarten de mobiele telefoon te verwisselen, wordt niet (volledig) onderschreven door één van de BKA respondenten. De laatste stelt namelijk dat het verwisselen van mobiele telefoon weliswaar gebeurt, maar in de regel worden alleen de telefoonkaarten

[201] Op basis van de cijfers uit de Grafieken 1 en 2 zijn er in 2005 in totaal 40.253 tapbevelen afgegeven. Grafe noemt overigens een aantal van 42.500 afgegeven tapbevelen voor 2005 (zie Grafe, 2008, p. 82; zie ook Albrecht & Kilchling, 2009).
[202] Zoals eerder aangegeven is de respondent van de Staatsanwalt werkzaam in de opsporing, bestrijding (en vervolging) van de internationale drugshandel.
[203] Aldus de respondent van de Staatsanwalt.
[204] *Idem*.

verwisseld.[205] Dit lijkt te worden bevestigd door een BKA respondent die stelt dat het vaak lastig is om van een verdachte een telefoonnummer te bemachtigen, omdat zij veelvuldig van telefoonnummer wisselen. Is eenmaal het nummer bij de politie bekend, dan kan (via de telefoontap) de verdachte goed worden gevolgd.[206]
Soms ook blijkt een enkel telefoonnummer niet voldoende aanknopingspunten te genereren voor verdere opsporing. In dat geval moeten andere opsporingsmiddelen dan de telefoontap worden ingezet zoals informanten.[207] Een andere reden om naast de telefoontap ook gebruik te maken van andere opsporingsmiddelen, in het bijzonder afluisterapparatuur, is volgens de Staatsanwalt respondent omdat verdachten via de telefoon weinig prijs geven over hun handelen. Dan blijkt de combinatie van het gebruik van de telefoontap met afluisterapparatuur (bugging) in bepaalde situaties vaak effectief. De Staatsanwalt beweert dat:

> "the best conversations, in my experience, are carried out either in the car, that's where men speak straight and are honest with each other. Or in prison where they have to be very precise, very quick and very concise in what they say. We have a distinction here in Germany, and this is all based on the subsidiary principle. We have 2 categories here which are heatedly discussed in Germany. One is the small bugging devices placed in cars. We call that the small cases. For example in cars. I say cars here in this case. Or we call the larger cases of bugging devices being placed in homes. Heated discussions went on in Germany about this particular, this larger bugging process. But in fact we established that no conversations take place in the apartments or in the homes of these people. They do not sit down around a coffee table and speak about the plans which are carried out. We don't use it. The best, as I said, comes from these more smaller actions in the car or in prison. (…).Some of the most revealing information is gained when both the telephone and the cars are being listened in to. Obviously the telephone, who is speaking to who, about what, where, but also when, [and] how the people in the car react to that telephone conversation. What they talk about in response to it. This is very revealing and useful information." - Staatsanwalt

Afhankelijk van het gedrag van degene(n) waar een opsporingsonderzoek zich op richt en de omstandigheden waaronder die personen (moeten) handelen, is de telefoontap volgens een BKA-respondent het meest gebruikte heimelijke opsporingsmiddel dat in de bestrijding van internationale (of interregionale) criminaliteit wordt gebruikt. Undercover operaties zijn bijvoorbeeld minder gemakkelijk uit te voeren en de resultaten van telefoontaps zijn volgens deze BKA respondent doorgaans goed en te gebruiken als bewijsmiddel ter terechtzitting. Volgens de andere BKA respondent is de telefoontap in de bestrijding van (internationale) drugshandel zelfs het belangrijkste opsporingsmiddel waarover de politie beschikt. Dit is

[205] Verder stelt deze BKA respondent dat, naast het gebruik van opgevraagde verkeersgegevens, "to be on the safe side, we start wire tapping the phone."

[206] Vanuit die optiek bekeken zal dan bij elke verandering van telefoonnummer een nieuwe tapaanvraag moeten worden gedaan indien de politie de telefoon(gesprekken) van die persoon wil blijven volgen. Door een respondent van de BKA wordt dit bevestigd: "Yes. If he uses 3 numbers, you have to request 3 orders. (…). For example in our last case we had 37 wire tappings, so we had to request 37 orders, and than the prolongation order[s]. A lot of paperwork."

[207] Door de respondent van de Staatanwalt wordt verder gewezen op een tegenovergestelde beweging met betrekking tot afluisteren: "We use all the means available to us. We use any technical surveillance available to us, but what we have experienced is that good people, our clients [r*espondent bedoelt hiermee bepaalde verdachten, althans personen die worden afgetapt*] also carry out surveillance on us. What we have experienced (…) is that we are also the subject of surveillance, carried out by the drug dealers and it is not an uncommon thing. Obviously, the people who do this are trained. Often they are former intelligence service personel, many from Eastern Europe. (…) They have technical experience with regard to encrypting, with regard to establishing what GPS are installed on vehicles and sometimes we find they removed our devices and put them on another vehicle, a family for example on a day trip somewhere and than we realise, 'hey its going in the wrong direction'."

omdat de drugshandelaren die contact moeten onderhouden met anderen (in andere landen), eigenlijk maar een reële optie hebben en dat is het gebruik van de telefoon.[208]

Het volgen en de verslaglegging van de telefoongesprekken
Volgens een BKA respondent worden de meeste gesprekken niet 'live' gevolgd. Doorgaans worden telefoongesprekken eerst opgenomen en na een bepaalde periode uitgeschreven. Alleen indien zich de noodzaak voordient, wordt er geluisterd terwijl het gesprek gaande is. Dat is onder andere het geval als er een undercover agenten actief zijn of er een observatie gaande is. Dan moet snel kunnen worden ingegrepen, bijvoorbeeld in verband met de veiligheid van de undercover agenten of om een verdachte op heterdaad aan te houden. De verslaglegging van relevante telefoongesprekken is volgens bovengenoemde respondent van het BKA letterlijk. Wanneer een gesprek niet relevant is, wordt in een paar woorden de inhoud genoteerd.[209] Verslaglegging is een tijdrovende bezigheid. Als de gesprekken plaatsvinden in het Duits dan worden de gesprekken volgens de respondent door de politieambtenaren zelf opgetekend. Bij gesprekken in andere talen worden tolken gebruikt die dan ook de verslaglegging voor hun rekening nemen. Door het vertalen gaat er volgens deze respondent altijd iets aan informatie verloren.

Opslag en overdracht van gegevens
Nadat een opsporingsonderzoek is afgerond moeten gegevens worden opgeslagen en overgedragen aan de Staatsanwalt. Een BKA-respondent legt uit dat de technische afdeling alle telefoongesprekken opneemt en opslaat. Wanneer een opsporingsonderzoek is afgerond worden alle gesprekken op een compactdisc gezet en overhandigd aan de Staatanwalt, "for example for a request for surveillance we write a report and we quote some calls, 'in this call he says this and this, this is the place where you can find this call'".

De inhoud van de telefoontap als bewijsmiddel
Uit het bovenstaande blijkt duidelijk dat sprake is van een toegevoegde waarde van het gebruik van de telefoontap in het opsporingsonderzoek. Of goed gebruik kan worden gemaakt van relevante telefoongesprekken, ook als belastend bewijsmiddel bij de zittingsrechter, is echter de vraag.[210] Het probleem is dat alleen op basis van tapgesprekken het verhaal van een Openbaar Aanklager juridisch moeilijk sluitend te krijgen is. Een verweer als: "wat er over de telefoon is gezegd was maar een grapje", kan volgens de respondent van de Staatsanwalt dan vaak moeilijk worden weerlegd. Daarom wordt de informatie uit de telefoongesprekken vaak niet (direct) gebruikt als bewijsmiddel in de strafzaak.

> "In such cases we do not need the information obtained by the telephone conversations which were wire tapped. What we in fact try to do is not mention that wire tapping was carried out (…). What we do is we carry out telephone surveillance and than this might lead to the arrest of several people, but the actual telephone conversations are no longer necessary for the case (…)." - Staatsanwalt

De internettap
Van de internettap wordt minder vaak gebruik gemaakt dan van de telefoontap, zo blijkt uit het gesprek met één van de BKA respondenten. Vaak is het volgens deze respondent

[208] Een respondent van de BKA: "Well of course, especially in our area, in the fight against drugs trafficking, it is the most important investigation method we have. (…) especially regarding international connections and international connected suspects, they have to stay in contact (…) when they are in different countries (one is in South America and the other one is here) they don't travel the whole distance just to talk, so they have to use phones."

[209] De respondent van de Staatsanwalt vertelt over de inhoud van de telefoongesprekken dat "the content of the conversation is of course important, but (…) what they talk about is nothing. They just talk, the say 'we meet there or here'." Veel ervaring is bovendien nodig om de gebruikte codetaal te ontcijferen.

[210] De zittingsrechter kan kiezen tussen het beluisteren van de tapgesprekken of een schriftelijk verslag van de tapgesprekken (tapverslagen), dat dan eventueel ter zitting worden voorgelezen (Juy-Birmann, 2002, p. 320).

moeilijk te achterhalen wat precies wordt gedaan door de persoon die door de politie wordt gevolgd. Bij chats op internet is dat vaak het geval. E-mail is volgens hem beter te volgen. Verdachten denken veelal dat e-mailen veilig is, maar dat is niet zo. Indien gebruik wordt gemaakt van een internetcafé of een buitenlandse provider, is het moeilijker om de e-mails te achterhalen.
Met betrekking tot het gebruik van internetcafés door een persoon die door de politie wordt gevolgd, is er nog een bijkomend probleem voor de politie, dat verder losstaat van het aftappen van het internetgebruik. Indien een door de politie gevolgde persoon in een internetcafé gebruik heeft gemaakt van het internet en een opsporingsambtenaar wil de opgeslagen informatie uit die computer halen, wordt de laatste niet zelden ontmaskerd in het geval het een internetcafé is "used by Macedonians and somebody else goes in (…) they can see you and if you want to sit at computer number 7, instead of 3, 4 or 5 than its obvious what you are doing, that you are a member of the police force and you want to extract information."

