Stratix

NORTON ROSE

Inventarisatie regelgeving aftappen in het buitenland

Rapport
uitgebracht aan:

Ministerie van
Economische Zaken
DGTP
Afdeling Veiligheid

Uitgebracht door:
Stratix Consulting B.V.
en Norton Rose

Schiphol, maart 2004

Voorwoord

Stratix heeft, in samenwerking met het internationale advocatenkantoor Norton Rose, onderzocht hoe aftappen wettelijk geregeld is in de landen Duitsland, Frankrijk, Oostenrijk en het Verenigd Koninkrijk, en hoe deze regelingen geïmplementeerd zijn. Stratix heeft daarbij de verschillende uitgangspunten en regelingen in de genoemde landen vergeleken met de Nederlandse situatie, om te komen tot een overzicht van de overeenkomsten en verschillen

In overeenstemming met onze opdracht, is een verkenning van thans geldende en publiek beschikbare wetsteksten en regelingen uitgevoerd welke is aangevuld met informatie uit interviews van betrokken overheidsinstanties. Dit tezamen heeft geleid tot een beschrijving van de situatie per land en van de overeenkomsten en verschillen met de Nederlandse situatie. De gedetailleerde analyse van de wet- en regelgeving is opgenomen in bijlage 5. Dit rapport is bedoeld een overzicht te geven van geldende regelgeving en de praktische interpretaties daarvan. Het kan evenwel niet gezien worden als specifiek juridisch advies over de behandelde onderwerpen.

Het onderzoek is uitgevoerd in opdracht van en ten behoeve van het Ministerie van Economische Zaken, Directoraat-Generaal Telecommunicatie en Post (DGTP), en is uitsluitend aan het Ministerie gericht. Het maakt deel uit van een evaluatie van de situatie rond aftappen in Nederland door DGTP. Zonder onze voorafgaande schriftelijke toestemming mogen geen andere (rechts)personen rechten ontlenen aan de inhoud van dit rapport.

De onderzoekers danken de overheden in de onderzochte landen voor hun medewerking aan dit onderzoek.

Inhoudsopgave

Samenvatting

Dit rapport beschouwt het aftappen van de inhoud van elektronische communicatie en het verzamelen van gegevens over gebruikers en verkeer.

Het Directoraat Generaal Telecom en Post (DGTP) evalueert het aftapregime in Nederland. Onderdeel van de evaluatie is deze vergelijking van het Nederlandse regime met dat in naburige Europese landen. Dit onderzoek vergelijkt regelgeving en praktijk in Nederland met Duitsland, Frankrijk, Oostenrijk en het Verenigd Koninkrijk. De informatie is verzameld uit wetteksten en interviews met betrokken overheidsinstanties in elk van de landen.

Wettig aftappen is in elk van de beschouwde landen in de wet geregeld als uitzondering op het communicatiegeheim. Alleen in het Verenigd Koninkrijk is afgetapte informatie niet ontvankelijk als bewijs.

Voor aanbieders van telecommunicatie gelden over het algemeen drie soorten verplichting:

- verlenen van medewerking bij aftappen;
- treffen van voorzieningen voor aftappen;
- leveren van gegevens over gebruikers en verkeer.

Over het algemeen gelden de verplichtingen voor alle aanbieders van *openbare* telecommunicatie. In Duitsland en Frankrijk gelden de verplichtingen ook voor een aantal aanbieders van *private* telecommunicatie. Vrijgesteld van het treffen van voorzieningen zijn over het algemeen aanbieders met een klein aantal gebruikers en, in Duitsland en Oostenrijk, aanbieders van transitnetwerken en internet toegangsdiensten. In het Verenigd Koninkrijk treffen aanbieders pas voorzieningen indien zij daartoe worden aangewezen.

Aanbieders moeten gegevens over gebruikers en verkeer, indien aanwezig, beschikbaar stellen. Deze gegevens mogen in het algemeen slechts bewaard worden indien noodzakelijk voor de bedrijfsvoering. In Frankrijk bewaren aanbieders bovendien identiteitsgegevens van houders van pre-paid diensten, en van aanbieders van content op het internet. Het Verenigd Koninkrijk experimenteert met vrijwillige opslag van gegevens voor de bestrijding van terrorisme en criminaliteit.

De kosten voor aftappen worden in zeer uiteenlopende mate vergoed. Nederland, Duitsland en Oostenrijk vergoeden alleen operationele kosten bij het uitvoeren van een tapbevel. De investeringen in voorzieningen en onderhoud komen voor rekening van de aanbieder. Het Verenigd Koninkrijk en Frankrijk kennen gehele of gedeeltelijke vergoedingen voor alle kosten. Veel overheden zoeken naar vereenvoudiging van de mechanismen en tarieven voor vergoeding.

1 Inleiding

Achtergrond

Het aftappen van elektronische communicatie is een van de hulpmiddelen die een moderne rechtstaat ter beschikking staan voor de opsporing en preventie van criminaliteit. Naarmate burgers (en in het bijzonder criminelen) meer gebruik maken van elektronische communicatiediensten, ontwikkelt aftappen zich tot een belangrijk hulpmiddel voor opsporings- en veiligheidsdiensten. Naast het eigenlijke aftappen van de *inhoud* van communicatie kunnen ook *gebruikersgegevens* en *verkeersgegevens* omtrent de communicatie van belang zijn. Dit rapport bespreekt zowel het eigenlijke aftappen als het bewaren en opvragen van deze gegevens.

Hoofdvraag

Het doel van dit rapport is inzicht te geven in de situatie in vier Europese landen buiten Nederland ten aanzien van het aftappen en ten aanzien van het opvragen van gegevens omtrent communicatie. Dit overzicht verschaft een basis voor vergelijking ten behoeve van de evaluatie van het Nederlandse aftapregime door DGTP.

Werkwijze

Het onderzoek is uitgevoerd aan de hand van de onderzoeksvragen zoals opgesteld door DGTP en de onderzoekers. Op basis van literatuuronderzoek zijn de relevante wettelijke regelingen van ieder land verzameld. Daarmee zijn de onderzoeksvragen (zie Bijlage 2: Vragenlijst) vanuit het formele wettelijke perspectief beantwoord. Deze inventarisatie is verricht door plaatselijke juristen met expertise in telecommunicatie-regelgeving. Vervolgens is in ieder land een interview afgenomen met een of meer vertegenwoordigers van de verantwoordelijke overheidsinstantie om een beeld te verkrijgen van de praktische uitwerking van de wettelijke regelingen.

Uitgangspunten

Het onderzoek inventariseert in een momentopname de wet- en regelgeving en de praktische implementatie daarvan in de verschillende landen. Daarnaast worden enkele wetswijzigingen genoemd die in deze landen in behandeling zijn. Het onderzoek doet geen aanbevelingen voor het Nederlandse beleid op het gebied van aftappen.

Structuur van dit rapport

Het rapport biedt verschillende ingangen tot de verzamelde informatie. Hoofdstuk 2 geeft een overzicht van de situatie per land. Hoofdstuk 3 beschrijft de voornaamste overeenkomsten en verschillen met de Nederlandse situatie. Bijlage 3 bevat een tabel met dezelfde informatie in telegramstijl als totaaloverzicht. Een uitgebreide juridische uiteenzetting per land, gestructureerd op basis van de vooraf gedefinieerde vragenlijst, is opgenomen in bijlage 5. Eveneens opgenomen zijn een verklarende woordenlijst, de gehanteerde vragenlijst en een overzicht van de geïnterviewde partijen, in bijlagen 1,2 en 4 respectievelijk.

2 Situatie per land

Dit hoofdstuk schetst de wettelijke regels en de praktijk van het aftappen en van het opvragen van gegevens in elk van de onderzochte landen. Om een vergelijking met Nederland mogelijk te maken wordt de Nederlandse situatie op dezelfde manier beschreven.

Verplichtingen rond aftappen vallen in twee categorieën:
- Een verplichting om op verzoek *mee te werken* aan het aftappen
- Een verplichting om *voorzieningen te treffen* om het aftappen mogelijk te maken

Aangezien deze twee verplichtingen op verschillende groepen van toepassing kunnen zijn, behandelt dit rapport ze afzonderlijk.

Naast de verplichtingen rond aftappen zijn er verplichtingen om gebruikersgegevens en verkeersgegevens beschikbaar te maken. Gebruikersgegevens beschrijven de gebruiker van een telecommunicatiedienst: bijvoorbeeld naam, adres, woonplaats, nummer en afgenomen dienst. Verkeersgegevens zijn gegevens over het gebruik van telecommunicatiediensten[1]: bijvoorbeeld routering, duur, tijdstip of grootte van een communicatie, het gebruikte protocol, en de locatie van de eindapparatuur van verzender of ontvanger.

Veel landen kennen naast specifieke regels voor telecommunicatie ook een algemene bevoegdheid voor de autoriteiten om (elektronische) documenten voor justitieel onderzoek[2] te vorderen. Hoewel een dergelijke bevoegdheid in voorkomende gevallen gebruikt kan worden voor het vorderen van gebruikersgegevens of verkeersgegevens blijft deze algemene bevoegdheid buiten dit onderzoek.

2.1 Nederland

2.1.1 Wet- en regelgeving voor aftappen

De belangrijkste wet- en regelgeving van Nederland inzake aftappen is vastgelegd in:
- Wetboek van strafvordering
- Wet op inlichtingen- en veiligheidsdiensten 2002
- Telecommunicatiewet
- Besluiten en Regelingen

De Nederlandse grondwet bepaalt dat telecommunicatie in beginsel geheim is. Uitzonderingen hierop kunnen alleen bij wet worden vastgesteld. Een dergelijke

[1] In de Europese Richtlijn 2002/58/EG worden verkeersgegevens gedefinieerd als “gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-communicatienetwerk of voor de facturering ervan”.

[2] Voor Nederland is dit bijvoorbeeld vastgelegd in het Wetboek van Strafvordering, artikel 125i.

uitzondering ten behoeve van het aftappen van openbare telecommunicatie is beschreven in het Wetboek van Strafvordering en in de Wet op de Inlichtingen- en Veiligheidsdiensten van 2002. De Telecommunicatiewet bevat de specifieke verplichtingen die in dit kader gelden voor aanbieders van telecommunicatienetwerken en -diensten; deze verplichtingen zijn in diverse wetten, besluiten en regelingen verder uitgewerkt.

De nieuwe Telecommunicatiewet ligt, ten tijde van dit onderzoek, voor aan de Eerste Kamer. Deze conceptwet is aangepast aan onder andere de nieuwe privacy-richtlijn van de Europese Unie. Ten aanzien van aftappen en het bewaren van gebruikers- en verkeersgegevens bevat de nieuwe wet nauwelijks wijzigingen.

2.1.2 Aanbieders en diensten

Verplichting tot medewerking

De verplichting om aan het aftappen mee te werken geldt in Nederland uitsluitend voor aanbieders van openbare telecommunicatienetwerken en -diensten.

