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 gebruikgemaakt 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 onder meer 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 opsporings-

bevoegdheden 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 veertien deskundigen en drie 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 Consulting, 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 artikel 8 lid 2 EVRM moet bij het gebruik van de telefoon- en innternettap onder meer 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 Wetboek van Strafvordering) 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 Wetboek van Strafvordering (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 ingrijpend 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 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, enz.) langs een filter geleid. Als een telefoonnummer door het systeem wordt herkend, 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 nummerherkenningsysteem 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 gebonden. 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 zogenoemd '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 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) onderschept dat over een bepaalde internetlijn loopt.

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 en het gebruikte protocol.

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 voldaan is 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 Cen-

traal 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 Wet op de inlichtingen- en veiligheidsdiensten (Wiv) en artikel 10.10 Telecommunicatiewet (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, International Mobile Equipment Identity (IMEI)-nummer, IP- of e-mailadres 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 is voor het eerst het aantal internettaps bekendgemaakt (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 prepaid 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 gebruikgemaakt 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 kunnen ze 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 het deze betrokkene wil 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 betrokkene dan wanneer het een tap op een verdachte betreft. Toch kan een tap op een betrokkene 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 uitmaakt, aldus een respondent.

Geheimhouders

Informatie uit gesprekken met personen die vallen onder het verschoningsrecht mogen niet in het opsporingsproces terechtkomen. 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.

1 Instructie vernietiging geïntercepteerde gesprekken met geheimhouders.

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 twintig 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. 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 wordt, 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

2 De Aanwijzing opsporingsbevoegdheden (2011A002), 14 februari 2011, *Staatscourant* 2011, 3240.

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, vindt 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 deze 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 deze zich een aantal jaar geleden heeft 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 'nuldossier' 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 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 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 inspelen. 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 zo veel mogelijk te ver-

mijden. Deze slechte ervaringen met de internettap heeft deze groep respondenten negatief beïnvloed 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 analysetechnieken 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 getapte 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 ervan 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 mee 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 Justitie geadviseerd 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, persoonlijke 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 (EVRM) 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 Europese Hof voor de Rechten van de Mens (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 van 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 vier weken, in Zweden een termijn van een

maand. In Engeland en Wales geldt een termijn van drie maanden. In Duitsland geldt eveneens een termijn van drie 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 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 integriteitsbelangen 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 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 gebruik 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 verkeersgegevens (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 verkeersgegevens 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 prijsgeven 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 erop 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.