11.3 Waarborgen bij het gebruik van heimelijke opsporingsmiddelen

11.3.1 Inbreuk op het recht op privacy

Zoals in de vorige hoofdstukken ook al naar voren is gekomen, wordt er inbreuk gemaakt op de privacy van burgers indien de overheid gebruik maakt van opsporingsmethoden, zoals de telefoon- en internettap. Het recht op privacy is ondermeer neergelegd in artikel 8 lid 1 EVRM.[211] Het recht van de Europese Unie heeft volgens artikel 23 van de Federale Constitutie (*Grundgesetz*) voorrang op Duits recht.
De inmenging van het openbaar gezag in het privé-, familie- en gezinsleven, de woning en correspondentie van burgers is volgens deze bepaling echter niet toegestaan. Uit de (vaste) rechtspraak[212] van het Europese Hof voor de Rechten van de Mens (EHRM) komt naar voren dat een telefoontap een inbreuk oplevert van zowel het recht op privéleven[213] als dat van de correspondentie.
Uitzondering op deze regel, in de zin dat er wel door het openbaar gezag inbreuk mag worden gemaakt op de privacy van burgers, wordt geformuleerd in artikel 8 lid 2 EVRM. Daarbij moet dan aan drie voorwaarden worden voldaan. De inbreuk van het openbaar gezag moet zijn gebaseerd op een wettelijke regeling (*in accordance with the law*), in het belang zijn van de nationale veiligheid, de openbare orde of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, of de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen (*in the interests of among other the prevention of disorder or crime or the rights and freedoms of others*) en noodzakelijk zijn in een democratische samenleving (*necessary in a democratic society*). Een Lidstaat heeft bij de bepaling hiervan overigens wel enige interpretatieruimte (*a margin of appreciation*).
De rechtspraak van het Europese Hof voor de Rechten van de Mens (EHRM) over artikel 8 lid 2 EVRM blijkt toch vrij casuistisch te zijn en concentreert zich met name op de voorwaarden 'accordance with the law' en 'necessary in a democratic society' (Bleichrodt et al., 2011, p. 145-147; Krabbe, 2004, p. 161). Dit betekent dat aftappen van telefoon- en internetverkeer steeds aan de eisen van artikel 8 lid 2 EVRM moet voldoen. Daarbij zal het EHRM steeds in het concrete geval toetsen aan de bovengenoemde voorwaarden.

211 De Bondsrepubliek Duitsland is sinds 13 juli 1950 lid van de Raad van Europa en heeft het EVRM op 5 december 1952 geratificeerd.
212 Zie onder andere *Klass tegen Duitsland*, EHRM 6 september 1978, *Malone tegen het Verenigd Koninkrijk*, EHRM 2 augustus 1984, *Lüdi tegen Zwitserland*, EHRM 15 juni 1992, *Halford tegen het Verenigd Koninkrijk*, EHRM 25 juni 1997 en *Kopp tegen Zwitserland*, EHRM 25 maart 1998. Deze uitspraken zijn te vinden op http://www.echr.coe.int/ECHR/EN/Header/Case-Law/.
213 Een definitie van het begrip privéleven heeft het EHRM tot nog toe niet gegeven en zal dat naar alle waarschijnlijkheid ook niet doen, omdat op deze manier eventuele maatschappelijke veranderingen gemakkelijker kunnen worden meegewogen in het genoemde begrip, zie ook Krabbe, 2004, p. 151.

11.3.2 Notificatie

Wettelijk is de Staatsanwalt verplicht om achteraf degenen die zijn afgetapt hiervan op de hoogte te stellen (benachrichtigen). In de praktijk blijkt dat evenwel niet altijd mogelijk te zijn. Een respondent van het BKA legt uit dat alles afhangt van het kunnen identificeren van de personen waarmee de verdachte telefonisch contact heeft gehad. Daar waar identificatie mogelijk is, worden de personen geïdentificeerd. Als identificatie lastiger wordt, in de zin dat door onderzoek van de politie de identiteit van de betrokken personen bij derden bekend kan worden, blijft, met een beroep op bescherming van de privacy van de betrokkenen, verder onderzoek en notificatie veelal achterwege. Uiteindelijk wordt een beslissing hierover door de Staatsanwalt genomen.

Ook door de Staatsanwalt respondent wordt de spanning tussen de regeling en de praktijk van het uitvoeren onder de aandacht gebracht.

> "You have a situation where the government, in parliament, they present an ideal situation. But this is very [far] (…) [re]moved from the reality in which I work. Yes, there is a requirement to inform a person that wire tapping has taken place, but the problem is that I don't know who these people are. They use alias names, fantasy names. I don't know where they are or where they live. They do not provide an address (…). If an arrest is made, a person can be informed then that wire tapping has been taken place. But it doesn't apply in my case, because I don't know who we are talking about, the real names. But it is provided for by law. But in my case it is not possible." - Staatsanwalt

In *Klass tegen Duitsland* (EHRM 6 september 1978) oordeelde het Europese Hof dat moet worden nagegaan of het in de praktijk wel mogelijk is om in alle gevallen de betrokkene achteraf in kennis te stellen.[214] Aansluitend stelt het EHRM dat:

> "The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the 'interference' resulting from the contested legislation is in principle justified under Article 8 para. 2 (artikel 8-2) (see paragraph 48 above), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the 'interference'. Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction (see paragraphs 11 and 19 above)."

Van belang in dit geheel is wel dat een betrokkene de mogelijkheid heeft om zich te beklagen tegen schendingen van de grondrechten zoals neergelegd in het EVRM. In artikel 13 EVRM wordt een burger een dergelijk recht op een zogenaamde *effective remedy before a national authority* gegeven.[215] In *Klass tegen Duitsland* (6 september 1978) geeft het EHRM te kennen dat deze bepaling,

[214] *Klass tegen Duitsland*, EHRM 6 september 1978, r.o. 58.

[215] In artikel 13 EVRM staat: "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

> “read literally, seems to say that a person is entitled to a national remedy only if a "violation" has occurred. However, a person cannot establish a "violation" before a national authority unless he is first able to lodge with such an authority a complaint to that effect. Consequently, as the minority in the Commission stated, it cannot be a prerequisite for the application of Article 13 (artikel 13) that the Convention be in fact violated. In the Court’s view, Article 13 (artikel 13) requires that where an individual considers himself to have been prejudiced by a measure allegedly in breach of the Convention, he should have a remedy before a national authority in order both to have his claim decided and, if appropriate, to obtain redress. Thus Article 13 (artikel 13) must be interpreted as guaranteeing an "effective remedy before a national authority" to everyone who claims that his rights and freedoms under the Convention have been violated.”[216]

11.4 Concluderend

De wet bepaalt dat slechts ten aanzien van een bepaalde categorie strafbare feiten het mogelijk is om bij de opsporing daarvan gebruik te maken van de telefoon- of internettap. Daarbij kan naast de verdachte de tap ook gericht zijn tegen een derde persoon waarvan het waarschijnlijk is dat deze met de verdachte in contact staat. Ook mag een telefoonlijn van een derde worden afgetapt waarvan het waarschijnlijk is dat de verdachte hiervan gebruik maakt.
Met betrekking tot het aantal tapbevelen voor vaste lijnen in de periode van 1998 tot en met 2007 valt een bescheiden (rechtlijnige) groei te constateren. Over dezelfde periode is het aantal tapbevelen betreffende mobiele telefoons echter exponentieel gestegen. Een verklaring voor de grote toename van uitgegeven tapbevelen voor mobiele telefoons over de periode 1998-2007 is gelegen in de exponentiële groei in het gebruik van mobiele telefoons van de laatste jaren. Binnen de groep van afgetapte personen wordt frequent van telefoonkaarten of mobiele telefoons gewisseld. Ook het aantal verzoeken om gebruik te kunnen maken van abonneegegevens is in de periode van 2001 tot en met 2010 exponentieel gestegen. Dit lijkt samen te hangen met de stijging van het gebruik van mobiele telefoons en de stijging van het aantal tapbevelen voor mobiele telefoons. Het gebruik van verkeersgegevens blijkt steeds belangrijker te worden in de opsporing, maar concrete en actuele cijfers hierover ontbreken nog.
Uit de interviews komt niet een eensluidend oordeel naar voren over het moment waarop de telefoontap wordt ingezet bij het onderzoek naar zware en/of georganiseerde criminaliteit. Soms blijkt de telefoontap als een van de eerste middelen te worden ingezet, soms worden eerst andere methoden gebruikt. Een factor die hierin een rol speelt is het soort misdrijf (bijvoorbeeld drugshandel of mensenhandel) en de andere informatie die in het onderzoek kan worden achterhaald.
De waarde van een telefoontap op een bepaald mobiel telefoonnummer blijkt vaak maar van korte duur, omdat de betrokken personen frequent van telefoonkaart of mobiele telefoon wisselen. Om de verdachte telefonisch toch te kunnen blijven volgen, moet dan steeds een nieuw tapbevel moeten worden aangevraagd.
Het blijkt dat verdachten van zware en/of georganiseerde criminaliteit via de telefoon weinig prijs geven over hun handel en wandel met betrekking tot hun (vermeend) criminele activiteiten. Reden voor opsporingsdiensten om naast de telefoontap ook gebruik te maken van andere opsporingsmiddelen en in het bijzonder van afluisterapparatuur. De combinatie van het gebruik van de telefoontap met afluisterapparatuur blijkt in bepaalde situaties effectief te zijn. Toch is de telefoontap volgens de respondenten het meest gebruikte opsporingsmiddel dat hun ter beschikking staat. Van de internettap wordt veel minder gebruik gemaakt, omdat vaak moeilijk te achterhalen valt wat precies wordt gedaan op het internet door de persoon die door de politie wordt gevolgd.
De verslaglegging van afgetapte telefoongesprekken blijkt een tijdrovende bezigheid te zijn. Relevante telefoongesprekken worden letterlijk uitgewerkt, terwijl (naar de mening van

[216] *Klass tegen Duitsland*, EHRM 6 september 1978, r.o. 64.

degene die aftapt) niet ter zake doende gesprekken in een paar woorden worden beschreven. Gesprekken die in het Duits plaatsvinden worden door de opsporingsambtenaren zelf opgetekend en telefoongesprekken gevoerd in andere talen worden tolken gebruikt die dan ook de verslaglegging doen.
Tapverslagen worden niet vaak gebruikt als een direct bewijsmiddel in een strafzaak, zo wordt gesteld. De reden daarvoor is dat ter zitting de betrouwbaarheid en/of de volledigheid van de afgetapte telefoongesprekken nogal eens in twijfel wordt getroffen. Daarom wordt de informatie verkregen uit afgetapte telefoongesprekken veelal gebruikt om nieuwe bewijsmiddelen te verzamelen of verdachte personen aan te houden.

Hoewel het (legitiem) aftappen van telefoon- en internetverkeer in het kader van de opsporing van (vermeend) strafbare feiten een inbreuk is op artikel 8 lid 1 EVRM, hoeft het niet in strijd te zijn met het recht op privacy zoals geformuleerd in art 8 EVRM, indien wordt voldaan aan de uitzonderingen genoemd in lid 2. De rechtspraak van het EHRM is evenwel casuistisch en richt zich met name op de voorwaarden 'accordance with the law' en 'necessary in a democratic society' (artikel 8 lid 2 EVRM).
Na afloop van een taponderzoek moet de afgetapte persoon hiervan in beginsel op de hoogte worden gesteld. Dit blijkt in de praktijk op problemen te stuiten, in de zin dat de persoonsgegevens van de betrokkenen niet altijd te achterhalen zijn, waardoor notificeren om die reden al onmogelijk blijkt. Dit punt wordt ook door het EHRM erkend.