Verplichting tot het treffen van voorzieningen

De verplichting tot het treffen van voorzieningen geldt in Nederland voor alle aanbieders van openbare telecommunicatienetwerken en -diensten. Een aanbieder mag openbare telecommunicatiediensten slechts aanbieden indien aftapvoorzieningen voldoen aan de gestelde eisen en goedgekeurd zijn door de bevoegde autoriteiten.

De specificatie van de benodigde voorzieningen voor het aftappen van nieuwe diensten wordt in de praktijk in overleg tussen de industrie en de overheid opgesteld. Aanbieders krijgen daarbij enige tijd om de voorzieningen te implementeren.

2.1.3 Bewaren en leveren van gebruikersgegevens

Er bestaat momenteel geen verplichting tot het bewaren van gebruikersgegevens. Wanneer het Besluit Verstrekking Gegevens Telecommunicatie in werking treedt, zal het voorschrijven dat de aanbieders van elke gebruiker de naam, adres, woonplaats, en nummer aan een centraal bestand[3] aanleveren. Dit geldt echter uitsluitend voor gegevens die uit hoofde van de bedrijfsvoering ingewonnen worden; voor diensten waarvoor deze gegevens niet voor de bedrijfsvoering nodig zijn, zoals gratis of pre-paid diensten, hoeven de aanbieders geen gebruikersgegevens in te winnen en op te slaan.

De telefonieaanbieders in Nederland leveren op het moment van schrijven in het kader van een proef reeds gegevens aan voor het genoemde centrale bestand.

[3] CIOT, het Centraal Informatiepunt Onderzoek Telecommunicatie

Voor diensten waarbij de aanbieder niet over gebruikersgegevens beschikt, zoals gratis en pre-paid diensten, is de aanbieder verplicht op aanvraag het gebruikte nummer te achterhalen, bijvoorbeeld door een analyse van verkeersgegevens. De aanbieders kunnen verplicht worden om de hiertoe benodigde gegevens op te slaan; in de huidige situatie geldt dit alleen voor verkeersgegevens voor pre-paid mobiele diensten.

2.1.4 Bewaren en leveren van verkeersgegevens

Er bestaat in Nederland in het algemeen geen verplichting om verkeersgegevens vast te leggen. Aanbieders van telecommunicatienetwerken en -diensten zijn wel verplicht verkeersgegevens die ten behoeve van de normale bedrijfsvoering zijn vastgelegd op verzoek te overleggen. In de praktijk zijn in veel gevallen verkeersgegevens beschikbaar aangezien aanbieders deze bewaren voor de eigen bedrijfsvoering[4].

Voor pre-paid mobiele diensten, waarbij gebruikersgegevens niet beschikbaar zijn, is de aanbieder verplicht de verkeersgegevens te bewaren die nodig zijn om het nummer van een gebruiker te achterhalen. Voor dergelijke diensten bewaart de aanbieder van elke communicatie het A- en B-nummer, het base station en het tijdstip; deze gegevens dient de aanbieder 3 maanden te bewaren om uit twee observaties te kunnen achterhalen welk nummer door een bepaalde persoon gebruikt wordt.

2.1.5 Ontheffing van verplichtingen

De wetgeving stelt dat vrijstelling van verplichtingen in ‘bijzondere gevallen’ mogelijk is. Een dergelijke vrijstelling wordt per geval vastgesteld.

2.1.6 Geschilbeslechting

Eventuele geschillen worden administratief afgehandeld. Bij algemene maatregel van bestuur kunnen regels worden gesteld met betrekking tot het beslechten van geschillen tussen aanbieders en bevoegde autoriteiten. Een dergelijke regeling is tot op heden niet getroffen.

2.1.7 Regels ten aanzien van uitvoering

Aanbieders dienen de aftapvoorzieningen volgens voorgeschreven richtlijnen te treffen en in stand te houden. Aanbieders moeten een kopie van de inhoud plus informatie over afgetapt verkeer leveren. Eventuele netwerkgebaseerde encryptie dient verwijderd te worden. Een last tot aftappen moeten aanbieders ‘onverwijld’ uitvoeren; er zijn voor telefonie regels gesteld met betrekking tot het aantal abonnees dat gelijktijdig moet kunnen worden afgetapt.

De aanbieder dient de resultaten van het aftappen op meerdere fysieke locaties tegelijk te kunnen afleveren. Daarbij moet de aanbieder de data versleutelen wanneer meeluisteren door derden dreigt.

---

[4] Zie het rapport “*Bewaren van verkeersgegevens door telecommunicatie-aanbieders*” van het Ministerie van Justitie (www.justitie.nl/Images/11_41971.pdf)

De officier van justitie geeft opdracht tot aftappen. Aantallen taplasten en nummers worden niet centraal geregistreerd; de laatst bekende cijfers betreffen het jaar 1998, waarin ongeveer 10.000 nummers werden afgetapt[5].

2.1.8 Kosten en vergoedingen

De Nederlandse regeling biedt uitsluitend vergoedingen voor de kosten die direct voortvloeien uit het uitvoeren van een last. De aanbieders dragen de kosten voor aanleg en onderhoud van de noodzakelijke voorzieningen.

Deze regeling en de hoogte van de bijbehorende vergoedingen zijn in Nederland geregeld onderwerp van discussie.

2.2 Duitsland

2.2.1 Wet- en regelgeving voor aftappen

De belangrijkste wet- en regelgeving van Duitsland inzake aftappen is vastgelegd in:
- StrafProzessOrdnung (StPO)
- Außenwirtschaftsgesetz (AWG) en Art 10G
- TeleKommunikationsGesetz 1996 (TKG)
- TeleKommunikations-ÜberwachungsVerordnung (TKÜV)

De grondwet definieert het briefgeheim, dat ook voor telecommunicatie geldt. De StPO, AWG en Art 10G beschrijven een uitzondering op het briefgeheim: zij bieden de wettelijke gronden waarop aftappen is geregeld. De TKG, uit 1996, geeft het raamwerk van verplichtingen voor aftappen. Er bestaat een conceptversie van de nieuwe TKG die de nieuwe Europese richtlijnen implementeert. De TKÜV geeft de invulling van de verplichtingen beschreven in de TKG, en de uitzonderingen daarop. Technische richtlijnen schrijven de feitelijke implementatie van de verplichtingen voor. De enige bestaande technische richtlijn is de TR TKÜ (Technische Richtlinie TeleKommunikationsÜberwachung), voor de implementatie van de aftapverplichting voor vaste en mobiele telefonie.

2.2.2 Aanbieders en diensten

Verplichting tot medewerking

De Duitse wetgeving verplicht aanbieders van openbare en private telecommunicatiediensten met een zakelijk karakter om aan het aftappen mee te werken. Hieronder vallen naast openbare telecommunicatienetwerken ook netwerken en diensten voor gesloten gebruikersgroepen, *corporate* netwerken zoals PABX netwerken en LAN's voor interne communicatie, mailbox-services en

[5] Zie Kamerstukken 27 591 nr 2, vraag 68.

transmissiediensten. Alleen privé-gebruik is vrijgesteld van de verplichting tot medewerking.

Verplichting tot het treffen van voorzieningen

In Duitsland geldt de verplichting tot het treffen van voorzieningen in beginsel voor elke aanbieder van een openbaar telecommunicatienetwerk waarop eindgebruikers zijn aangesloten. *Transit* operators, aanbieders van *carrier select* diensten of *peering* diensten vallen niet onder de verplichting, behalve wanneer zij *Intelligent Network* (IN) diensten aanbieden zoals *freephone* en UPT[6]. Dergelijke IN-diensten beschouwt men als virtuele eindgebruikeraansluitingen. Bovendien kan in bijzondere gevallen een parlementaire commissie toestaan dat de *Bundesnachrichtendienst* alle verkeer over een specifieke internationale connectie bewaakt.

De verplichting tot het treffen van voorzieningen geldt expliciet niet voor internet-toegangsdiensten van *Internet Service Providers* (ISP's) zoals bepaald in de TKÜV. De ISP heeft wel een verplichting om mailbox-diensten, waaronder e-mail (zowel inkomende als uitgaande e-mail), direct aftapbaar te maken. Verder moeten ISP's die internettoegang over een vaste verbinding leveren dit verkeer wel kunnen tappen.

Diensten als webhosting en message boards worden beschouwd als diensten die informatie publiekelijk beschikbaar maken. Dergelijke diensten hoeven daarom niet op dienstniveau afgetapt te worden. De informatie voor deze diensten is eventueel wel in de IP-stroom terug te vinden.

De verplichting om voorzieningen te treffen hoeft alleen uitgevoerd te worden indien hiervoor een technische richtlijn bestaat. Momenteel is alleen de richtlijn voor spraaktelefonie volledig geïmplementeerd. Een aantal richtlijnen voor andere diensten is recentelijk gedefinieerd. Aanbieders krijgen enige tijd voor de implementatie van de richtlijn.

Formeel gezien mag een aanbieder een netwerk alleen exploiteren wanneer RegTP heeft vastgesteld dat de voorzieningen toereikend zijn. In de praktijk past men deze regel soepel toe. Nieuwe aanbieders of bestaande aanbieders met nieuwe diensten kunnen starten en krijgen enige tijd om de eisen te implementeren.

In plaats van individuele goedkeuring voor elke aanbieder kan een fabrikant een systeem door RegTP laten certificeren. Elke aanbieder die gebruik maakt van dergelijke gecertificeerde apparatuur voldoet daarmee aan de gestelde eisen.

---

6 UPT: Universal Personal Telecommunication service; ook wel bekend als bereikbaarheidsdienst, levert een gebruiker de mogelijkheid om op één nummer voor verschillende soorten aansluiting bereikbaar te zijn.

De conceptversie van de nieuwe TKG bepaalt dat dienstaanbieders, die netwerkdiensten afnemen bij een derde partij, moeten verifiëren dat deze partij voldoet aan de verplichting en moeten de autoriteiten daar van op de hoogte stellen.

Wanneer een dienstaanbieder zowel private als openbare diensten aanbiedt geldt de verplichting tot het treffen van voorzieningen alleen voor het openbare deel van de dienstverlening. VPN-diensten, of anderszins gedeelde netwerken, gelden als privaat zolang de gebruikers behoren tot een en dezelfde entiteit of het netwerk voor een gezamenlijk commercieel doel gebruiken. Communicatie over de grenzen van een VPN geldt als een openbare dienst.

Vrijgesteld van de verplichting om voorzieningen te treffen zijn aanbieders van interne diensten aan een beperkte groep, die zonder winstoogmerk handelen. Denk hierbij aan ziekenhuizen, hotels en bedrijfsnetwerken, maar ook aan brancheverenigingen die diensten aan hun leden aanbieden. Eveneens vrijgesteld zijn aanbieders van netwerken met maximaal 1000 klanten, en netwerken ten behoeve van omroep, meetgegevens, noodsignalen of algemeen beschikbare informatie.

Aanbieders die diensten leveren, gebruikmakend van het netwerk van een derde partij, worden in de praktijk niet betrokken bij aftappen. Hoewel zij formeel ook medewerking moeten verlenen, zijn het de netwerkaanbieders die feitelijk meewerken aan aftappen. In de nieuwe TKG zal een dienstaanbieder moeten aantonen aan de toezichthouder, dat de netwerkaanbieder over wiens netwerk hij de diensten aanbiedt, aan alle wettelijke verplichtingen voldoet.