Deel IV

Slotbeschouwing

12 Slotbeschouwing

Dit onderzoek geeft een beeld van het gebruik van de telefoon- en internettap in de opsporing in Nederland en enkele ons omringende landen. De bevindingen zijn gebaseerd op literatuuronderzoek en interviews die zijn gehouden met opsporingsambtenaren, officieren van justitie, parketsecretarissen, rechters-commissarissen, advocaten en enkele andere personen die beroepshalve met de tap te maken hebben. Het deel van het onderzoek dat zich richt op het gebruik van de tap in de Nederlandse opsporingspraktijk is verricht op landelijk niveau en in twee regio's die van elkaar verschillen in het aanbod aan misdrijven, de personele bezetting en de wijze waarop activiteiten die gepaard gaan met de inzet van bijzondere opsporingsbevoegdheden zijn georganiseerd. Deze regio's zijn niet gekozen om ze te vergelijken, maar om een breed beeld te kunnen schetsen van de wijze waarop de tap wordt ingezet. Onze gegevensverzameling heeft zich dus op regionaal niveau beperkt tot twee regio's, maar er zijn geen redenen om aan te nemen dat de algemene bevindingen uit dit onderzoek niet gelden voor andere Nederlandse politieregio's. In het deel dat zich richt op het gebruik van de tap in enkele ons omringende Europese landen, zijn de bevindingen opgetekend van de wijze waarop de tap wordt gebruikt in Engeland en Wales, Zweden en Duitsland. In dit afsluitende hoofdstuk brengen we de belangrijkste bevindingen uit dit rapport samen.

Waarborgen bij het gebruik van de telefoon en internettap

Met de inzet van een telefoon- of internettap maakt de overheid een inbreuk op de persoonlijke levenssfeer van een burger. Het recht op privacy is een grondrecht dat onder andere wordt gewaarborgd door het Europees Verdrag voor de Rechten van de Mens (art. 8 EVRM). Het openbaar gezag kan rechtmatig een inbreuk maken op dit grondrecht, maar in dat geval moet worden voldaan aan een aantal eisen. Het Europese Hof voor de Rechten van de Mens (EHRM) heeft een zestal criteria opgesteld waaraan het een nationale regeling met betrekking tot het aftappen van telefoon- en internetverkeer kan toetsen (zie onder andere de zaak *Valenzuela Contreras tegen Spanje*, EHRM 30 juli 1998). Zowel in Nederland als in de andere onderzochte landen heeft het gebruik van de telefoon- en internettap een wettelijke basis gekregen.

Eén van de voorwaarden gesteld door het EHRM is dat een tapbevel tot stand komt op basis van een rechterlijke beoordeling. In Nederland, Duitsland en Zweden is deze rechterlijke toetsing het sluitstuk van het autorisatieproces dat moet leiden tot een tapbevel. Het is hierbij steeds de openbare aanklager (OvJ) die een verzoek tot het gebruik van de telefoon- of internettap voorlegt aan de (onderzoeks)rechter (RC). In Engeland (en Wales) blijft de openbaar aanklager echter buiten het autorisatieproces en wordt het gebruik van de telefoon- of internettap geautoriseerd door een Secretary of State in plaats van een rechter. Daarmee lijkt Engeland (en Wales) niet te voldoen aan de genoemde verdragsrechtelijke eis. Niettemin heeft het EHRM in de zaak *Kennedy tegen het Verenigd Koninkrijk* (18 mei 2010) geoordeeld dat er op dit punt geen sprake is van een tekortkoming in de Britse regeling (RIPA 2000).
In alle onderzochte landen is in een wettelijke regeling vastgelegd bij welk soort strafbare feiten de telefoon- en internettap als opsporingsmiddel kan worden ingezet. Hoewel de regelingen per land verschillen, gaat het steeds om ernstige misdrijven. Of het gebruik van de telefoon- of internettap wordt geautoriseerd, hangt in alle onderzochte landen af van het oordeel over de noodzaak van de informatie die met een tap kan worden achterhaald voor de voortgang van het opsporingsonderzoek. Hierbij wordt steeds meegewogen of deze informatie niet op een *andere wijze* die *minder inbreuk maakt* op de privacy van de burger kan worden verkregen (subsidiariteitsbeginsel) en de inzet van het opsporingsmiddel in verhouding staat tot het misdrijf (proportionaliteitsbeginsel). In alle onderzochte landen kan een telefoon- of internettap zowel worden ingezet tegen verdachten als tegen betrokkenen. De maximale wettelijke termijn waarvoor een tapbevel (en de eventuele verlenging van dat tapbevel) geldt, verschilt per onderzocht land. In Nederland geldt een termijn van 4 weken, in Zweden een termijn van een maand. In Engeland (en Wales) geldt een termijn van 3

maanden (en in sommige gevallen zelfs van 6 maanden) en in Duitsland geldt eveneens een termijn van 3 maanden.
In Nederland, evenals in Zweden en Duitsland, geldt dat tapgesprekken gebruikt mogen worden als bewijsmiddel in een strafzaak. In Engeland (en Wales) mag dat niet als de informatie is verzameld op basis van een Engels tapbevel. In dat geval kan de informatie verkregen met een tap enkel gebruikt worden als (sturings)informatie in het opsporingsonderzoek. Komt het afgetapte materiaal echter uit het buitenland, bijvoorbeeld uit Nederland, en is dit materiaal naar Nederlandse maatstaven rechtmatig verkregen, dan mag het in een Engelse strafzaak wel als bewijs worden gebruikt.

In 2008 heeft een door de Britse regering ingestelde commissie, de *Privy Council*, geconcludeerd dat informatie die wordt verkregen door gebruikmaking van de telefoon- of internettap in beginsel wel gebruikt zou moeten kunnen worden als bewijsmiddel in een strafzaak. Vooralsnog is deze aanbeveling echter niet overgenomen door de Britse regering. In het kader van verdere waarborgen tegen schending van de privacy (onder andere art. 8 EVRM) is in Nederland, Duitsland en Zweden een regeling van kracht waarbij een burger die is onderworpen aan een telefoon- of internettap achteraf moet worden genotificeerd over het gebruik van dit heimelijke opsporingsmiddel. In Engeland (en Wales) bestaat een dergelijke regeling niet. Naar aanleiding van een notificatie kan een burger vervolgens beklag doen over bijvoorbeeld een mogelijke schending van de privacy. Hoewel een notificatie geen constitutief vereiste is om (eventueel later) beklag te doen, kan het wel dienstbaar zijn aan de rechtsbescherming van een burger. Voor het doen van beklag bestaan er in Engeland (en Wales) en Zweden onafhankelijke instanties die een dergelijke klacht in behandeling kunnen nemen. Daarnaast kent Zweden de figuur van de Openbaar Vertegenwoordiger (*Offentliga Ombud*), die als taak heeft om in de opsporing de rechten en integriteitsbelangen van individuen in het algemeen te bewaken. Daarbij dient deze vertegenwoordiger tevens toe te zien op de bescherming van de integriteit van derden.

Heersend beeld versus de realiteit
Het heersende beeld is dat er in Nederland veel wordt getapt. Het aantal taps op vaste lijnen is in Nederland al jaren stabiel, maar de opkomst van de mobiele telefoon heeft geresulteerd in een flinke toename van het aantal in gebruik zijnde telefoons, en daarmee ook van het aantal benodigde taps. Door de tapstatistieken af te zetten tegen het aantal in gebruik zijnde telefoonaansluitingen, krijgen de Nederlandse tapstatistieken meer perspectief. Hieruit blijkt dat vanaf 2007 voor minder dan één op de duizend in gebruik zijnde telefoonnummers in Nederland een tapbevel is afgegeven. Overigens neemt het aantal taps in Nederland de laatste jaren af, zowel in absolute zin (met bijna 17% in 2010 t.o.v. 2008) als in relatie tot het totale aantal in gebruik zijnde telefoonaansluitingen. Desondanks werden er in het jaar 2010 22.006 telefoontaps aangesloten. Dit lijkt – vooral ook in vergelijking met de statistieken die over andere landen beschikbaar zijn – veel te zijn.

De tapstatistieken van verschillende onderzochte landen zijn moeilijk met elkaar te vergelijken, doordat het aantal ingezette taps in deze landen verschillend wordt geregistreerd. Zo telt men in Engeland en Wales het aantal personen voor wie een tapbevel wordt afgegeven. Binnen één tapbevel kunnen vervolgens verschillende nummers en toestellen waar deze persoon gebruik van maakt worden opgenomen. Tussentijdse mutaties – bijvoorbeeld door verandering van telefoontoestel of simkaart – worden in Engeland apart geregistreerd. Uit de Engelse tapstatistieken kan worden afgeleid dat personen frequent wisselen van toestel en van nummer, aangezien het aantal tussentijdse mutaties van de lopende bevelen veel groter is dan het aantal tapbevelen. In Zweden kunnen er meerdere tapbevelen worden afgegeven op één persoon, en binnen elk bevel kunnen weer meerdere nummers of toestellen worden opgenomen. Hoewel er in Zweden gegevens voorhanden zijn over het aantal afgetapte nummers, blijken deze gegevens niet compleet te zijn.
De wijze waarop de Duitse tapstatistieken zijn samengesteld is niet geheel duidelijk. In Duitsland worden tapbevelen per nummer geregistreerd, maar de beschikbare cijfers lijken niet allesomvattend te zijn. Zo lijken ondermeer de korte spoedtaps die binnen drie dagen weer worden afgesloten niet te worden opgenomen in de statistieken.

De Nederlandse statistieken lijken het meest compleet te zijn als het gaat om de aantallen afgetapte nummers, telefoontoestellen en IP- en e-mailadressen. De Nederlandse cijfers geven echter geen inzicht in het aantal personen dat jaarlijks wordt onderworpen aan een tap (zoals dat in Engeland en Zweden het geval is) of in het aantal opsporingsonderzoeken waarin de tap wordt ingezet en de aard van deze zaken (zoals bijvoorbeeld in Zweden). Hierdoor geven de Nederlandse cijfers weinig inzicht in de mate waarin Nederlandse opsporingsdiensten door het inzetten van een tap een inbreuk maken op de privacy van verdachten en betrokkenen. De politieke belangstelling voor het gebruik van de tap in de opsporingspraktijk komt voort uit het belang dat wordt gehecht aan de persoonlijke levenssfeer van betrokkenen. De mate waarin opsporingsinstanties hierop een inbreuk maken kan echter uit de voorhanden zijnde statistieken niet goed worden afgeleid, omdat niet duidelijk wordt hoeveel personen precies zijn getapt.
Omdat uit de beschikbare statistieken moeilijk kan worden afgeleid op welke wijze de tap in de praktijk wordt ingezet, is het beeld dat in dit rapport wordt geschetst vooral gebaseerd op interviews met personen die beroepshalve een brede kijk hebben op de wijze waarop de tap in de praktijk wordt gebruikt, de overwegingen die aan de inzet van de tap ten grondslag liggen, de ervaringen die ermee zijn opgedaan en de resultaten die ermee worden bereikt.

Gewaardeerd opsporingsmiddel

Een algemeen beeld dat uit dit onderzoek naar voren komt, is dat de tap in Nederland en in de andere door ons onderzochte landen een door politie en justitie gewaardeerd opsporingsmiddel is dat zijn nut in de loop der jaren ruimschoots heeft bewezen. De informatie die met behulp van een tap wordt verkregen speelt op verschillende manieren een rol in het opsporingsproces. Zo kan een tap inzichtelijk maken welke mensen met elkaar in contact staan, hoe de verhoudingen tussen deze mensen zijn en ook waar deze personen zich bevinden en soms met welke activiteiten zij zich bezighouden. Er blijkt nog steeds veel gecommuniceerd te worden via de telefoon. Wel blijkt uit het onderzoek dat de opbrengst van de tap in de loop van de tijd is veranderd. Waar informatie uit de tap vroeger gebruikt kon worden als direct bewijs, wordt de tap tegenwoordig steeds vaker ingezet om sturingsinformatie, opsporingsinformatie en indirect bewijs te kunnen vergaren. Wat betreft de wijze waarop de informatie uit de tap in de opsporing wordt benut is er – zoals hierboven al werd aangegeven – een opvallend verschil te constateren tussen Engeland en Wales en de andere onderzochte landen. In Engeland en Wales kan informatie die wordt verkregen met een tap niet gebruikt worden als bewijsmiddel. Telefoon- en internettaps worden daar alleen ingezet om sturingsinformatie te verkrijgen.
Aan het feit dat de opbrengst van de tap in de loop der jaren is veranderd kunnen twee mogelijke redenen ten grondslag liggen. Allereerst blijkt dat personen die zich bezighouden met criminele activiteiten bewust rekening houden met de mogelijkheid dat ze kunnen worden getapt. Zij maken gebruik van versluierde communicatie en van andere strategieën waarmee ze hun werkelijke bedoelingen proberen af te schermen van de buitenwereld. Ten tweede is het communiceren op afstand de afgelopen jaren sterk veranderd door de opkomst van mobiele telefoons, de smartphone en communicatiemogelijkheden via internet. Hierdoor is communicatie versnipperd geraakt en niet eenvoudig meer te ondervangen met een (enkele) telefoontap.

Het gebruik van de tap in de praktijk

Hoewel er in Nederland veel 'lijnen' worden afgetapt, geven respondenten aan dat de tap eerder gericht en doelmatig wordt ingezet, dan breed en ongericht. Dat men probeert de tap zo gericht mogelijk in te zetten heeft een aantal achtergronden. In de eerste plaats wordt met de tap een inbreuk gemaakt op de privacy, niet alleen van de getapte persoon, maar ook van de personen die met deze persoon in contact staan. In het algemeen blijken opsporingsteams zorgvuldig te overwegen of een tap noodzakelijk is, en neigen zij ertoe te kiezen voor lichtere opsporingsmiddelen (die een minder grote inbreuk maken op de privacy van personen) als men met deze lichtere middelen toe kan. De overwegingen hieromtrent vinden overigens niet zozeer plaats op ethische gronden, maar vooral omdat de inzet van de tap als een arbeidsintensief opsporingsmiddel wordt gezien dat niet lukraak moet worden ingezet. Voorts wordt door zowel de OvJ als door de RC getoetst of het middel proportioneel is gezien de zwaarte van het misdrijf waarnaar onderzoek wordt verricht, en in hoeverre het

noodzakelijk is om het middel in te zetten (subsidiariteit). Rechters-commissarissen geven aan slechts weinig tapaanvragen af te wijzen. Bovendien zoeken zij de bescherming van de persoonlijke levenssfeer van de betrokkenen vooral in het begrenzen van duur van de inbreuk door te letten op de termijnen waarvoor ze een tapbevel afgeven. Voor lichtere misdrijven worden doorgaans kortere termijnen aangehouden. Voorts zijn zij geneigd om tapbevelen op betrokkenen voor een kortere periode af te geven dan een tapbevel op een verdachte.
Zoals gezegd zitten opsporingsteams niet te wachten op het uitluisteren en uitwerken van allerlei telefoonlijnen die niet van belang zijn voor het opsporingsonderzoek, omdat met het uitwerken daarvan veel capaciteit is gemoeid. Daarom zijn zij genoodzaakt gerichte keuzen te maken om het nodeloos verlies van opsporingscapaciteit te voorkómen. Echter, als een verdachte tien telefoons in gebruik heeft, is het noodzakelijk om alle tien deze lijnen af te tappen, omdat het moeilijk is om vooraf te bepalen over welke lijnen cruciale informatie komt. Achteraf kan soms worden geconstateerd dat bepaalde lijnen niet relevant waren, maar van tevoren is dat meestal minder goed te bepalen. Om die reden worden er ook tussentijds wel taps afgesloten op instigatie van het opsporingsteam.

Hoewel met het aftappen en uitwerken van telefoon- en internetlijnen veel capaciteit is gemoeid blijkt – uit de interviews – dat de opbrengsten van de tap vaak opwegen tegen de kosten ervan (in termen van tijd en menskracht). Zoals gezegd is de tap nog steeds een gewaardeerd opsporingsmiddel. Deze waardering voor het middel blijkt ook uit het feit dat de infrastructuur voor het tappen in Nederland goed is georganiseerd. Er is de afgelopen jaren flink geïnvesteerd in de mogelijkheden om efficiënt gebruik te kunnen maken van de telefoontap. Het vertrouwen binnen de opsporingsdiensten in het middel is groot, en de opsporingsteams zijn goed bekend met de werkzaamheden en de administratieve handelingen die gepaard gaan met het aftappen van telefoonlijnen. De ruime expertise op het gebied van dit opsporingsmiddel staat in schril contrast met de ervaring, expertise en opsporingscapaciteit die aanwezig is op het gebied van sommige andere bijzondere opsporingsmiddelen. Het feit dat opsporingsambtenaren bij het aftappen van telecommunicatie nauwelijks persoonlijke risico's lopen en dat de tap ook nauwelijks een afbreukrisico voor het onderzoek in zich draagt – in tegenstelling tot de risico's die gepaard gaan met bijvoorbeeld infiltratie – draagt zeker bij aan de waardering van de tap als opsporingsmiddel.
De respondenten die zich in Nederland bezighouden met de opsporing van zware en georganiseerde criminaliteit geven aan dat de tap voor hen vaak het belangrijkste opsporingsmiddel is. Volgens eigen zeggen sluiten ook deze teams echter geen taps aan zonder zorgvuldig het nut en de noodzaak van het middel te overwegen. Een belangrijke reden daarvoor is gelegen in het feit dat opsporingsteams proberen de beschikbare opsporingscapaciteit zo efficiënt mogelijk in te zetten. Wanneer besloten wordt tot de inzet van de tap, is de capaciteit van het team een belangrijke factor die bepaalt hoeveel taps er worden aangesloten en voor welke periode. Bij het opstellen van een plan van aanpak en bij de besluitvorming over de inzet van de tap wordt door de teamleider en de officier van justitie op de beschikbare opsporingscapaciteit geanticipeerd. Toch kan het voorkomen dat er uiteindelijk te veel energie en capaciteit wordt besteed aan het uitluisteren en uitwerken van de taps, waardoor er te weinig capaciteit overblijft voor andere opsporingsactiviteiten, of waardoor er achterstanden ontstaan bij het uitwerken van de verzamelde informatie.
Naast de wettelijke eisen en de capaciteit van het team, spelen bij de keuze voor de inzet van de tap factoren een rol zoals de persoonlijke voorkeur van de teamleider, het relatieve gemak waarmee het middel van achter het bureau kan worden ingezet en het ontbreken van andere gelijkwaardige opsporingsmiddelen waarmee de benodigde informatie kan worden achterhaald.

Als we kijken naar de wijze waarop de tap in het buitenland wordt ingezet bij de aanpak van verschillende soorten misdrijven, dan lijkt dat vergelijkbaar te zijn met de wijze waarop deze in Nederland wordt ingezet. In de vergelijkingslanden blijkt de tap veelvuldig te worden ingezet bij de aanpak van georganiseerde misdaad, de opsporing van levensdelicten en andere vormen van zware criminaliteit. Evenals de Nederlandse respondenten geven de

buitenlandse respondenten aan dat ze bij de aanpak van dergelijke delicten feitelijk niet zonder de tap kunnen.

Administratieve last

Uit het onderzoek naar de inzet van de tap in Nederland, blijkt dat het grote aantal lijnen dat per jaar wordt getapt, gepaard gaat met een aanzienlijke administratieve last. In de huidige situatie wordt voor elk telefoonnummer of toestel dat wordt afgetapt een apart bevel gemaakt. Overwogen zou kunnen worden om, in het huidige tijdperk waarin mensen vaak over meer dan één communicatiemiddel beschikken, over te stappen naar een tapbevel dat gekoppeld is aan een persoon in plaats van aan een telefoonnummer of toestel, een werkwijze die ook in een aantal onderzochte landen wordt gebezigd. Dit zou de administratieve druk kunnen verminderen. De administratieve last zou nog verder kunnen worden verminderd door ook een oplossing te zoeken voor tussentijdse wijzigingen in het gebruik van telecommunicatiemiddelen. Zo zou de rechter-commissaris bijvoorbeeld kunnen beslissen over de vraag of de verdenking tegen een bepaalde persoon zwaar genoeg is om gedurende de wettelijk vastgestelde termijn van maximaal 4 weken, alle telecommunicatiemiddelen van deze persoon te mogen tappen indien het opsporingsteam dit van belang acht, zonder dat er bij tussentijdse wijzigingen van telefoon of -nummer opnieuw toestemming bij de rechters-commissarissen gevraagd hoeft te worden. Een dergelijke werkwijze zou tevens meer inzicht bieden in het daadwerkelijke aantal getapte personen in Nederland.