Er treden problemen op bij diensten die vanuit het buitenland worden aangeboden; alleen als de aanbieder in Duitsland een vertegenwoordiger heeft kunnen de verplichtingen daadwerkelijk worden afgedwongen.

2.2.3 Bewaren en leveren van gebruikersgegevens

Alle aanbieders van openbare telecommunicatienetwerken en -diensten moeten volgens de TKG gebruikersgegevens bewaren en aan een centraal bestand bij de toezichthouder RegTP aanleveren. Van de gebruikersgegevens die een aanbieder opslaat in het kader van de bedrijfsvoering, moet de aanbieder nummer, naam en adres doorgeven aan RegTP. Wijzigingen moeten steeds binnen 24 uur doorgeven worden. De gegevens dienen tot een jaar na beëindiging van het contract te worden bewaard.

Recent heeft een rechtbank geoordeeld dat deze wetgeving niet van toepassing is op pre-paid diensten, aangezien dit in tegenspraak is met de privacywetgeving. Die rechterlijke uitspraak stelt dat het aanbieders niet is toegestaan om gebruikersdata te verwerken tenzij dit nodig is voor het aanbieden van de dienst.

2.2.4 Bewaren en leveren van verkeersgegevens

Verkeersgegevens mogen uitsluitend worden bewaard indien noodzakelijk voor het leveren en factureren van de dienst. Voor zover zij niet dienen voor de facturering moeten zij na maximaal 1 dag worden gewist. Gegevens die wel voor facturering dienen, mogen maximaal 6 maanden worden bewaard, op voorwaarde dat ten minste 3 cijfers uit het B-numer zijn gewist.

Voor pre-paid en flat-rate diensten slaat een aanbieder in het algemeen geen verkeersgegevens op. Uitzondering hierop zijn verkeersgegevens voor fraudeonderzoek en gegevens die nodig zijn voor het afhandelen van verrekening tussen aanbieders in het geval van roaming.

De autoriteiten kunnen per bevel zowel opgeslagen historische verkeersgegevens als toekomstige verkeersgegevens vorderen.

2.2.5 Ontheffing van verplichtingen

Op basis van de regelgeving kunnen de Duitse autoriteiten (RegTP) gehele of gedeeltelijke dispensatie verlenen voor netwerkaanbieders met maximaal 10.000 abonnees. Dit geldt ook voor *field trials*, commerciële tests met maximaal 10.000 gebruikers en voor nieuwe diensten waarvoor nog geen richtlijn bestaat.

Hoewel netwerkaanbieders met maximaal 10.000 gebruikers ontheffing kunnen krijgen, blijken er in de praktijk, behalve startende ondernemingen, vrijwel geen aanbieders te zijn met minder dan 10.000 gebruikers. Een ontheffing wordt dan ook voornamelijk gegeven aan startende bedrijven of bedrijven die een nieuwe dienst introduceren.

2.2.6 Geschilbeslechting

In Duitsland bestaan er geen specifieke mechanismen voor disputen tussen autoriteiten en aanbieders inzake aftappen; de formele rechtsgang is via de administratieve rechtbanken.

In de meeste geschillen kan de toezichthouder, RegTP, bemiddelen tussen de aanbieders en de inlichtingendienst die de tap gelast. RegTP heeft daarbij de macht om aanbieders tot medewerking te dwingen, al dan niet op straffe van een boete. In de praktijk komt dit echter zelden voor.

Disputen betreffen over het algemeen capaciteitsissues of incorrecte implementatie van voorzieningen.

2.2.7 Regels ten aanzien van uitvoering

Aanbieders dienen de aftapvoorzieningen volgens voorgeschreven richtlijnen te treffen en in stand te houden.

Aanbieders moeten een kopie van de inhoud plus informatie over afgetapt verkeer leveren. Eventuele netwerkgebaseerde encryptie dient verwijderd te worden. Een last tot aftappen moeten aanbieders 'onverwijld' uitvoeren. Bij het leveren van aftapdata zegt de regelgeving expliciet dat de aanbieder geen andere telecommunicatiedata mee mag zenden dan die waarnaar in de last wordt gevraagd. De aanbieder dient de informatie op meerdere fysieke locaties tegelijk te kunnen afleveren.

De aanbieder moet er voor zorgen dat onderschepping niet mogelijk is; dit kan via encryptie maar andere oplossingen zijn ook toegestaan. Dit kan bijvoorbeeld door gebruik te maken van ISDN en een Closed User Group. Voor het transport van IP-verkeer (als inhoud of als informatie over het verkeer) wordt in het algemeen IPsec gebruikt.

Het tappen van IP-verkeer doet men in Duitsland in de praktijk vrijwel uitsluitend op het niveau van het netwerk of het toegangsnetwerk. Dit is een erfenis uit de tijd dat inbellen de enige beschikbare vorm van Internettoegang was, en IP-verkeer afgetapt kon worden door de telefoonaansluiting af te tappen. Nu tapt men ook op toegangsniveau en niet op IP-niveau voor DSL, kabel, GRPS en leased lines.

De Duitse overheid interpreteert het 'onverwijld' aanleveren van afgetapt verkeer in het algemeen als niet meer dan een uur. De rechtbank geeft echter aan hoe urgent een individuele last is. Buiten kantooruren wordt het acceptabel geacht dat een aanbieder maximaal zes uur tijd nodig heeft voor het ten uitvoer brengen van een tapopdracht.

Met betrekking tot het realiseren van nieuwe richtlijnen en standaarden hanteert men in Duitsland zoveel mogelijk een pragmatische aanpak. De uitvoeringsorganisaties van de overheid formuleren een interim-oplossing, en in samenspraak met de betrokken partijen komt men tot een definitieve oplossing. Hierbij maakt men zoveel mogelijk gebruik van internationale standaarden.

Opdrachten tot aftappen worden door de rechter gegeven. RegTP is toezichthouder en verantwoordelijk voor het keuren en monitoren van de werkelijke implementatie van aftapfaciliteiten door aanbieders. Tevens heeft RegTP de bevoegdheid om in samenspraak met belanghebbende partijen de technische implementatierichtlijnen op te stellen, en kan RegTP door de politiek geconsulteerd worden bij verandering in wet- en regelgeving.

2.2.8 Kosten en vergoedingen

De Duitse regeling biedt uitsluitend vergoedingen voor de directe kosten en de aanbieders dragen de kosten voor aanleg en onderhoud van de noodzakelijke voorzieningen. De Duitse regeling biedt voor de directe kosten een maximale vergoeding van 13 Euro per gewerkt uur.

Het feit dat in Duitsland alle investeringskosten voor de rekening van de aanbieder zijn, en dat de variabele kosten slechts met 13 Euro per uur worden vergoed, leidt tot veel discussie. Men voert deze discussie op politiek niveau omdat een verandering alleen mogelijk is door een wetswijziging.

2.3 Frankrijk

2.3.1 Wet- en regelgeving voor aftappen

De belangrijkste wet- en regelgeving van Frankrijk inzake aftappen is vastgelegd in:
- Loi sur le secret des correspondances (“Wet van 1991”)
- Code de procédure pénale
- Code des Postes et Télécommunications

Het aftappen is een uitzondering op het communicatiegeheim zoals vastgelegd in de ‘Loi relative à la liberté de communication’. Aftappen mag alleen door bepaalde publieke autoriteiten uitgevoerd worden in het publieke belang, en binnen de kaders van de ‘Loi relative à la liberté de communication’. Op basis van de *Code de procédure pénale* kan de rechter een besluit tot aftappen nemen.

De *Code des Postes et Télécommunications* schrijft de verplichtingen van de aanbieders voor. Deze verplichtingen zijn gekoppeld aan licenties. In het eerste kwartaal van 2004 treedt een nieuw decreet in werking waarin de verplichtingen van telecommunicatieaanbieders zijn vastgelegd. Dit decreet schrijft verplichtingen voor die gelden voor alle aanbieders, los van eventuele licenties.

2.3.2 Aanbieders en diensten

Verplichting tot medewerking

Elke aanbieder van openbare of private telecommunicatiediensten is verplicht aan aftappen mee te werken. Hieronder vallen ook de aanbieders van netwerken voor gesloten gebruikersgroepen en netwerken voor intern gebruik. Omroepdiensten vallen niet binnen de definitie van telecommunicatiediensten.

Verplichting tot het treffen van voorzieningen

De Franse autoriteiten specificeren in de licentie voor elke aanbieder van openbare telecommunicatiediensten de verplichting tot het treffen van voorzieningen. Deze verplichtingen zijn in de praktijk echter voor alle licentiehouders identiek.

De wetgeving geldt ook voor aanbieders van zogenaamde ‘onafhankelijke netwerken’. Dit zijn netwerken voor *closed user groups* die zich uitstrekken over grondgebied van meer dan een eigenaar. Ook aanbieders van *transit* diensten vallen onder de verplichtingen.

De wetgeving maakt een uitzondering voor omroepdiensten. De informatie van omroepdiensten beschouwt men als publiek toegankelijk; deze informatie hoeft dan ook niet aftapbaar te zijn.

In het eerste kwartaal van 2004 worden de verplichtingen tot het treffen van voorzieningen opgenomen in een decreet. Vanaf dat moment gelden dezelfde verplichtingen voor alle aanbieders van telecommunicatiediensten, inclusief ISP's. Aangezien ISP's geen licentieplichtige aanbieders zijn, vallen zij tot inwerkingtreding van het decreet niet onder de verplichting tot het treffen van voorzieningen.

Aanbieders zijn niet verplicht de werking van de voorzieningen te tonen voordat zij een dienst lanceren.

In de praktijk ziet men problemen in het aftappen van IP-stromen en maakt men zich zorgen om privacy bij aftappen wanneer de aanbieder buiten Europa gevestigd is. Het aftappen van een emaildienst van een aanbieder buiten Europa zou bijvoorbeeld impliceren dat de buitenlandse partij op de hoogte is dat er onderzoek plaatsvindt naar een verdachte in Frankrijk. De Franse autoriteiten geven aan dat het onwenselijk kan zijn dergelijke informatie te delen met een partij buiten Europa.

2.3.3 Bewaren en leveren van gebruikersgegevens

Er geldt een verplichting beschikbare gegevens op te leveren op last van de rechtbank. Het decreet dat in het eerste kwartaal van 2004 van kracht wordt specificeert welke gegevens de aanbieder dient te bewaren.

Aanbieders dienen, voor een periode van maximaal een jaar, de naam en adresgegevens te bewaren van gebruikers van openbare diensten en van aanbieders of medeaanbieders van *content*. De verplichting om de gegevens te bewaren van contentaanbieders dient om deze te kunnen achterhalen in geval van illegale content zoals kinderporno.

De identiteit van de afnemer van een pre-paid betaalde mobiele telefoniedienst is in Frankrijk altijd bekend. Verkoop van de benodigde SIM-kaarten geschied in combinatie met registratie van naam en paspoortnummer van de klant.