Het verwerken van tapgesprekken

Een ander punt dat uit dit onderzoek naar voren komt en aandacht verdient, is dat met het uitluisteren en uitwerken van telefoontaps veel opsporingscapaciteit is gemoeid. Alle gesprekken die over een lijn komen moeten worden uitgeluisterd en vaak ook worden uitgewerkt. Hiermee wordt eigenlijk afgestapt van de doelgerichte wijze waarmee de meeste andere opsporingsmiddelen worden ingezet. Wanneer ergens een huiszoeking plaatsvindt, worden doorgaans alleen die items gezocht en in beslag genomen die mogelijk gerelateerd zijn aan een misdrijf; tijdens het forensische onderzoek worden alleen die sporen veiliggesteld en geanalyseerd waarvan men vermoedt dat ze samenhangen met het misdrijf; en ook het observatieteam wordt vooral ingezet wanneer men denkt misdrijf gerelateerd handelen te kunnen observeren. Bij de inzet van de meeste opsporingsmethoden wordt de ruis – dus de informatie die vermoedelijk niet met het vermeende misdrijf samenhangt – zo veel mogelijk gefilterd en genegeerd. Op deze manier probeert men de opsporing gericht en efficiënt te laten verlopen en geen onnodige inbreuk te maken op de privacy van die personen tegen wie deze opsporingsmiddelen worden ingezet. Bij de tap ligt dit anders. Er wordt niet alleen geluisterd op momenten waarop men denkt dat er mogelijk misdrijfgerelateerde gesprekken kunnen worden opgevangen. Alle gesprekken die gevoerd worden via de afgetapte lijnen moeten worden verwerkt. Niet ter zake doende gesprekken hoeven weliswaar niet letterlijk te worden uitgewerkt en mogen als zodanig worden weggeschreven, maar ze moeten wel worden uitgeluisterd en worden geregistreerd. Kortom, bij tappen mag er niet gericht op misdrijfgerelateerde informatie worden gefocust. Dit is opvallend. Door het middel gerichter in te zetten zou de privacyschending kunnen afnemen en zou de opsporing efficiënter kunnen verlopen. Vermoedelijk is het idee hierachter ooit geweest dat informatie die afkomstig is uit telefoongesprekken niet uit de context mag worden gehaald, omdat deze anders eenzijdig zou kunnen worden geïnterpreteerd. Toen alle ‘communicatie op afstand’ nog plaatsvond via één vaste telefoonlijn was het wellicht nog mogelijk om deze contextafhankelijkheid van informatie te waarderen. Het probleem is echter dat mensen hun communicatiestromen tegenwoordig zelf in allerlei opzichten hebben gefragmenteerd. Ze gebruiken meerdere telefoons voor verschillende doelen en communiceren deels door middel van geschreven tekst. Welk deel van de communicatie wel en niet wordt opgevangen in een opsporingsonderzoek is nu afhankelijk van het aantal telefoons dat wel en niet wordt afgetapt en van de mate waarin ook de internetcommunicatie wordt meegenomen. Daarmee verdwijnt feitelijk het belang van de eis om alle gesprekken die via een afgetapte telefoon worden opgevangen uit te luisteren en te verwerken.
Een punt dat hiermee samenhangt betreft de eisen die gesteld worden aan het uitwerken van de *internettap*. Als het van belang wordt geacht om communicatiestromen in hun

context te beschouwen, zouden de gegevens die worden opgevangen met een internettap op dezelfde manier moeten worden verwerkt als de gegevens die met een telefoontap worden achterhaald. De grote hoeveelheid informatie die via het internet wordt uitgewisseld noodzaakt echter tot anders handelen. Momenteel wordt er aan gewerkt om internettaps in de opsporing zo doelgericht mogelijk in te zetten en om zo slim mogelijk te zoeken in de onderschepte datastroom, waarbij dan maar een deel van de afgetapte informatie kan worden bekeken. Dit roept de vraag op waarom bij de telefoontap nog steeds wordt vastgehouden aan de eis dat alle opgevangen communicatie moet worden verwerkt. Door in de opgevangen gesprekken meer gericht te zoeken naar relevante informatie zou de telefoontap beslist aan efficiëntie kunnen winnen.

Alternatieven voor de tap

Uit de voor dit onderzoek gevoerde gesprekken blijkt dat het tappen is verankerd in de Nederlandse opsporingspraktijk en een lange geschiedenis kent met vele succesverhalen. Dit heeft het denken en werken in de opsporing gevormd. Echter, het grote belang dat wordt gehecht aan de tap zou een bedreiging kunnen vormen voor de creativiteit van de opsporing. De Nederlandse respondenten geven aan dat het in hun perceptie ontbreekt aan goede alternatieven voor de tap.

Dit beeld, dat er geen goed alternatief opsporingsmiddel voor de telefoontap aanwezig zou zijn, wordt in het buitenlandse onderzoek niet direct bevestigd. Allereerst blijkt dat er in Engeland (en Wales), veel vaker gebruik wordt gemaakt van Covert Human Intelligence Sources (CHIS) dan van de telefoontap. In Nederland wordt slechts zeer sporadisch gebruik gemaakt van de inzet van infiltranten. In de ogen van de Nederlandse opsporingsinstanties wordt met de inzet van infiltranten een grotere inbreuk gemaakt op de persoonlijke levenssfeer van de personen die aan dit opsporingsmiddel worden onderworpen, dan met de inzet van de telefoontap. De terughoudendheid die in Nederland wordt betracht als het gaat om de inzet van andere bijzondere opsporingsmiddelen dan de tap is mogelijk een gevolg van de IRT-affaire, die er eind jaren '90 van de vorige eeuw toe heeft geleid dat de inzet van heimelijke opsporingsmiddelen in Nederland is gereguleerd, hetgeen de inzet ervan heeft beperkt. In Nederland is de inzet van de telefoontap feitelijk naast stelselmatige observatie het enige heimelijke opsporingsmiddel dat echt veelvuldig wordt ingezet. In Engeland en Wales, maar ook in Duitsland en Zweden wordt ten aanzien van de inzet van andere heimelijke opsporingsmiddelen relatief minder terughoudendheid betracht en is de verhouding tussen het inzetten van de tap en het inzetten van andere heimelijke opsporingsmiddelen anders dan in Nederland.

De Nederlandse respondenten geven aan niet te beschikken over andere opsporingsmiddelen waarmee ze zo snel en ongemerkt zo dicht bij een verdachte kunnen komen zonder daarmee het gedrag van de verdachte te beïnvloeden. Minder ingrijpende middelen hebben niet dezelfde opbrengsten en van de meer ingrijpende opsporingsmiddelen – die soms wel zouden kunnen dienen als alternatief – zijn de procedurele drempels en administratieve lasten hoger. Bovendien is er in zaken waarin voor deze alternatieve methoden wordt gekozen vaak toch nog behoefte aan de tap om deze opsporingsmethoden goed in te kunnen zetten, te kunnen sturen of te kunnen ondersteunen. In die zin gaat het eerder om een aanvulling op dan om een alternatief voor de tap. Daarnaast blijkt het in Nederland niet mogelijk te zijn om in elk opsporingsonderzoek waarin is voldaan aan de gestelde eisen van proportionaliteit en subsidiariteit gebruik te maken van alle voorhanden zijnde bijzondere opsporingsmiddelen, omdat voor de inzet van bepaalde opsporingsmethoden specialistische teams of diensten moeten worden ingehuurd. Deze diensten zijn voorbehouden aan geprioriteerde onderzoeken waarvoor voldoende budget en capaciteit wordt vrijgemaakt. Daarmee is de subsidiariteitseis dus feitelijk een formaliteit en een juridische eis waarvan de uitkomst van te voren vaststaat door het ontbreken van alternatieven voor de telefoontap.

Als het gaat om de inzet van lichtere alternatieven, lijkt het opvragen van verkeersgegevens zich met name in Engeland en Duitsland te ontwikkelen tot een zelfstandig opsporingsmiddel, dat naast de telefoontap wordt ingezet. In Zweden is het aftappen van telefoonlijnen en het opvragen van (toekomstige) verkeersgegevens veel vaker aan elkaar gekoppeld en is het verschil in de mate waarin deze middelen worden ingezet klein. In Engeland (en Wales) is het verschil in de mate waarin verkeersgegevens worden opgevraagd en de mate waarin

gebruik wordt gemaakt van de telefoontap veel groter, in die zin dat er veelvuldig gebruik wordt gemaakt van verkeersgegevens. Een mogelijke verklaring voor deze ontwikkeling kan zijn dat opsporingsdiensten de wijze waarop ze telecommunicatiegegevens gebruiken hebben aangepast aan het feit dat afgetapte personen, bekend met de praktijk van het aftappen, inhoudelijk niet veel zeggen door de telefoon, terwijl aan het uitwerken van die gesprekken veel opsporingscapaciteit verloren gaat. Mogelijk heeft dit ertoe geleid dat het gebruik van de tap is verschoven van het afluisteren van gesprekken naar het in kaart brengen van sociale contacten (netwerken) en van de locaties waar verdachte personen zich bevonden tijdens bepaalde gebeurtenissen. Verkeersgegevens zijn voor dit doel uitermate geschikt en het is bovendien veel minder arbeidsintensief om telecomgegevens op deze wijze te benutten. Het onderzoek in Duitsland geeft eenzelfde beeld te zien als we voor Engeland en Wales hebben geschetst. In een onderzoek van het Max-Planck-Institut (Albrecht, Grafe & Klichling, 2008) wordt er op gewezen dat het gebruik van verkeersgegevens zich in Duitsland in feite heeft ontwikkeld tot een onafhankelijke opsporingsmethode, die een ruime toepassing vindt, ook bij de opsporing van meer conventionele misdrijven. Hierbij moet wel worden opgemerkt dat de cijfermatige gegevens over de ontwikkelingen in het gebruik van verkeersgegevens vooral gebaseerd zijn op schattingen en prognoses. Een trend die wel duidelijk zichtbaar is in de Duitse geregistreerde cijfers, is de forse toename in het opvragen van abonneegegevens door opsporingsdiensten. Deze forse toename hangt vermoedelijk samen met de toename in het gebruik van verkeersgegevens. Als gevoerde gesprekken worden afgetapt en uitgeluisterd, kunnen de opsporingsdiensten via deze gesprekken vaak achterhalen aan wie de telefoonnummers toebehoren waarmee de afgetapte persoon contacten onderhoudt. Zonder deze gespreksgegevens moeten van alle nummers die in de verkeersgegevens naar voren komen de identificerende gegevens worden opgevraagd bij een centrale instantie om er betekenis aan te kunnen geven. Ook in Nederland worden er vaak abonneegegevens opgevraagd bij het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Dit levert voor Nederlandse opsporingsteams echter niet altijd het gewenste resultaat op, omdat er veel gebruik wordt gemaakt van niet op naam staande telefoons en prepaid kaarten.
Verkeersgegevens worden in de Nederlandse praktijk ook ingezet voor het in kaart brengen van criminele organisaties en netwerken. De locatiegegevens die bij verkeersgegevens worden geleverd, kunnen soms gebruikt worden om de inzet van andere opsporingsmiddelen, zoasl een observatieteam, te kunnen sturen. Echter, voor een gerichte sturing van het opsporingsonderzoek mist men volgens de Nederlandse respondenten toch te veel informatie wanneer enkel afgegaan wordt op verkeersgegevens, en er geen zicht is op de inhoud van de gesprekken. Volgens de Nederlandse respondenten is het opvragen van verkeersgegevens een waardevol opsporingsmiddel, maar vormt het geen volwaardig alternatief voor de tap.