2.3.4 Bewaren en leveren van verkeersgegevens

In de regel dienen verkeersgegevens te worden verwijderd of geanonimiseerd zodra de communicatie is afgerond. Verkeersgegevens mag de aanbieder, anders dan voor facturering, alleen bewaren met uitdrukkelijke toestemming van de gebruiker. Deze historische factureringsgegevens mag de aanbieder niet langer bewaren dan nodig is voor betaling en bezwaar, met een maximum van 1 jaar.

Uitzonderingen op deze regel bestaan voor het geval dat de gegevens nodig zijn in het kader van justitieel onderzoek. Het gaat hierbij om het bewaren van gebelde nummers en plaatsgegevens, voor maximaal een jaar. Het bewaren van andere verkeersgegevens, zoals het url en IP-adressen, is nog niet geregeld. Het decreet dat in het eerste kwartaal van 2004 van kracht wordt specificeert ook hiervoor welke gegevens de aanbieder dient te bewaren.

Vordering van gegevens is in een bevel altijd voor een enkel individu gespecificeerd. In de uitvoering leidt deze eis tot complicaties, aangezien de aanbieder niet altijd in staat is precies het verkeer van een enkele gebruiker te isoleren.

2.3.5 Ontheffing van verplichtingen

Er bestaan geen gronden voor ontheffing.

2.3.6 Geschilbeslechting

In Frankrijk bestaan er geen specifieke mechanismen voor disputen omtrent aftappen, en gebeurt de afhandeling door administratieve procedures.

2.3.7 Regels ten aanzien van uitvoering

De Franse autoriteiten geven specifieke aanwijzingen welke voorzieningen de aanbieders moeten treffen. Tevens geeft het aftapbevel de eisen aan in ieder specifiek geval, onder andere voor wat betreft het soort informatie, eventuele bewerking van de data, en de encryptie. Het uitgangspunt is echter dat zonder specifieke aanwijzingen de aftapdata in onaangetaste, ruwe vorm blijven.

Behalve voor justitieel onderzoek, kan opdracht tot aftappen ook door de minister-president worden uitgevaardigd in het belang van de nationale veiligheid.

De Franse autoriteiten vermelden het begintijdstip in het bevel, en zoniet dient de aanbieder de gegevens ‘onverwijld’ beschikbaar te hebben. In de praktijk moet de aanbieder in staat zijn een aftaplast voor een justitieel verzoek binnen een aantal uur uit te voeren. Een aftaplast in het kader van veiligheid moet binnen enkele dagen verwezenlijkt worden.

Een opdracht tot aftappen is in beginsel altijd gericht op een individu. Wanneer een aftapopdracht in de praktijk onmogelijk is doordat de interne aanbieder het zicht op de eindgebruiker afschermt, dan zullen de autoriteiten de medewerking van de interne aanbieder moeten inroepen. Dit is bijvoorbeeld het geval wanneer een verdachte zich bevindt in een intern bedrijfsnetwerk.

In de praktijk mag een aanbieder de inhoud van de getapte communicatie niet inzien. De autoriteiten verrichten alle benodigde data-analyse zelf. Aflevering van data gebeurt op één afleverpunt via een elektronische koppeling met de autoriteiten. De

implementatie van de koppeling is volgens ETSI-normen. Bij een telefoongesprek eisen de autoriteiten naast de inhoud ook de volgende metagegevens: tijd, datum, duur, A- en B-nummers en de locatie, indien er sprake is van een mobiel gesprek.

Een commissie, *Commission Nationale de Contrôle des Interceptions de Sécurité*, bepaalt het toegestane aantal taplasten per jaar. Het aantal taplasten is in 2003 sterk toegenomen. De rechtbank vaardigt per jaar tussen de 10.000 en 15.000 taplasten uit, exclusief veiligheidsgerelateerde taplasten. In het geval dat een taplast door zowel de justitiële autoriteiten als door autoriteiten belast met de veiligheid wordt uitgevaardigd, krijgt justitie voorrang. Onderzoek in het kader van veiligheid resulteert in de praktijk veelal tot nader justitieel onderzoek.

2.3.8 Kosten en vergoedingen

De Franse overheid betaalt een volledige vergoeding voor het treffen van voorzieningen en voor de kosten van het meewerken. De staat maakt de keuze of de investeringskosten ineens vergoed worden of dat deze verwerkt worden in de vergoeding voor de uitvoering van taplasten. Vergoedingen voor kosten worden met elke aanbieder apart geregeld.

De volledige vergoeding is het resultaat van een besluit van de Constitutionele Rechtbank dat dergelijke kosten niet horen tot de noodzakelijke uitgaven voor het aanbieden van telecommunicatiediensten. Op basis hiervan kunnen aanbieders niet worden geacht de kosten te dragen. De Franse overheid heeft voor de vergoeding richtbedragen die het uitgangspunt vormen in het overleg met de aanbieders. De aanbieders moeten hun werkelijke kosten onderbouwen.

De Franse autoriteiten geven aan dat het besluit van de Constitutionele Rechtbank in de praktijk heeft geleid tot een aanzienlijke werklast. Het budget voor justitiële autoriteiten voor 2003 voorzag €13.500.000 voor vergoedingen aan aanbieders, en €10.500.000 voor het huren van aftapapparatuur om aftapopdrachten te implementeren. De autoriteiten noemen het opmerkelijk dat alle aanbieders dezelfde tarieven hanteren voor vergoedingen. De Franse staat onderzoekt mogelijkheden om de standaardvergoedingen vast te stellen.

2.4 Oostenrijk

In Oostenrijk speelt aftappen een belangrijke rol in de opsporing. In de afgelopen jaren is de aandacht toegenomen voor het gebruik van gebruikers-, verkeers- en locatiegegevens; het vorderen van deze gegevens valt in Oostenrijk onder het aftappen. In 2002 werden voor 2064 aansluitingen lasten tot aftappen afgegeven, waarbij bij 1423 van deze aansluitingen alleen verkeers- en locatiegegevens gevorderd werden zonder aftappen van inhoud.

2.4.1 Wet- en regelgeving voor aftappen

De belangrijkste wet- en regelgeving rond aftappen is in Oostenrijk vastgelegd in:
- StrafProzessOrdnung (StPO)
- TeleKommunikationsGesetz 2003 (TKG)
- ÜberwachungsVerOrdnung (ÜVO)

De StrafProzessOrdnung (StPO) regelt de strafvordering, en vormt daarmee de basis voor het aftappen. Het TeleKommunikationsGesetz (TKG), die in 2003 vernieuwd is, legt de verplichtingen vast voor aanbieders van telecommunicatiediensten, terwijl de ÜberwachungsVerOrdnung (ÜVO) deze verplichtingen nader specificeert. De ÜVO, die gebruik maakt van ETSI-normen, wordt nu ook vernieuwd om aan te sluiten op de nieuwe versie van de TKG.

2.4.2 Aanbieders en diensten

Verplichting tot medewerking

Alle aanbieders van openbare netwerken en diensten zijn in Oostenrijk verplicht aan aftappen medewerking te verlenen. Expliciet vrijgesteld zijn aanbieders van defensienetwerken en van netwerken die exclusief bedoeld zijn voor de telecommunicatieautoriteiten.

Verplichting tot het treffen van voorzieningen

De Oostenrijkse wetgeving legt de verplichting tot het treffen van voorzieningen op aan alle aanbieders van openbare telecommunicatienetwerken, tenzij deze geen eindgebruikers aansluiten of alleen bestaan uit *point-to-point* vaste verbindingen. Dit betekent dat *transit* operators, aanbieders van *carrier select* diensten of *peering* diensten niet onder de verplichting vallen. De term ‘openbaar’ in TKG 2003 is niet specifiek gedefinieerd. Redelijkerwijs mag aangenomen worden dat gesloten groepen met een beperkt aantal gebruikers niet onder de noemer openbaar gevat worden. Met aanbieders die vanuit de wet- en regelgeving geen verplichting hebben tot het treffen van voorzieningen, kan aftappen op individuele basis worden geregeld via de verplichting tot medewerking.

De nieuwe ÜVO sluit de internet-toegangsdienst expliciet uit van de verplichting tot het treffen van voorzieningen. De reden voor deze uitsluiting is dat de ISP’s vaak kleiner van bedrijfsomvang zijn, en de investeringslasten voor het implementeren van tapfaciliteiten kunnen voor deze partijen relatief hoog uitvallen.

Internet-verkeer wordt afgetapt op toegangsniveau door het aftappen van telefoonlijnen, van de ADSL infrastructuur, of van andere toegangsinfrastructuren. Tot nog toe zijn alleen voor internet-verkeer via inbellen en via huurlijnen de voorzieningen gespecificeerd; in andere gevallen gebruikt men de verplichting tot medewerking om een individuele oplossing te vinden.

In Oostenrijk biedt de medewerkingverplichting voldoende ruimte om nieuwe diensten te accommoderen en behandelt men dergelijke zaken per geval.

2.4.3 Bewaren en leveren van gebruikersgegevens

Er bestaat in Oostenrijk geen verplichting om gebruikersgegevens te bewaren. De aanbieder mag gebruikersgegevens uitsluitend bewaren ten behoeve van de bedrijfsvoering en moet deze data vernietigen na beëindiging van het contract met de gebruiker. Aanbieders moeten eventueel aanwezige gebruikersgegevens op last van de rechtbank opleveren.

2.4.4 Bewaren en leveren van verkeersgegevens

Verkeersgegevens mogen uitsluitend bewaard worden voor de bedrijfsvoering. Op bevel van de rechter kunnen verkeersgegevens gevorderd worden.

In de praktijk worden verkeersgegevens in Oostenrijk, omwille van de bedrijfsvoering, een jaar bewaard. Formeel bestaat er geen termijn en spreekt de wet over een ‘passende’ periode. Locatiedata van mobiele telecommunicatie bewaren aanbieders normaliter niet, tenzij een tapbevel dit eist.

2.4.5 Ontheffing van verplichtingen

De Oostenrijkse justitie kan kleine aanbieders vrijstellen van het implementeren van specifieke elementen van de ÜVO die een onredelijke operationele of financiële belasting vormen.

2.4.6 Geschilbeslechting

Geschillen worden behandeld door de rechtbank die het bevel tot tappen geeft. Indien er een dispuut blijft bestaan vindt de formele rechtsgang in eerste instantie plaats via administratieve afhandeling door de telecommunicatieautoriteiten, en in tweede instantie door een onafhankelijk tribunaal.

2.4.7 Regels ten aanzien van uitvoering

Aanbieders dienen de aftapvoorzieningen volgens voorgeschreven richtlijnen te treffen en in stand te houden. De regelgeving geeft expliciet aan welke extra informatie bij het afgetapte verkeer meegeleverd dient te worden, zoals het complete adres van de gebruiker, begin- en eindtijd van het gesprek en de gebruikte cel bij mobiele telefonie. Eventuele netwerkgebaseerde encryptie dient verwijderd te worden.

Opdrachten tot aftappen worden door de rechter gegeven. Een last tot aftappen moet een aanbieder ‘onverwijld’ uitvoeren. In Oostenrijk interpreteert men ‘onverwijld’ in het algemeen als enkele uren, maar de rechtbank geeft aan hoe urgent een individueel aftapverzoek is.

De Oostenrijkse autoriteiten bepalen zelf hoe zij het datatransport vanaf de voorgeschreven technische tapvoorziening regelen. De overheidsdienst die zorg draagt voor het verzenden, zorgt ook voor de versleuteling van de data.

2.4.8 Kosten en vergoedingen

De Oostenrijkse wet voorziet vooralsnog alleen in een vergoeding van de directe kosten. De rechtbank die de tap gelast, vergoedt na verificatie de kosten die de aanbieder opvoert.

Recentelijk oordeelde een gerechtshof echter dat de wetgeving niet voldoende recht doet aan de belangen van de aanbieders. De verwachting is dat in de nabije toekomst de investeringskosten verdisconteerd mogen worden in de kosten van het tappen. De nieuwe regelgeving zal naar verwachting een vergoedingsregeling vaststellen voor zowel de indirecte als de directe kosten voor reguliere diensten.

De operationele kosten per tap ziet men in Oostenrijk in de praktijk omhoog gaan, met name als gevolg van de toenemende complexiteit. Eén van de achterliggende redenen is de toenemende vervolging van drugskoeriers die gebruikmaken van meerdere pre-paid telefoons, waardoor het tappen complexer wordt.

2.5 Verenigd Koninkrijk

Het Verenigd Koninkrijk gebruikt aftappen uitsluitend ter ondersteuning van onderzoek of in misdaadpreventie; informatie uit aftappen is niet ontvankelijk als bewijsmateriaal.

Overweging hierbij is dat aftapresultaten als bewijsmateriaal zeer hoge eisen stelt aan de processen en de toetsing van aftappen. De grote complexiteit en hoge kosten kan de overheid niet rechtvaardigen vanuit de waarde van dergelijk bewijs. Bovendien zou aftappen veel meer openbaar geraken en naar verwachting minder nuttige informatie opleveren, wanneer aftapresultaten ingezet worden als bewijsmateriaal.

2.5.1 Wet- en regelgeving voor aftappen

De belangrijkste wet- en regelgeving van het Verenigd Koninkrijk inzake aftappen is vastgelegd in:

- Regulation of Investigatory Powers Act (RIPA)
- Anti-Terrorism, Crime and Security Act (ATCS)

De RIPA regelt zowel het strafvorderingproces als de specifieke verplichtingen van aanbieders van telecommunicatienetwerken en -diensten (sectie 11 en 12).

2.5.2 Aanbieders en diensten

Verplichting tot medewerking

De Britse wetgeving verplicht elke rechtspersoon mee te werken aan het aftappen van elke telecommunicatiedienst. De medewerking dient redelijkerwijs uitvoerbaar te zijn.

Verplichting tot het treffen van voorzieningen

In het Verenigd Koninkrijk leggen de autoriteiten per geval verplichtingen op aan openbare aanbieders. Dit gebeurt alleen wanneer men dit noodzakelijk acht en het de veiligheid niet in het geding brengt. Een aanbieder die geen opdracht krijgt tot het treffen van voorzieningen, hoeft zich uitsluitend te houden aan de verplichting tot medewerking. Alle *openbare* aanbieders kunnen een opdracht tot het treffen van voorzieningen krijgen, ongeacht de telecommunicatiedienst die zij leveren. VPN's en andere oplossingen die private diensten over openbare netwerken mogelijk maken kunnen ook binnen de verplichting vallen. Dienstaanbieders zonder eigen netwerk dienen met de partij waarvan zij de netwerkdiensten afnemen afspraken te maken om aan een opgelegde verplichting te voldoen.

De verplichting geldt niet voor aanbieders met maximaal 10.000 gebruikers, en ook niet voor aanbieders van openbare telecommunicatiediensten ten behoeve van het verzorgen van financiële diensten.

In het Verenigd Koninkrijk speelt het aftappen van gegevens een ondersteunende rol in het recherchewerk. De autoriteiten vertrouwen op een individuele, redelijke en proportionele aanpak ten aanzien van medewerking en het treffen van voorzieningen. Men geeft de voorkeur aan samenwerking met aanbieders, in plaats van hen te dwingen. Dit laatste gebeurt alleen wanneer de gegevens uitermate belangrijk zijn. Jurisprudentie kan hierbij van pas komen.

De Britse autoriteiten beschouwen het als weinig zinvol om in nichemarkten of aan kleinschalige aanbieders eisen op te leggen ten aanzien van aftapvoorzieningen. De autoriteiten vertrouwen in dergelijke gevallen op de verplichting tot medewerking. Nieuwe diensten worden in het Verenigd Koninkrijk door de NTAC[7] onderzocht op effectieve wijze van aftappen. Dankzij de specifieke individuele manier van het opleggen van voorzieningen kan men flexibel inspelen op nieuwe diensten.

2.5.3 Bewaren en leveren van gebruikersgegevens

Er geldt nu geen verplichting tot bewaren van gebruikersgegevens. ATCS beschrijft gegevens en termijnen voor vrijwillige opslag, de 'voluntary retention'. De regeling

[7] *National Technical Assistance Centre*, de organisatie die assistentie verleent voor alle technische zaken rond aftappen

lijkt in tegenspraak te zijn met Europese privacy-richtlijnen. Beschikbare gegevens dienen te worden opgeleverd op verzoek van een groot aantal geautoriseerde instanties.

In de praktijk verwacht men weinig navolging van de vrijwillige opslag. Indien onvoldoende aanbieders de vrijwillige richtlijn volgen kan wetgeving de regeling vervangen.

2.5.4 Bewaren en leveren van verkeersgegevens

Er geldt nu geen verplichting tot bewaren van verkeersgegevens, maar uitsluitend de vrijwillige opslag volgens ATCS. Er zijn bij eventuele opslag duidelijk gespecificeerde regels welke data, hoe en hoe lang worden opgeslagen.

Anders dan de afgetapte inhoud van communicatie, dienen verkeersgegevens in het Verenigd Koninkrijk wel als bewijs in rechtszaken Alle relevante instanties genoemd in de RIPA kunnen verkeersgegevens opvragen. Daartoe behoren bijvoorbeeld ook lokale overheden.

Evenals voor gebruikersgegevens verwacht men ook voor verkeersgegevens dat de ‘vrijwillige opslag’ weinig navolging zal vinden.

2.5.5 Ontheffing van verplichtingen

RIPA kent geen dispensatie. Voorzieningen worden per geval en in redelijkheid overeengekomen.

Indien een aanbieder niet in staat is een aftapbevel op te volgen, volgt zelden dwang. Alleen in zeer belangrijke gevallen wordt medewerking afgedwongen. Precedenten helpen beoordelen welke verzoeken en weigeringen billijk zijn.

2.5.6 Geschilbeslechting

In het Verenigd Koninkrijk is de Technical Advisory Board (TAB) de laatste stap in een formeel proces voor een dispuut. De *Communications Commisioner* en een *Investigatory Powers Tribunal* verwerken alle klachten over inlichtingendiensten.

2.5.7 Regels ten aanzien van uitvoering

De Britse autoriteiten geven specifieke aanwijzingen welke voorzieningen een aanbieder moet treffen. Aanbieders moeten een kopie van de inhoud plus informatie over afgetapt verkeer leveren. Eventuele netwerkgebaseerde encryptie dient verwijderd te worden.

Aftapgegevens dienen ‘onverwijld’ beschikbaar te zijn. De Britse overheid stelt dat aanbieders in staat moeten zijn te tappen binnen 1 werkdag na opdracht.

Alle afgetapte data dient onverkort, en bij voorkeur ontdaan van netwerkgebaseerde encryptie, overhandigd te worden aan de NTAC. In het geval van permanente tapfaciliteiten bij aanbieders leveren zij hun tapdata via vaste verbindingen aan de NTAC. Deze verbindingen zijn eigendom van de NTAC. De NTAC, of de inlichtingendienst in kwestie, verzorgt zelf de bewerking van de ruwe data. Data worden versleuteld voor transport.

Britse inlichtingendiensten kunnen per dienst specifieke eisen stellen aan aanbieders ten aanzien van bijvoorbeeld het formaat en de snelheid van oplevering.

De huidige Britse standaarden voor aftappen zijn vrijwel gelijk aan die van ETSI.

2.5.8 Kosten en vergoedingen

De Britten voorzien in compensatie voor directe en indirecte kosten. Het Britse ministerie van binnenlandse zaken stelt de vergoedingen vast in samenspraak met de betrokken instanties en de aanbieders. Kosten voor aanpassingen aan de aftapinstallatie bij wijzigingen in de dienst worden niet vergoed wanneer deze wijzigingen niet strikt noodzakelijk zijn.

De autoriteiten in het Verenigd Koninkrijk zijn positief over de samenwerking tussen NTAC en de dienstaanbieders. Het begrensde het budget stelt NTAC in staat aanbieders technisch en financieel te assisteren bij het treffen van voorzieningen. De bijdrage in de noodzakelijke investeringen wordt per geval door de NTAC en de aanbieder bepaald. De inlichtingendienst die specifiek baat heeft bij een permanente installatie, betaalt ook de bijdrage in de operationele kosten.

3 Overeenkomsten en verschillen met Nederland

3.1 Inleiding

De wetgeving en de praktijk van het aftappen vertonen in de onderzochte landen duidelijke overeenkomsten, maar ook opvallende verschillen.

Harmonisatie op Europees niveau beperkt zich tot nog toe tot regels voor wederzijdse rechtshulp en harmonisatie van de technische implementatie. Voor het overige gaat er van de Europese regelgeving vooral een beperkende werking uit. Met name het Europees Verdrag van de Rechten van de Mens, de algemene privacyrichtlijn[8], en de privacyrichtlijn voor elektronische communicatie[9] zijn gericht op het waarborgen van de persoonlijke leefsfeer, en bepalen daarmee vooral wat *niet* is toegestaan.

Dit hoofdstuk beschrijft de belangrijkste verschillen en overeenkomsten tussen Nederland en de andere vier landen.

3.2 Wet- en regelgeving aftappen

In elk van de onderzochte landen is aftappen een wettelijke uitzondering op het telecommunicatiegeheim. De wetgeving bepaalt de plaats van aftappen in het opsporingsproces en de verplichtingen voor de aanbieders. Wettelijke verplichtingen in dit kader bestaan uit:

- Een verplichting tot medewerking
- Een verplichting tot het treffen van voorzieningen

In het Verenigd Koninkrijk zijn, in tegenstelling tot de overige onderzochte landen, de resultaten uit het aftappen niet ontvankelijk als bewijsmateriaal. Dit geeft aftappen een geheel andere plek in de opsporing dan in de overige landen. Gegevens over de gebruiker en over het gebruik van telecommunicatiediensten kunnen in het Verenigd Koninkrijk wel als bewijsmateriaal gebruikt worden.

3.3 Aanbieders en diensten

3.3.1 Verplichting tot medewerking

In elk van de onderzochte landen zijn aanbieders van openbare telecommunicatienetwerken en -diensten, net als in Nederland, verplicht mee te werken aan aftappen. In Duitsland geldt deze verplichting ook voor private aanbieders met een zakelijk karakter, zoals de telecommunicatieafdeling binnen een bedrijf. In Frankrijk en in het Verenigd Koninkrijk is zelfs elke rechtspersoon verplicht mee te werken.