De perceptie van de zwaarte van verschillende bijzondere opsporingsmiddelen verschilt tussen de onderzochte landen. In Nederland vinden we het inzetten van infiltranten bijvoorbeeld een zwaarder opsporingsmiddel dan de inzet van een telefoontap, en is het aantal infiltraties zeer beperkt. Afgaande op de statistieken lijkt dit in Engeland precies andersom te zijn. Daar blijkt het inzetten van infiltranten het meest ingezette bijzondere opsporingsmiddel te zijn, terwijl het aantal ingezette telefoontaps daar relatief beperkt is. Deze verschillen in perceptie zijn boeiend en de bevindingen uit de landenvergelijking laten zien dat een maatschappelijke discussie over de waarde van verschillende bijzondere opsporingsbevoegdheden zinvol is om de opsporingspraktijk verder te kunnen ontwikkelen. Een discussie over de bijdrage die verschillende opsporingsmiddelen leveren aan het opsporingsproces, van de verschillende wijzen waarop deze middelen kunnen worden ingezet en van de inbreuken die daarmee worden gemaakt op de persoonlijke levenssfeer van verdachten en betrokkenen is zinvol om het nut, de noodzaak en de keerzijde van afzonderlijke opsporingsmethoden te kunnen evalueren. Daarbij gaat het ondermeer om de vraag wat in Nederland meer is gewenst; een korte gerichte inzet van een opsporingsmiddel dat als minder ingrijpend wordt gezien, of de langdurige inzet van een minder ingrijpend middel.
Bij het doorontwikkelen van opsporingsmethoden, zouden vooral ook de mogelijkheden van het internet dienen te worden overwogen. De geïnterviewde respondenten geven aan dat er

wel wordt nagedacht over de nieuwe mogelijkheden die het internet biedt voor traditionele bijzondere opsporingsbevoegdheden zoals observatie en pseudo-koop. Van een brede inzet is echter geen sprake, terwijl het internet voor veel mensen steeds meer een verlengde is geworden van het dagelijkse leven. Om die reden zou de opsporing zich ook veel sterker op het internet kunnen concentreren. Door bijzondere opsporingsbevoegdheden toe te passen op het internet zullen deze methoden breder en efficiënter kunnen worden ingezet, hetgeen nieuwe mogelijkheden voor de opsporing biedt. Voorts zullen ontwikkelingen op dit gebied ook gevolgen hebben voor de perceptie van de inbreuk van dergelijke middelen op de privacy van de personen tegen wie ze worden ingezet. Ontwikkelingen op dit gebied zijn volop gaande en de inzet van deze middelen is vooralsnog voorbehouden aan specialistische eenheden. Een bredere toepassing van bijzondere opsporingsbevoegdheden op internet zal het voor de recherche naar verwachting mogelijk maken om meer doordachte keuzes te maken tussen de verschillende alternatieve opsporingsmethoden en duidelijkere afwegingen te maken gebaseerd op de proportionaliteit en subsidiariteit van de in te zetten alternatieven.

De toekomst van de (internet)tap

Door technologische ontwikkelingen en veranderingen in het telefoongebruik, zal de huidige telefoontap naar verwachting steeds minder relevante opsporingsinformatie opleveren. De respondenten constateren dat er steeds meer wordt gecommuniceerd via het internet. Zowel de internettap zelf als de opsporingsambtenaren blijken echter nog niet klaar te zijn voor de grotere rol die de internettap naar verwachting zal gaan innemen. Vooralsnog is het middel weinig gebruiksvriendelijk en lijkt het nog niet toegerust te zijn voor een bredere inzet. De grote hoeveelheid gegevens die via het internet wordt opgevangen wordt genoemd als probleem bij het verwerken van de afgetapte informatie. Kennis over gedegen analyses in grote databestanden is schaars. Daarnaast hebben respondenten problemen met het uitlezen van de getapte informatie. Anders dan bij de telefoontap krijgt men met de internettap geen mooie één op één weergave van wat de getapte persoon op zijn beeldscherm ziet. De gegevens die via de internettap worden binnengehaald vergen een nadere interpretatie. Of het wenselijk en technisch mogelijk is om het middel zo vorm te geven dat het net zo breed kan worden ingezet als de telefoontap is een belangrijke vraag.

Ook in de interviews met experts in de ons omringende landen is ingegaan op het gebruik en de inzet van de internettap. Over de inzet van het opsporingsmiddel zijn echter minder gegevens verstrekt dan verwacht. De belangrijkste reden hiervoor is dat het een opsporingsmiddel blijkt te zijn waarover de geïnterviewde personen niet veel in de openbaarheid willen brengen. Het gebrek aan openheid op dit punt lijkt te maken te hebben met mogelijkheden maar vooral ook met de onmogelijkheden van de inzet van de internettap. Het algemene beeld dat in de onderzochte landen wel naar voren komt is dat, net als in Nederland, de internettap veel minder vaak wordt ingezet dan de telefoontap. Daarnaast geven de buitenlandse respondenten aan dat de grote hoeveelheden data die met een internettap binnengehaald kunnen worden moeilijk te interpreteren zijn, hetgeen overeenkomt met de Nederlandse situatie.

Uit het onderzoek blijkt dat de internettap op dit moment in Nederland om diverse redenen niet breed kan worden ingezet. Zo blijken er in de korpsen te weinig specialisten op dit gebied voorhanden om de internettap zoals we die nu kennen optimaal te kunnen benutten. Door een respondent werd zelfs opgemerkt dat er korpsen zijn die de inzet van de internettap mijden door een gebrek aan kennis. Het op korte termijn toevoegen van meer kennis en specialisten om dit probleem op te lossen ligt dan ook voor de hand.

Ook het opsporingsmiddel zelf zou echter aangepast kunnen worden. Een door de respondenten veel genoemd probleem van de internettap is de grote hoeveelheid data die wordt afgevangen. De huidige internettap vangt al het verkeer af op een getapte lijn. Deze gegevens worden later doorzocht op relevantie voor de opsporing of voor de bewijsvoering. Om deze grote hoeveelheid data te kunnen beperken, opperen specialisten de inzet van technieken zoals *deep-packet-inspection*. Dit is een techniek die het mogelijk maakt om in grote datastromen informatie te selecteren die men wel en niet wil onderscheppen. Vanuit het oogpunt van de inbreuk op de persoonlijke levenssfeer die een internettap maakt is hiermee winst te behalen, aangezien met het selectief aftappen enkel voor de opsporing relevante informatie van een persoon wordt opgeslagen. Alle informatie die

opsporingsdiensten niet selecteren wordt niet opgeslagen. Een aanpassing zoals deze maakt de inzet van het opsporingsinstrument naar verwachting doelmatiger en efficiënter.
Een ander belangrijk knelpunt dat de inzet van de internettap bemoeilijkt, is het feit dat steeds meer informatie die via het internet wordt verzonden is voorzien van encryptie. Dit maakt het ingewikkeld en soms zelfs onmogelijk om de inhoud van gegevens te kunnen ontsluiten ten behoeve van de opsporing. Telecommunicatiediensten via internet worden bijna standaard versleuteld. Nederlandse aanbieders van online telecommunicatie vallen onder de aftapplicht zoals omschreven in hoofdstuk 13 van de Telecommunicatiewet en vormen geen probleem voor de aftapbaarheid van de communicatie die via deze aanbieders verloopt. Maar buitenlandse aanbieders van online telecommunicatiediensten blijken, ook wanneer deze zich nadrukkelijk op de Nederlandse markt richten, niet altijd goed aftapbaar te zijn. In het rapport van Stratix (2009) werd hier al op gewezen en dit probleem neemt volgens een expert toe. Het internet en de diensten die daarop worden aangeboden zouden een duidelijker plek moeten krijgen in de regelgeving (zie: Stratix 2009) om de aftapbaarheid te waarborgen en de inzet van de internettap effectief te houden. Dit zal uiteindelijk de inzet van zwaardere opsporingsmiddelen kunnen beperken.
Het probleem van niet te ontsleutelen encryptie kan in theorie worden ondervangen door een computer of telefoon op afstand binnen te dringen en de informatie af te tappen voordat deze wordt versleuteld. Maar dit is een techniek waarbij altijd gevaar voor detectie bestaat en die bovendien niet generiek toepasbaar is. Daarbij mag, vanwege de grote inbreuk die het middel maakt op de persoonlijke levenssfeer, worden verwacht dat aan een eventuele inzet hiervan zeer strenge eisen worden gesteld.
Voor het toepassen van hierboven genoemde technieken zoals *deep-packet inspection* en het binnendringen van een computer op afstand ontbreekt op dit moment een expliciete wettelijke basis. Om de opsporing bij de tijd te houden en om digitale communicatie toegankelijk te houden voor opsporingsdiensten, zijn wettelijke aanpassingen een vereiste. De Wet BOB is geschreven in een tijdperk waarin internet en mobiel telefoneren nog in de kinderschoenen stonden. Daarnaast blijkt de aftapbaarheid van online communicatiediensten in gevaar door een te beperkte reikwijdte van de regelgeving hieromtrent. Vanuit deze oogpunten is het raadzaam een nieuwe discussie over aanpassingen van de BOB-wetgeving en de aftapbaarheid van online telecommunicatiediensten te agenderen.

Summary

Under construction

Literatuur

Albrecht, H.J., Dorsch, C., & Krüpe, C. (2003). *Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen.* Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht.

Albrecht, H.J., Grafe, A., & Kilchling, M. (2008). *Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO*. Berlin: Duncker & Humblot.

Albrecht, H.J., & Kilchling, M. (2009). *Die Überwachung von Telekommunikations-Verkehrsdaten*, Forschungsbericht 2009. München: Max-Planck-Institut für ausländisches und internationales Strafrecht 2009.

Asscher, L.F., & Ekker, A.H. (red.) (2003). *Verkeersgegevens: Een juridische en technische inventarisatie*. Amsterdam: Otto Cramwinckel Uitgever.

Baardewijk, J., Brink, G.J.M. van den, & Os, P. van (2007). *Meer heterdaadkracht: 'Aanhoudend in de buurt'*. Apeldoorn: Politieacademie.

Beijer, A., Bokhorst, R. J., Boone, M., Brants, C. H., & Lindeman, J. M. W. (2004). *De Wet Bijzondere opsporingsbevoegdheden: eindevaluatie.* Den Haag: Boom Juridische uitgevers. Onderzoek en Beleid 222.

Bernardt, Y., & Canoy, M. (1997). Hordenlopen van monopolie naar markt. *Economisch Statistische Berichten*, 82(4114), pp. 556-559.

Bleichrodt, F.W., Mevis, P.A.M., & Volker, B.W.A. (2011). *Vergroting van de slagvaardigheid van het strafrecht, een rechtsvergelijkend perspectief.* Rotterdam: Erasmus Universiteit Rotterdam.

Bloem, A., & Aarts, R.A.J. (2000). Het gebruik van gegevens van telecommunicatie. In: H. Moerland & B. Rovers (red.), *Criminaliteitsanalyse in Nederland. '*s-Gravenhage: Elsevier bedrijfsinformatie BV.