---

[8] Richtlijn 95/46/EC betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

[9] Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie

3.3.2 Verplichting tot het treffen van voorzieningen

Net als in Nederland zijn aanbieders van openbare telecommunicatienetwerken in Duitsland en Oostenrijk bij voorbaat verplicht om voorzieningen te treffen ten behoeve van het aftappen. In het Verenigd Koninkrijk *kunnen* aanbieders de opdracht krijgen voorzieningen te treffen; aanbieders hoeven niets te ondernemen zolang de autoriteiten geen specifieke opdracht geven. In Frankrijk krijgen aanbieders formeel gezien specifieke verplichtingen opgelegd, vastgelegd in de licentie. In de praktijk zijn de opgelegde verplichtingen echter gelijk voor alle licentiehouders. Een aanstaande wijziging in regelgeving brengt de situatie in Frankrijk in overeenstemming met de Nederlandse regelgeving.

De verplichting tot het treffen van voorzieningen geldt in Duitsland en Oostenrijk uitsluitend voor aanbieders van openbare telecommunicatie netwerken. In tegenstelling tot de Nederlandse situatie hoeven aanbieders van telecommunicatiediensten zonder eigen netwerk er niet voor te zorgen dat de geboden diensten aftapbaar zijn. Verder geldt de verplichting in deze twee landen uitsluitend voor netwerken waarop gebruikers aangesloten zijn[10]; transit operators vallen hier bijvoorbeeld niet onder. Ook zijn in deze twee landen internet-toegangsdiensten expliciet uitgesloten; het IP-verkeer wordt waar nodig op toegangsniveau afgetapt.

In het Verenigd Koninkrijk kan iedere aanbieder van openbare telecommunicatie-netwerken of -diensten opdracht krijgen om voorzieningen te treffen.

In Frankrijk geldt de verplichting tot het treffen van voorzieningen behalve voor publieke aanbieders met een licentie ook voor aanbieders van ‘onafhankelijke netwerken’: closed user groups op het grondgebied van meer dan een eigenaar. In het eerste kwartaal van 2004 zal een decreet dezelfde verplichtingen tot het treffen van voorzieningen van toepassing verklaren op alle publieke en onafhankelijke aanbieders, ongeacht hun licentie. ISP’s zullen dan ook onder de verplichting vallen.

3.4 Bewaren en leveren van gebruikersgegevens

In elk van de onderzochte landen is het in beginsel verboden om gebruikersgegevens te bewaren die niet voor de bedrijfsvoering noodzakelijk zijn; dit is in overeenstemming met de Europese privacyrichtlijnen.

Frankrijk kent expliciet de verplichting gegevens te bewaren van aanbieders van ‘content’. Deze regel is gericht op het achterhalen van aanbieders van illegale content zoals kinderporno.

[10] Een “aansluiting” kan in dit verband virtueel zijn, zoals in het geval van bepaalde Intelligent Network diensten

Gebruikersgegevens bij pre-paid telefoniediensten zijn in Frankrijk beschikbaar. Afnemers dienen zich te legitimeren en worden geregistreerd.

Voor zover gebruikersgegevens beschikbaar zijn kunnen deze in alle onderzochte landen gevorderd worden. In Duitsland moeten alle beschikbare gebruikersgegevens aan een centrale instantie aangeleverd worden, zodat de autoriteiten er direct bij kunnen. Dit komt overeen met de toekomstige Nederlandse situatie.

3.5 Bewaren en leveren van verkeersgegevens

In de onderzochte landen geldt in het algemeen geen bewaarplicht ten aanzien van verkeersgegevens. Telecommunicatieaanbieders moeten verkeersgegevens verwijderen na beëindiging van de communicatie, tenzij deze noodzakelijk zijn voor de normale bedrijfsvoering of voor een specifiek justitieel onderzoek. Alleen in Nederland geldt hierop een uitzondering voor pre-paid diensten om achteraf alsnog een gebruikt nummer te kunnen achterhalen. In het Verenigd Koninkrijk kent men ‘vrijwillige opslag’ van verkeersgegevens. De autoriteiten verwachten weinig navolging van deze vrijwillige opslag.

In alle onderzochte landen kunnen de autoriteiten verkeersgegevens vorderen indien de aanbieder deze heeft.

3.6 Ontheffing van verplichtingen en geschilbeslechting

3.6.1 Ontheffing van verplichtingen

Ontheffing van verplichtingen is in enkele landen geregeld voor aanbieders met relatief kleine aantallen gebruikers. Ook verleent men gehele of gedeeltelijke ontheffing voor *field trials* of *pilots*. In Duitsland is dit expliciet geregeld: aanbieders met ten hoogste duizend aansluitingen zijn vrijgesteld, en aanbieders met ten hoogste 10.000 aansluitingen kunnen door RegTP geheel of gedeeltelijk vrijgesteld worden.

Voor nieuwe diensten duurt het in alle landen enige tijd voordat de aftapmechanismen voldoende gespecificeerd zijn om van de aanbieders te eisen dat zij deze implementeren. Tot die tijd wordt wel van de aanbieders verwacht dat zij in voorkomende situaties per geval meewerken aan een oplossing.

3.6.2 Geschilbeslechting

Formele geschilbeslechting verloopt in alle landen via administratieve afhandeling; in de meeste gevallen gaat daar een informele bemiddeling door de toezichthouder aan vooraf.

3.7 Regels ten aanzien van uitvoering

Net als in Nederland beschrijft wet- en regelgeving in Duitsland en in Oostenrijk de uitvoering. In Frankrijk en het Verenigd Koninkrijk is dit veel minder het geval; in deze landen geven de autoriteiten aan individuele aanbieders specifieke opdrachten waarin de uitvoering wordt geregeld.

In alle landen wordt de term ‘onverwijld’, of een synoniem, gebruikt voor de snelheid waarmee een aanbieder dient te reageren op een aftapbevel. De interpretatie van de term ‘onverwijld’ varieert daarbij tussen enkele uren en enkele dagen.

Telecommunicatieaanbieders leveren in alle onderzochte landen op een last tot aftappen een kopie van de inhoud plus informatie over afgetapt verkeer. Tevens moet in alle onderzochte landen door het netwerk uitgevoerde encryptie verwijderd worden. Dit is in enkele landen expliciet in de regelgeving opgenomen, in andere wordt dit impliciet als onderdeel gezien van de verplichting tot medewerking of staat het specifiek in elke last.

3.8 Kosten en vergoedingen

Nederland en Duitsland hebben vergelijkbare systemen van kostenvergoedingen. Zowel in Nederland als in Duitsland dient de aanbieder op eigen kosten de aftapsystemen te implementeren en te onderhouden, en worden alleen de directe kosten voor het uitvoeren van een taplast vergoed. De Duitse autoriteiten werken daarbij met een wettelijk vastgelegd uurtarief van € 13,-, terwijl in Nederland de werkelijke kosten het uitgangspunt vormen.

De Franse en Britse autoriteiten vergoeden in principe zowel indirecte als directe kosten van aftappen. De Britse autoriteiten geven aan dat dit een werkbare situatie is. De Franse autoriteiten ervaren de huidige situatie als zeer belastend en verrichten onderzoek naar een systeem dat uitgaat van standaardvergoedingen. In Frankrijk mag een aanbieder investeringskosten in één keer declareren bij de autoriteiten of deze verdisconteren in de taplasten.

Oostenrijk heeft volgens de wet eenzelfde beleid als Nederland, waarbij aanbieders de voorzieningen op eigen kosten moeten treffen, maar recentelijk oordeelde een Oostenrijkse rechtbank dat deze wetgeving geen recht doet aan de belangen van aanbieders. Het is de verwachting dat op afzienbare termijn de indirecte kosten verdisconteerd mogen worden.

4 Tot slot

In elk van de onderzochte landen speelt aftappen een belangrijke rol in de opsporing.

De toename in diensten, en met name in internet-diensten, geeft het aftappen van nieuwe diensten een steeds grotere rol naast het traditionele aftappen van telefoongesprekken. Het aanpassen van de regelgeving aan nieuwe diensten blijkt in veel gevallen enkele jaren te duren. In veel gevallen wordt dit ondervangen door een algemene verplichting aan aanbieders om in elk geval mee te werken aan aftappen, ook als de invulling nog niet in regels geïmplementeerd is.

Het aftappen van telefoniediensten gebeurt vrijwel altijd op het netwerk waarop de gebruiker aangesloten is[11]. Het tappen van internet-diensten is daarentegen op verschillende niveaus mogelijk. Zo kan de aanbieder van de fysieke toegang, bijvoorbeeld de telefoonlijn waarmee ingebeld wordt of de ADSL-verbinding, die toegang aftappen; de ISP kan het IP-verkeer van de internet-toegangsdienst aftappen; en de aanbieder van de dienst -bijvoorbeeld e-mail- kan deze dienst aftappen. Verschillende landen maken op dit onderwerp verschillende keuzes.

Het grootste punt van discussie is in veel landen de verrekening van de kosten die voor het aftappen gemaakt worden. In enkele landen voorziet de wet in een vergoeding voor alle kosten, terwijl andere landen alleen de operationele kosten of slechts een deel daarvan vergoeden. In alle gevallen is het moeilijk de werkelijk gemaakte kosten vast te stellen; daarom streven de autoriteiten steeds naar algemene richtbedragen.

[11] In principe zouden ook de aanbieders van Carrier (Pre-)Select diensten kunnen tappen, maar dit zou een onvolledig beeld geven van het totale verkeer over de aansluiting.