Blom, T. (2009). Inleidende opmerkingen bij de Titels IVA-VE van Boek I. In: C.P.M. Cleiren & J.F. Nijboer (red.). *Strafvordering: Tekst & Commentaar: De tekst van het Wetboek van Strafvordering en enkele aanverwante wetten voorzien van commentaar* (8e druk) (pp. 439-657). Deventer: Kluwer.

Bokhorst, R.J. (2004). De telefoontap in grote opsporingsonderzoeken. *Justitiële Verkenningen, 30(4)*, pp. 84-95.

Bokhorst, R. J., Kogel, C. H. de, & Meij, C. F. M. van der (2002). *Evaluatie van de Wet BOB: fase 1. De eerste praktijkervaringen met de Wet Bijzondere opsporingsbevoegdheden.* Den Haag: WODC. Onderzoek en Beleid 197.

Bokhorst, R. J., Steeg, M. van der, & Poot, C. J. de (2011). *Rechercheprocessen bij de bestrijding van georganiseerde criminaliteit.* Den Haag: WODC. Cahier 2011-11.

Bureau Jansen & Jansen (1999). *Luisterrijk: Een gids over afluisteren*. Amsterdam: Bureau Jansen & Jansen / Papieren Tijger.

Buruma, Y. (2001). *Buitengewone opsporingsmethoden.* Deventer: Tjeenk Willink.

Carlson, L. (2009). *The Fundamentals of Swedish Law*. Lund: Studentlitteratur.

Chavannes, R. (2008). Veel taps, weinig verantwoording. *Mediaforum,* 2008(6), 245.

CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie) (2008). *Jaarverslag 2008*. Den Haag: CIOT.

CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie) (2009). *Jaarverslag 2009*. Den Haag: CIOT.

Cleiren, C. P. M., & Nijboer, J. F. (red.) (2009). *Strafvordering: Tekst & Commentaar: De tekst van het Wetboek van Strafvordering en enkele aanverwante wetten voorzien van commentaar* (8e druk). Deventer: Kluwer.

CBP (College Bescherming Persoonsgegevens) (2003). *Onderzoek naar de waarborging van de vertrouwelijke communicatie van advocaten bij de interceptie van telecommunicatie*. Den Haag: CBP.

CBP (College Bescherming Persoonsgegevens) (2007). *De vernietiging van geheimhoudersgesprekken: Een onderzoek naar de naleving van artikel 126aa lid 2 Sv door de tapkamers in Epe en Driebergen.* Den Haag: CBP.

Colvin, M., & Cooper, J. (red.) (2009). *Human rights in the investigation and prosecution of crime*. Oxford: Oxford University Press.

Commissie- Van Traa (1996). *Inzake opsporing: eindrapport*. Den Haag: SDU.

Custers, B. (2008). Tapping and data retention in ultrafast communication networks*. Journal of international commercial law and technology*, 3(2), 94-100.

De politie tapt zich een ongeluk, of het helpt weet niemand, www.depers.nl, 09-09-09.

Elsner, B., & Peters, J. (2006). The Prosecution Service Function within the German Criminal justice System. In: J.-M. Jehle & M. Wade (red.), *Coping with Overloaded Criminal Justice Systems: The Rise of Prosecutorial Power Across Europe* (pp.207-236). Berlijn/Heidelberg: Springer.

Fisher, H.D. (2009). *The German Legal System and Legal Language*. London/New York: Routledge-Cavendish.

Gestel, B. van, Poot, C. J. de, Bokhorst, R. J., & Kouwenberg, R. F. (2009). *Signalen van terrorisme en de opsporingspraktijk: De Wet opsporing terroristische misdrijven twee jaar in werking.* Den Haag: WODC. Cahier 2009-10.

Gestel, B. van, Poot, C.J, de, & Kouwenberg, R.F. (2010). De wet opsporing terroristische misdrijven drie jaar in werking. Den Haag: WODC, memorandum 2010-3.

Grafe, A. (2008). *Die Auskunftserteilung über Verkehrsdaten nach §§ 100g, 100h StPO; Staatliche Kontrolle unter Mintwirkung Privater*. Freiburg: Albert-Ludwigs-Universität.

Hartog, A. den (2001). De getuige in het strafprocesrecht: voorstellen voor een nieuwe regeling. In: M.S. Groenhuijsen & G. Knigge (red.), *Het Onderzoek ter Zitting, onderzoeksproject Strafvordering 2001; 1e interimrapport* (pp. 275- 342). Den Haag: WODC.

Holdsworth, M. (2006). *Introduction to the English Legal System*. Oxford: Oxford University Press.

Hopkins, A. (2009a). An Introduction to Covert Policing. In: M. Colvin & J. Cooper (red.), *Human rights in the Investigation and Prosecution of crime* (pp. 23-34). Oxford: Oxford University Press.

Hopkins, A. (2009b). The Interception of Communications: The Regulation of Investigatory Powers Act 2000 Pt I. In: M. Colvin & J. Cooper (red.), *Human rights in the Investigation and Prosecution of crime* (pp. 51-86). Oxford: Oxford University Press.

Interception of Communications Commissioner (2007). *Report of the Interception of Communications Commissioner for 2005-2006*, HC 315 SG/2007/17. Londen: The Stationary Office.

Interception of Communications Commissioner (2008a). *Report of the Interception of Communications Commissioner for 2007*, HC 947 SG/2008/127. Londen: The Stationary Office.

Interception of Communications Commissioner (2008b). *Report of the Interception of Communications Commissioner for 2006*, HC 252 SG/2008/9. Londen: The Stationary Office.

Interception of Communications Commissioner (2009). *Report of the Interception of Communications Commissioner for 2008*, HC 901 SG/2009/138. Londen: The Stationary Office.

Interception of Communications Commissioner (2010). *Report of the Interception of Communications Commissioner for 2009*, HC 901 SG/2010/138. Londen: The Stationary Office.

Interception of Communications Commissioner (2011). *2010 Annual Report of the Interception of Communications Commissioner*, HC 1239 SG/2011/117. Londen: The Stationary Office.

ITU (International Telecommunication Union). World telecommunication/ICT indicators database. 15Th edition 2011.

Jehle, J.-M. (2006). The Function of Public Prosecution within the Criminal Justice System Aim, Approach and Outcome of a European Comparative Study. In: J.-M. Jehle & M. Wade (red.), *Coping with Overloaded Criminal Justice Systems: The Rise of Prosecutorial Power Across Europe* (pp. 3-26). Berlijn/Heidelberg: Springer.

Jurgens, G.T.J.M., & Ommeren, F.J. van (2009). *De opmars van het onderscheid tussen publiekrecht en privaatrecht in het Engelse recht: Vanuit rechtsvergelijkend perspectief*. Den Haag: Boom Juridische Uitgevers.

Juy-Birmann, R. supervised by H. Jung, revised by J. Biermann (2002). The German system. In: M. Delmas-Marty & J.R. Spencer (red.), *European Criminal Procedures* (pp. 292-347). Cambridge: Cambridge University Press.

Kamerstukken II (1995-1996). Vergaderjaar 1995-1996, 24 072, nrs. 10-11.
Kamerstukken II (1996-1997). Vergaderjaar 1996-1997, 25 403, nr. 3.
Kamerstukken II (2009-2010). Vergaderjaar 2009-2010, 30 517, nr. 16.
Kamerstukken II (2009-2010). Vergaderjaar 2009-2010, 32 185, nr. 2.

Keizer, M., & en Kouwenberg, R.F. (1996). Telefoontap blijft populaire methode: Nut blijkt vooral in combinatie met andere middelen. *Algemeen Politieblad*, 145(21), 10-12.

Kleemans, E.R., Brienen, M.E.I., Bunt, H.G. van de, Kouwenberg, R.F., Paulides, G., & Barensen, J. (2002). *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor.* Den Haag: WODC / Boom Juridische Uitgevers. Onderzoek en beleid 198.

Koops, B.J. (2002). *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002: Het grensvlak tussen opsporing en privacy*. Deventer: Kluwer.

Koops, B.-J., Bekkers, R., Bongers, F., & Fijnvandraat, M. (2005). *Aftapbaarheid van telecommunicatie: Een evaluatie van hoofdstuk 13 Telecommunicatiewet*. Tilburg: TILT - Centrum voor Recht, Technologie en Samenleving.

Krabbe, H.G.M. (2004). Artikel 8: De eerbiediging van het privé-leven. In: A.E. Hartelveld, J. Hielkema, B.F. Keulen & H.G.M. Krabbe (red.), *Het EVRM en het Nederlandse strafprocesrecht* (pp. 137-183). Deventer: Kluwer.

Krey, V. (2009a). *German Criminal Procedure Law, Volume 1: Basics, Prosecution Authorities, Glossary*. Stuttgart: Kohlhammer.

Krey, V. (2009b). *The Public Prosecution's Role in Criminal Proceedings under the Rule of Law: Legal Situation in Germany with Comparative Law Remarks on UK and USA*. Trier: Institut für Rechtspolitik an der Universität Trier, p. 1-23.

Krommendijk, M., Terpstra, J., & Kempen, P. H. van (2009). *De Wet BOB: Titels IVa en V in de praktijk: Besluitvorming over bijzondere opsporingsbevoegdheden in de aanpak van georganiseerde criminaliteit.* Den Haag: Boom Juridische Uitgevers.

Kruisbergen, E. W., Jong, D. de, & (m.m.v.) Kouwenberg, R. F. (2010). *Opsporen onder dekmantel.* Den Haag: Boom Juridische uitgevers. Onderzoek en Beleid 282.

Kruyer, F. (2010). Heterdaad is resultaat. *Blauw*, 6(2), pp. 8-11.

Lewis, C. (2006). The Prosecution Service Function within the English Criminal Justice System. In: J-M. Jehle & M. Wade (red.), *Coping with Overloaded criminal Justice systems: The Rise of Prosecutorial Power Across Europe* (pp. 151-184). Berlijn: Springer.

Lindblom, P.H. (2000). Civil and Criminal Procedure. In: M. Bogdan (red.), *Swedish law in the new millennium* (pp. 201-242). Stockholm: Norstedt Juridik.

Oerlemans, J.J. (2011). Hacken als opsporingsbevoegdheid. *Delikt en Delinkwent*, 8(62), 888-908.

Office of Surveillance Commissioners (2007). *Annual Report of the Chief Surveillance Commissioner to the Prime minister and to Scottish Ministers for 2006-2007*, HC 713 SE/2007/126. Londen: The Stationery Office.

Office of Surveillance Commissioners (2008). *Annual Report of the Chief Surveillance Commissioner to the Prime minister and to Scottish Ministers for 2007-2008*, HC 659 SG/2008/86. Londen: The Stationery Office.

Office of Surveillance Commissioners (2009). *Annual Report of the Chief Surveillance Commissioner to the Prime minister and to Scottish Ministers for 2008-2009*, HC 704 SG/2009/94. Londen: The Stationery Office.

Office of Surveillance Commissioners (2010). *Annual Report of the Chief Surveillance Commissioner to the Prime minister and to Scottish Ministers for 2009-2010*, HC 168 SG/2010/66. Londen: The Stationery Office.

Office of Surveillance Commissioners (2011). *Annual Report of the Chief Surveillance Commissioner to the Prime minister and to Scottish Ministers for 2010-2011*, HC 1111 SG/2011/99. Londen: The Stationery Office.

OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) (2009). *Markt Monitor 2009*. Den Haag: OPTA.

OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) (2011). *Presentatie Markt Monitor 2010*. Den Haag: OPTA.

OM (Openbaar Ministerie) (2011). *Instructie geïntercepteerde gesprekken met geheimhouders (2011I002).* Den Haag: OM.

Pol, W. van de (2006). *Onder de tap: Afluisteren in Nederland*. Amsterdam: Uitgeverij Balans.

Poot, C. J. de, Bokhorst, R. J., Koppen, P. J. van, & Muller, E. R. (2004). *Rechercheportret: Over dillemma's in de opsporing.* Alphen aan den Rijn: Kluwer.

Poot, C. J. de, Bokhorst, R. J., Smeenk, W. H., & Kouwenberg, R. F. (2008). *De opsporing verruimd? De Wet opsporing terroristische misdrijven een jaar in werking.* Den Haag: WODC. Cahier 2008-9.

Privy Council Review of Intercept as Evidence (2008). *Report to the Prime Minister and the Home Secretary 30 January 2008*. Londen: The Stationary Office.

Reijne, Z., Kouwenberg, R. F., & Keizer, M. P. (1996). *Tappen in Nederland.* Arnhem: Gouda Quint.

Regeringens Skrivelse (*schrijven van de regering*), Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid fö rundersökning i brottmål under år 2009 (*Het geheim aftappen van telecommunicatie en geheime camerabewaking bij vooronderzoeken in strafzaken in het jaar 2009*) Stockholm, 16 december 2010/11:66.

Schacter, D.L. (2001). *The Seven Sins of Memory: How the mind forgets and remembers.* Boston: Houghton Mifflin.

Smits, A.H.H. (2006). *Strafvorderlijk onderzoek van telecommunicatie*. Nijmegen: Wolf Legal Publishers.

Spapens, A.C.M. (2008). *Georganiseerde misdaad en strafrechtelijke samenwerking in de Nederlandse grensgebieden.* Antwerpen/Oxford: Intersentia.

Spencer, J.R. (2002). The English system. In: M. Delmas-Marty & J.R. Spencer (red.), *European Criminal Procedures* (pp. 142-217). Cambridge: Cambridge University Press.

Staatsblad (2011). Besluit van 17 januari 2011, houdende regels met betrekking tot het elektronisch proces-verbaal (Besluit elektronisch proces-verbaal). *Staatsblad*, nr. 15.

Staatscourant (2011). Aanwijzing opsporingsbevoegdheden. *Staatscourant*, 24 februari 2011, nr. 3240.

Strategische Beleidsgroep Intelligence (2008). Waakzaam tussen wijk en wereld, Nationaal Intelligence Model, sturen op en met informatie.

Stratix Consulting (2009). *Grenzen aan de aftapbaarheid?* Hilversum: Stratix.

Stelfox, P. (2009). *Criminal investigation: An introduction to principles and practice*. Uffculme: Willian Publishing.

Telefoontaps in Nederland; wordt Nederland een politiestaat?, www.rechtennieuws.nl, 14-09-10.

TNO (Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek) (2010). *Marktrapportage Elektronische Communicatie.* Delft: TNO.

TNO (Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek) (2011). *Marktrapportage Elektronische Communicatie*. Delft: TNO.

Universiteit Utrecht (z.j.). *Geschiedenis van het Internet*. Geraadpleegd op 10 februari 2012: www.hum.uu.nl/ict-onderwijs/studenten/cursusmateriaal/index.php?content=ict_kennis/geschiedenis_internet

Verhoeven, M.A., Gestel, B. van, & Jong, D. de (2011). *Mensenhandel in de Amsterdamse raamprostitutie: Een onderzoek naar aard en opsporing van mensenhandel*. Den Haag: WODC. Onderzoek en beleid, 295.

Winkelhorst, R. C. (2006). *Elektronische communicatie en privacy.* Zutphen: Uitgeverij Paris.

Wörner, L. (2004). *The Effectiveness of Wiretapping and Electronic Surveillance to Fight against Terrorism: A comparative analysis between the United States and Germany, part 1: Overview of the current problem and law.* Baden-Baden: Nomos Verlagsgesellschaft.

www.coe.int, geraadpleegd d.d. 5 oktober 2011.

www.rijksoverheid.nl/documenten-en-publicaties/wob-verzoeken, geraadpleegd d.d. 5 oktober 2011.

Zila, J. (2006). The Prosecution Service Function within the Swedish Criminal justice System. In: J.-M. Jehle & M. Wade (red.), *Coping with Overloaded Criminal Justice Systems: The Rise of Prosecutorial Power Across Europe* (pp. 285-311). Berlijn/Heidelberg: Springer.

Jurisprudentie

Europese Hof voor de Rechten van de Mens (EHRM)
EHRM, 6 september 1978, Klass tegen Duitsland
EHRM, 26 april 1979, Sunday Times tegen het Verenigd Koninkrijk
EHRM, 2 augustus 1984, Malone tegen het Verenigd Koninkrijk
EHRM, 30 maart 1989, Chappell tegen het Verenigd Koninkrijk
EHRM, 24 april 1990, Kruslin tegen Frankrijk
EHRM, 15 juni 1992, Lüdi tegen Zwitserland
EHRM, 25 juni 1997, Halford tegen het Verenigd Koninkrijk
EHRM, 25 maart 1998, Kopp tegen Zwitserland
EHRM, 30 juli 1998, Valenzuela Contreras tegen Spanje
EHRM, 12 mei 2000, Khan tegen het Verenigd Koninkrijk
EHRM, 25 september 2001, P.G. en J.H. tegen het Verenigd Koninkrijk
EHRM, 16 juli 2002, Armstrong tegen het Verenigd Koninkrijk
EHRM, 5 november 2002, Allan tegen het Verenigd Koninkrijk
EHRM, 1 juli 2008, Liberty tegen het Verenigd Koninkrijk
EHRM, 18 mei 2010, Kennedy tegen het Verenigd Koninkrijk

Hoge Raad
Hoge Raad, 11 oktober 2005, *LJN* AT4351
Hoge Raad, 21 november 2006, *LJN* AY9673
Hoge Raad, 30 maart 2010, *LJN* BL2828

Gerechtshof
Gerechtshof Amsterdam, 24 juni 2004, *LJN* AP9856
Gerechtshof Arnhem, 24 januari 2012, *LJN* BV3076

Rechtbank
Rechtbank 's-Gravenhage, 30 december 2003, *NJ* 2004, 276
Rechtbank Amsterdam, 20 december 2007, *LJN* BC0685
Rechtbank 's-Gravenhage, 3 september 2008, *LJN* BE9675
Rechtbank Amsterdam, 8 maart 2011, *LJN* BP7233
Rechtbank Amsterdam, 31 mei 2011, *LJN* BQ9049

Bijlage 1 Samenstelling begeleidingscommissie

Voorzitter	Prof. Mr. M.J. Borgers; Hoogleraar straf(proces)recht bij de faculteit Rechtsgeleerdheid, Vrije Universiteit Amsterdam
Leden	Een afgevaardigde van het Landelijk Parket, Openbaar Ministerie Een afgevaardigde van de Politie Een afgevaardigde van de Universiteit van Tilburg Een afgevaardigde van het ministerie van Veiligheid en Justitie/PIDS Een afgevaardigde van het ministerie van Veiligheid en Justitie/DRC Een afgevaardigde van het ministerie van Veiligheid en Justitie/DRC

Bijlage 2 Notificatiebrieven

Notificatiebrief uit regio A

Briefhoofd Arrondissementsparket regio A
Adres

Telefoonnummer …

Naam en adres geadresseerde …

Datum:
Ons kenmerk:
Onderwerp: mededeling gebruik bijzondere opsporingsbevoegdheden

Geachte heer/mevrouw,

Enige tijd geleden is onder leiding van een officier van justitie te … een opsporingsonderzoek verricht. Dit onderzoek is inmiddels beëindigd. Bij dat onderzoek is gebruik gemaakt van opsporingsbevoegdheden waardoor inbreuk gemaakt kan zijn op uw persoonlijke levenssfeer. Art. 126bb van het Wetboek van Strafvordering schrijft voor dat u van dit gebruik op de hoogte wordt gesteld.

In het onderzoek zijn op bevel van de officier van justitie en met toestemming van de rechter-commissaris door de politie telefoongesprekken opgenomen en afgeluisterd die zijn gevoerd via het telefoonnummer …. In de periode van …

Dit bevel is gebaseerd op artikel 126m/126t van het wetboek van Strafvordering.

Door het verschaffen van deze informatie heb ik voldaan aan de verplichting, op grond van artikel 126bb van het Wetboek van Strafvordering, u te informeren.

De wet verplicht mij niet tot mededeling van meer informatie. Met name heeft u geen recht op informatie over de resultaten van het gebruik van de toegepaste bevoegdheid. Vanwege het vertrouwelijke karakter van die resultaten zullen dergelijke mededelingen daarom niet worden gedaan, noch aan u zelf, noch aan anderen.

Hoogachtend,

De Officier van Justitie

Notificatiebrief uit regio B

Briefhoofd Arrondissementsparket te regio B

Naam en adres geadresseerde

Onderdeel	…
Contactpersoon	…
Doorkiesnummer(s)	…
Datum	…
Ons kenmerk	‹‹parketnummer››
Onderwerp	Notificatie i.v.m. aftappen van telefoonverkeer

Geachte heer, mevrouw,

Onlangs is onder mijn leiding een strafrechtelijk onderzoek uitgevoerd.

Daarbij is/zijn na te noemen opsporingsbevoegdhe(i)d(en) toegepast die een inbreuk gemaakt kunnen hebben op uw privacy, omdat deze bevoegdhe(i)d(en) (mede) tegen u is/zijn uitgeoefend.

Op grond van artikel 126bb van het Wetboek van Strafvordering deel ik u hierbij mede, dat in de periode van ‹‹datum_aanvang›› tot ‹‹datum_einde››, de gesprekken die gevoerd zijn met een of meer telefoonnummer(s) dat/die bij u in gebruik is/zijn, ingevolge artikel 126m/126t Wetboek van Strafvordering, zijn afgeluisterd en opgenomen:

Nadere informatie wordt niet verstrekt.

Hoogachtend,

De Officier van Justitie

<Achterflaptekst>
Under construction