Bijlage 1: Verklarende woordenlijst

Term	Verklaring
ADSL	Asymmetric Digital Subscriber Line; netwerktoegangstechnologie via de telefoonlijn
A-nummer, B-numer	A-nummer is het nummer van de telefoonaansluiting waarvandaan een gesprek is opgezet. Het B-nummer is het nummer van de telefoonaansluiting die gebeld wordt.
Carrier (Pre-) Select	De mogelijkheid om voor het opzetten van telefoongesprekken een specifieke telefonieaanbieder te kiezen (per gesprek of permanent).
Corporate netwerk	Bedrijfsnetwerk
DSL	Digital Subscriber Line; netwerktoegangstechnologie.
Encryptie	Versleuteling van data. Encryptie wordt toegepast om te voorkomen dat niet-geautoriseerden data kunnen lezen of veranderen.
ETSI	European Telecommunications Standards Institute
Flat-rate	Afrekensysteem waarbij de gebruiker een vast bedrag betaalt voor het gebruik van een dienst.
Freephone	Dienst voor nummers die voor de beller gratis zijn (0800-nummers)
GPRS	General Packet Radio Service; GPRS is een functionaliteit in het mobiele (GSM) netwerk die het mogelijk maakt de data in pakketjes te versturen en te ontvangen zonder dat hiervoor continu een verbinding bezet wordt.
Huurlijn	Vaste verbinding die permanent beschikbaar is voor de gebruiker.
Intelligent Network diensten	Diensten die in telefonienetwerken zijn opgenomen en een toevoeging vormen op de standaard telefoniedienst.
IP	Internet Protocol; het communicatieprotocol dat zowel in het internet als binnen de meeste interne datanetwerken gebruikt wordt.
IPsec	Versleutelde verbinding op basis van IP
ISDN	Integrated Services Digital Network; digitale telefonietechnologie
ISP	Internet Service Provider; Internet-dienstaanbieder
LAN	Local Area Network; lokaal computer netwerk
Leased Line	Zie huurlijn
Mailbox-services	Postbus-dienst. Voorbeelden hiervan zijn e-mail en voice-mail.
PABX netwerk	Private Automatic Branch Exchange; Intern telefonienetwerk dat aangesloten is op het publieke

Term	Verklaring
	telefonienetwerk.
Peering	Wederzijdse uitwisseling van data door ISP's
Pre-paid	Afrekensysteem waarbij de gebruiker vooruitbetaalt voor het gebruik van een dienst.
Roaming	Het gebruik van een mobiele telefoniedienst van een andere aanbieder omdat de gebruiker buiten het bereik is van het eigen netwerk.
SIM-kaarten	Subscriber Identity Module; de kaart die de gebruiker van een mobiele telefoniedienst identificeert.
Transit operator	Aanbieder van transportdiensten tussen andere netwerken.
Transmissiediensten	Diensten voor het transporteren van data.
UPT	Universal Personal Telecommunication service; ook wel bekend als bereikbaarheidsdienst, levert een gebruiker de mogelijkheid om op een enkel nummer via verschillende aansluitingen bereikbaar te zijn.
URL	Uniform Resource Locator
VoIP	Voice Over IP; mechanisme om telefonie over IP netwerken mogelijk te maken
VPN	Virtual Private Network

Bijlage 2: Vragenlijst

Onderstaande vragenlijst is als basis gebruikt voor de analyse van de regelgeving in de onderzochte landen.

Research questions to be applied to each country

1. Which laws and other rules (including guidelines from regulators or important court rulings) govern lawful interception?
   - Please provide references to or copies (preferably in electronic form) of the legal texts. Please reference specific articles of these texts in answering the remaining questions.
2. How do these rules define the providers' obligations?
3. To which providers these obligations apply?
   - To providers of *networks* (i.e. operators) or *services*? If both, are the obligations the same?
   - For *public* telecommunications services only, or for *private* services (e.g. VPNs) as well?
   - For *retail* services (directly provided to end-users) only, or for *wholesale* (intermediate) services as well?
   - For all telecommunications services or for services listed specifically? Which ones? What is the definition of "telecommunications service" (does it include e-mail messages, chat, web surfing, internet service provision)? Are the rules identical (as far as possible) for all services?
   - Are there grounds to exempt providers or services from the obligations (e.g. size, revenue, number of subscribers)? What are the exemption criteria, and who establishes them?
4. How is the interception capability implemented? Does the provider need to realise these facilities, or does the law enforcement organisation provide the facilities?
5. If the provider has to implement the interception capability,
   - What information must the provider deliver and how does delivery take place?
   - Is the provider expected to perform processing of the content, (e.g. filtering, summarising, decryption)? Which?
   - How quickly does a provider have to respond to an interception order?
   - Is the provider expected to deliver the intercepted content to multiple locations simultaneously?
   - Does the intercepted content have to be encrypted for delivery?
   - How are the technical specifications for interception and delivery formats established? Do providers play a role?
6. How are the costs of lawful intercept allocated?
   - Who pays for the investment in lawful interception facilities?
   - Who pays for the maintenance and ongoing costs?
   - Who pays for the operational costs of the actual interception order?

- Who pays for leased lines or other connections needed for delivery of intercepted information to the law enforcement organisation?

7. Is there any cost recovery or fee paid by the law enforcement organisation (or other public body)?
   - Is this payment based on the direct costs only of the execution of an interception order, or does it allow for recovery of investments and ongoing costs?
   - Are the amounts fixed or determined case by case?
   - How are the amounts determined?
8. Is there an obligation
   - To store user data (information about users and services subscribed to) or traffic data (information about the actual use of services)?
   - If yes, what information has to be stored, and for how long?
   - If yes, are there rules for the storage medium, the response time and criteria for delivery, and the precise data elements to be stored?
   - If there is no obligation to store user data, but the provider stores it for other reasons, is there then an obligation to deliver this information ?
   - What rules are there for the deletion of such information (e.g. rules based on Directive 2002/58/EC or its predecessor 97/66/EC)?
9. Is a mechanism available to resolve disputes between providers and law enforcement organisations?
   - Does resolution take place through a court or a public body? In first instance, second instance?
10. Can dispensation of these obligations be given to a provider?
    - On what grounds, by whom, to what providers?

Bijlage 3: Schematisch overzicht bevindingen

Vraag	Nederland	Verenigd Koninkrijk	Frankrijk	Oostenrijk	Duitsland
1) Wat is de belangrijkste wet- en regelgeving waarin de aftapverplichting is gerealiseerd?	Telecommunicatiewet Wetboek van strafvordering Wet op inlichtingen- en veiligheidsdiensten 2002; Diverse Besluiten en Regelingen	RIPA (Regulation of Investigatory Powers Act) ATCS (Anti-Terrorism, Crime and Security Act) Opmerking: aftapgegevens vormen nooit bewijsmateriaal	Loi sur le secret des correspondances ("Wet van 1991") Code de procédure pénale Code des Postes et Télécommunications	TeleKommunikationsGesetz (TKG) 2003 StrafProzessOrdnung (StPO) ÜberwachungsVerOrdnung (ÜVO)	TeleKommunikationsGesetz (TKG) 1996 TeleKommunikations-ÜberwachungsVerordnung (TKÜV) StrafProzessOrdnung (StPO)
2) Hoe is de verplichting in de wetgeving gedefinieerd?	Elke aanbieder: • Verplichting tot medewerking • Verplichting voorzieningen te treffen voor aftappen	Elke rechtspersoon: • Verplichting tot medewerking Publieke aanbieders: • Verplichting voor specifieke diensten voorzieningen te treffen voor aftappen indien zij daartoe worden aangewezen	Elke aanbieder: • Verplichting tot medewerking • Verplichting voorzieningen te treffen voor aftappen	Elke aanbieder: • Verplichting tot medewerking • Verplichting voorzieningen te treffen voor aftappen	Elke aanbieder op zakelijke basis: • Verplichting tot medewerking • Verplichting voorzieningen te treffen voor aftappen • Verplichting jaarlijks cijfers over intercepts leveren aan de toezichthouder
3a) Welke aanbieders vallen onder de verplichting *t.a.v. medewerking*?	De verplichting tot medewerking geldt voor elke aanbieder van • Publiek netwerk of • Publieke dienst Vrijstelling van de verplichting tot medewerking kan worden verleend in bijzondere gevallen	De verplichting tot medewerking geldt voor elke rechtspersoon voor elke dienst	De verplichting tot medewerking geldt voor elke aanbieder van • Publiek of privaat netwerk of • Publieke of private dienst, behalve broadcast-diensten	De verplichting medewerking geldt voor alle aanbieders van • Publiek netwerk of • Publieke dienst Vrijgesteld van de verplichtingen zijn defensienetwerken en netwerken exclusief bedoeld voor Telecomautoriteiten.	De verplichting tot medewerking geldt voor elke aanbieder van • Zakelijk publiek of privaat netwerk of • Zakelijke publieke of private dienst Hieronder vallen ook CUG, CN, mailbox, ISP en transmissiediensten

Vraag	Nederland	Verenigd Koninkrijk	Frankrijk	Oostenrijk	Duitsland
3b) Welke aanbieders vallen onder de verplichting *t.a.v. het treffen van voorzieningen*?	De verplichting tot het treffen van voorzieningen voor aftappen geldt voor elke aanbieder van • Publiek netwerk of • Publieke dienst Vrijstelling van de verplichting tot treffen van voorzieningen voor aftappen kan worden verleend in bijzondere gevallen	Een specifieke aanwijzing om voorzieningen te treffen kan worden opgelegd aan elke aanbieder van • Publiek netwerk of • Publieke dienst Hieronder vallen ook diensten die gebruikmaken van privacy-technieken (VPN, encryptie) De verplichting geldt niet voor diensten die alleen gebruik maken van telecommunicatie voor het beschikbaar maken van financiële diensten. De verplichting geldt niet voor aanbieders met maximaal 10.000 gebruikers. Aanwijzing geschiedt alleen waar noodzakelijk, en indien de veiligheid daarmee niet in het geding komt.	De verplichting tot het treffen van voorzieningen voor aftappen geldt voor elke aanbieder van • Publiek of privaat netwerk of • Publieke of private dienst, behalve broadcast	De verplichting geldt voor alle aanbieders van • Publiek netwerk of • Publieke dienst Niet van toepassing op diensten voor CUG's. De verplichting geldt niet voor ISP's. Vrijgesteld van de verplichtingen zijn defensienetwerken en netwerken exclusief bedoeld voor Telecomautoriteiten.	De verplichting tot het treffen van voorzieningen voor aftappen geldt voor elke zakelijke aanbieder van • Zakelijk publiek netwerk of • Zakelijke publieke dienst, inclusief CUG, CN, mailbox, ISP en transmissiediensten De verplichting voor het leveren van voorzieningen voor tappen geldt niet voor aanbieders van • interne diensten aan beperkte groepen zonder winstoogmerk: ziekenhuizen, hotels en corporate networks. • een systeem dat geen eigen klanten heeft: interconnectie van accessnetwerken of met internet • netwerkaanbieders met maximaal 1000 klanten • aanbieders van broadcast, meetgegevens, noodsignalen of algemeen beschikbare informatie
4) Op welke wijze is de aftapbaarheid gerealiseerd? Moet de aanbieder hier iets voor doen, of plaatst de overheid zelf een voorziening direct op de lijn?	Aanbieder: • treft voorzieningen, • levert eventueel ruimte en mensen • en levert gegevens en afgetapt verkeer op verzamelpunt	Elke aanbieder krijgt specifieke aanwijzingen indien hij voorzieningen dient te treffen.	Aanbieder bouwt voorzieningen volgens specificatie van Ministerie.	Aanbieder voorziet in alle installaties, en werkt mee aan intercept.	De aanbieder houdt de voorzieningen voor aftappen in stand. Aanbieder kiest een hand-over punt, met instemming van de toezichthouder.

Vraag	Nederland	Verenigd Koninkrijk	Frankrijk	Oostenrijk	Duitsland
5) Indien de aanbieder iets moet doen, wat dient er dan getapt worden en op welke wijze dient dit te worden aangeleverd?					
*Wat dient er getapt worden en op welke wijze dient dit te worden aangeleverd***?**	Kopie van inhoud plus meta-informatie over afgetapte verkeer	Kopie van inhoud plus meta-informatie over afgetapte verkeer	Kopie van inhoud, indien specifiek vereist met bewerking, plus meta-informatie over afgetapte verkeer	Adres van getapte lijn, (partiële) gekozen B-nummers (ook zonder succes), A-nummers die het getapte nummer bellen. Begin eind en duur van (gepoogde) gesprekken. Bij mobiel: gebruikte cellen.	Kopie van inhoud plus meta-informatie over afgetapte verkeer. Expliciet geen telecommunicatie die niet in het bevel is benoemd.
Moet de aanbieder zelf een bewerking op de afgetapte inhoud uitvoeren?	Aanbieder verwijdert netwerk gebaseerde encryptie	Aanbieder verwijdert netwerk gebaseerde encryptie	Naar eis van behoeftesteller. Instanties zullen sleutel eisen of decryptie.	Aanbieder levert noodzakelijke medewerking aan tappen door autoriteiten.	Geen processing voorgeschreven
Hoe snel moet een aanbieder aan een last voldoen?	Onverwijld	Onverwijld met maximaal 1 dag	Zoals in het bevel aangegeven, anders onverwijld	Niet bij wet vastgelegd. Autoriteiten verrichten tapwerkzaamheden	Onverwijld
Moet de inhoud op meerdere locaties kunnen worden afgeleverd?	Ja	Niet gespecificeerd, normaliter 1 afleverpunt	Indien het bevel dit eist	Aanbieder levert voorzieningen voor intercept op vaste technische interface.	Ja
Moet de inhoud versleuteld aangeleverd worden?	Alleen indien gevaar op meeluisteren dreigt	Op interface met aanbieder realiseert autoriteit zelf encryptie	Nee, niet door de aanbieder.	Bepaalt de tappende instantie zelf.	Informatie beveiligen tegen meelezen. Encryptie niet voorgeschreven.
Hoe komen de technische specificaties tot stand?	Autoriteiten betrekken aanbieder bij keuze van format	Advisory board geeft ETSI-achtige standaarden	Het specifieke bevel en de generieke lijst geautoriseerde tap-installaties bepalen de formaten.	Technische formats in Surveillance Regulation. ETSI norm ES 201671. Nieuwe technische regeling verwacht.	Regulator met hulp van aanbieders, fabrikanten en opsporingsinstanties

Vraag	Nederland	Verenigd Koninkrijk	Frankrijk	Oostenrijk	Duitsland
6) Wie betaalt voor de voorzieningen voor aftappen?	Aanbieder betaalt voor investering en onderhoud. De autoriteiten betalen voor feitelijk gebruik en transport van de afgetapte inhoud.	Aanbieder en overheid (via NTAC) betalen samen investering en onderhoud. De belanghebbende overheidsinstantie betaalt voor gebruik en transport.	De overheid betaalt door middel van ‘ fair compensation’ alle kosten, aangezien deze niet horen tot de noodzakelijke uitgaven voor het aanbieden van telecommunicatie.	Voorheen vergoeding voor medewerking in intercept. Nieuwe regel voorziet in vergoeding voor intercept en voor vereiste voorzieningen	De aanbieder betaalt investering en onderhoud; deze betaalt ook voor het jaarlijkse overzicht van intercepts. De aanbieder ontvangt een compensatie voor personeel en gebruik van voorzieningen. De opsporingsinstantie betaalt het transport naar de behoeftestellers
7) Worden er vergoedingen betaald aan aanbieders, en zo ja, waarvoor?	Alleen directe kosten, naar werkelijke kosten	De overheid participeert in de kosten voor de voorzieningen om af te tappen, zowel in investering als in onderhoud. De opsporingsinstantie betaalt voor gebruik van de voorziening. Home office modelleert kosten met instanties en aanbieders.	Overheid geeft ‘fair compensation’ voor alle kosten die de aanbieder maakt. ‘ Fair compensation wordt bepaald in overeenkomst tussen overheid en aanbieder. Overheid gaat met richtbedragen overleg met aanbieder aan. Aanbieder moet werkelijke kosten onderbouwen.	Vergoeding voor installatie en medewerking nog niet vastgelegd Vaste vergoedingen gepland Regeling moet nog gemaakt worden	De overheid geeft compensatie voor gebruik. Vaste bedragen conform de tarieven voor andere afnemers gelden ter compensatie van directe kosten. De vaste vergoeding bedraagt 13 Euro per uur.
8a) Is er een verplichting ten aanzien van gebruikersgegevens?					
Om gegevens over gebruikers vast te leggen?	Ja, mits beschikbaar	Vrijwillige ‘retention’ vanwege ATCSA, kan verplicht worden.	Ja, voor gebruik in onderzoek naar misdrijven	Nee	Gegevens over gebruikers dienen te worden bewaard, maar uitsluitend indien deze gegevens noodzakelijk zijn voor het leveren van de dienst.

Vraag	Nederland	Verenigd Koninkrijk	Frankrijk	Oostenrijk	Duitsland
Zo ja, welke informatie dient er bewaard te worden, en hoe lang?	NAW en nummer van gebruikers, op 24 uur actueel *(nog niet ingegaan)*	NAW en nummers (ook IP, MAC, enz.), 12 maanden	NAW van abonnees, NAW van (mede)aanbieders van content Maximaal een jaar bewaren	-	NAW en nummer.
Indien er een bewaar-plicht is, zijn er regels voor de wijze van opslag, snelheid en criteria voor op-levering, en specifieke gegevens die bewaard moeten worden?	Een centraal bestand bij het CIOT *(nog niet ingegaan)*	Data-elementen in data retention consultation	Nog bij besluit te bepalen.	-	Gegevens dienen te worden bewaard in een geautomatiseerd systeem dat volgens bekende procedures te raadplegen is.
Indien er geen bewaar-plicht is, is er dan wel een verplichting om gegevens te leveren die om een andere reden bewaard zijn?	Gegevens moeten ter beschikking worden gesteld indien beschikbaar.	Ja, voor alle instanties in RIPA, (meer dan voor tappen)	Per bevel te bepalen. Gegevens anders dan voor facturering alleen bewaren met uitdrukkelijke toestemming van gebruiker; dit geldt ook voor marketingdoeleinden	Alleen bij gerechtelijk bevel	Alleen bij gerechtelijk bevel
Welke regels gelden voor het verwijderen voor dergelijke gegevens? (Bijvoorbeeld gebaseerd op Directive 2002/58/EC of de voorganger 97/66/EC)?	Zodra de gegevens niet meer nodig zijn voor de bedrijfsvoering	Ja, voor alle instanties in RIPA, Opmerking: dit zijn meer instanties, in aantal, dan voor tappen	Uiterlijk een jaar na beëindiging contract wissen.	Alleen bewaren gedurende contractduur. Onmiddellijk na beëindiging contract wissen.	Uiterlijk een jaar na beëindiging van het contract dienen de gegevens over de gebruiker te worden gewist.
8b) Is er een verplichting ten aanzien van het 'verkeersgegevens'?					
Om gegevens over gebruikers en hun gebruik van de diensten vast te leggen?	Nee, tenzij het nummer van een gebruiker anders onbekend is (Pre-Paid telefonie)	Vrijwillige 'retention' vanwege ATCSA, kan verplicht worden	Ja, voor gebruik in onderzoek naar misdrijven	Nee	Nee

Vraag	Nederland	Verenigd Koninkrijk	Frankrijk	Oostenrijk	Duitsland
Zo ja, welke informatie dient er bewaard te worden, en hoe lang?	In geval het nummer anders onbekend is (pre-paid), gegevens over alle gesprekken, 3 maanden bewaren om te kunnen achterhalen uit twee observaties met welk nummer een persoon belt	Vrijwillig bewaren: Nummers, tijdstip, duur, IP-adres, base stations: 12 maanden SMS, email, ISP: 6 maanden Web: 4 dagen	Gebelde nummers en plaatsgegevens, maximaal een jaar bewaren Andere gegevens (url, IP) nog bij besluit te bepalen.	-	-
Indien er een bewaarplicht is, zijn er regels voor de wijze van opslag, snelheid en criteria voor oplevering, en specifieke gegevens die bewaard moeten worden?	Gegevens: A- en B-nummer, base station en tijdstip	Zie hierboven	Nog bij besluit te bepalen.	-	-
Indien er geen bewaarplicht is, is er dan wel een verplichting om gegevens te leveren die om een andere reden bewaard zijn?	Ja	Ja, voor alle instanties in RIPA, (meer dan voor tappen)	Per bevel te bepalen.	Alleen bij gerechtelijk bevel	Alleen bij gerechtelijk bevel: nummers, kaartnummer en locatie van de gebruikers, en tijdstip van de verbinding.
Welke regels gelden voor het verwijderen voor dergelijke gegevens? (Bijvoorbeeld regels gebaseerd op Directive 2002/58/EC of de voorganger 97/66/EC)?	Gebruik: Alleen bewaren voor billing, marketing, sales, fraudepreventie en juridisch gebruik, weggooien indien niet meer nodig	-	Gegevens voor afrekening niet langer bewaren dan nodig voor betaling en bezwaar. Gegevens andere doelen zoals marketing alleen bewaren met uitdrukkelijke toestemming van gebruiker. Gegevens van online diensten direct na gebruik vernietigen, behalve voor onderzoek naar misdrijven, en indien nodig voor afrekening en beveiliging van het netwerk.	Alleen bewaren voor afrekening en bezwaarperiode.	Gegevens die niet dienen voor facturering dienen na maximaal 1 dag te worden gewist. Gegevens die wel voor facturering dienen mogen maximaal 6 maanden worden bewaard, op voorwaarde dat tenminste 3 cijfers uit het B-nummer zijn gewist.

Vraag	Nederland	Verenigd Koninkrijk	Frankrijk	Oostenrijk	Duitsland
9) Is er een geschilbeslechting?	Wet laat een mechanisme voor geschilbeslechting toe, maar dit is niet geïmplementeerd.	Normaliter in overleg afstemmen. *Technical Advisory Board* administratieve laatste instantie.	Nee, gebruikelijke afwikkeling door bemiddeling en administratieve behandeling van bezwaar.	Behandeling door lokale telecommunicatieautoriteiten. In laatste instantie door administratief tribunaal.	Administratieve behandeling.
10) Kan er ontheffing worden verleend?	Is wel mogelijk, geen geval van dispensatie bekend.	Indien een aanbieder onmachtig is volgt zelden dwang. Alleen bij direct belang van overheidsinstanties worden aanbieders aangewezen voor tappen.	Een bevel moet worden opgevolgd.	Nee. Voorzieningen en medewerking moeten worden geleverd.	Kleine aanbieders (minder dan 10000 abonnees) kunnen worden vrijgesteld. Afwijkingen van de technische implementatie kunnen worden toegestaan

Bijlage 4: Geïnterviewde partijen

Land	Gesprekspartners
Duitsland	RegTP, Abteilung Informationstechnik und Sicherheit, technische Umsetzung von Überwachungsmaßnahmen
Frankrijk	Ministère de l'Economie, des Finances et de l'Industrie, Service Sécurité des Technologies de l'Information et de la Communication
Oostenrijk	Bundesministerium für Justiz, Straflegislativsektion, Abteilung II 3 (Angelegenheiten der Strafprozessordnung)
Verenigd Koninkrijk	Home Office, NTAC

Bijlage 5: Gedetailleerde juridische analyse