Vaststelling van Geharmoniseerde Beleidsregels voor de ICT-Markt in de ACS-landen

Aftappen van communicatie: Richtlijnen voor Model Beleid & Wetteksten

HIPCAR

Harmonisatie van Beleid, Wetgeving en Regelgevings procedures op het stuk van ICT in het Caribisch gebied

Europese Commissie

CARICOM

CTU

ITU

Aftappen van communicatie:

Richtlijnen voor Model Beleid

& Wetteksten

HIPCAR

Harmonisatie van Beleid, Wetgeving en Regelgevings procedures op het stuk van ICT in het Caribisch gebied

Dit document is tot stand gekomen met de financiële ondersteuning van de Europese Unie. De standpunten die hierin tot uiting worden gebracht zijn geenszins een weergave van de officiële mening van de Europese Unie.

De gehanteerde benamingen en de presentatie van materiaal, waaronder begrepen kaarten, houden geen uiting in van enige mening van de ITU met betrekking tot de juridische status, of de afbakening van de grenzen, van enig land, territorium, stad of gebied. De vermelding van specifieke ondernemingen of van bepaalde producten betekent niet dat deze worden onderschreven of aanbevolen door de ITU boven andere van soortgelijke aard die niet worden vermeld. Dit Rapport heeft geen redactionele revisie ondergaan.

Denk aan het milieu voordat u dit rapport print.

© ITU 2012

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, op enige manier dan ook, zonder voorafgaande schriftelijke toestemming van de ITU.

Voorwoord

Informatie- en communicatietechnologie (ICT) geeft vorm aan het proces van het globalisatie. Het potentieel hiervan erkennend voor het bespoedigen van de economische integratie van de Caribische regio en daarbij haar grotere welvarendheid en sociale transformatie, heeft de CARICOM Interne Markt en Economie (CSME) een ICT-strategie ontwikkeld die gefocust is op versterkte connectiviteit en ontwikkeling.

Liberalisatie van de telecommunicatiesector is een van de sleutelelementen van deze strategie. Coördinatie binnen de gehele regio is essentieel indien beleid, wetgeving en praktijken voortvloeiend uit de liberalisatie door elk land niet dermate verschillend moeten zijn dat ze een belemmering gaan vormen voor de ontwikkeling van een regionale markt.

Het project 'Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT' (HIPCAR) was gericht op het aanpakken van deze potentiële belemmering door het samenbrengen en begeleiden van alle 15 Caribische landen in de Groep van Staten in Afrika, het Caribisch Gebied en de Stille Oceaan (ACP) terwijl zij hun geharmoniseerd Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT formuleerden en aannamen. Uitgevoerd door de Internationale Telecommunicatie-Unie (ITU), is het project ondernomen in nauwe samenwerking met de Caribische Telecommunicatie-Unie (CTU), die de voorzitter is van de HIPCAR-Stuurgroep. Een mondiaal stuurcomité bestaande uit de vertegenwoordigers van het ACP-Secretariaat en het Directoraat-generaal EuropeAid Ontwikkeling en Samenwerking (DEVCO, Europese Commissie) houdt toezicht op de totale implementatie van het project.

Het project vindt plaats in het kader van het programma ACP Informatie- en Telecommunicatietechnologie (@CP-ICT) en wordt gefinancierd uit het 9e Europees Ontwikkelingsfonds (EDF), dat het voornaamste instrument is voor het verstrekken van Europese hulp voor ontwikkelingssamenwerking in de ACP-Staten, met medefinanciering van de ITU. Het @CP-ICT is gericht op het ondersteunen van de ACP-regeringen en -instituten bij het harmoniseren van hun ICT-beleid in de sector door het bieden van beleidsadvies, training en gerelateerde capaciteitsopbouw van hoge kwaliteit, met referentiepunten over de hele wereld doch van plaatselijke relevantie.

Alle projecten die meerdere belanghebbenden bij elkaar brengen worden geconfronteerd met de dubbele uitdaging van het creëren van een gevoel van gedeeld ownership en het waarborgen van optimale resultaten voor alle partijen. HIPCAR heeft bijzondere aandacht besteed aan deze kwestie vanaf het prille begin van het project in december 2008. Overeenstemming bereikt hebbend over gedeelde prioriteiten, werden werkgroepen van belanghebbenden gevormd voor het aanpakken daarvan. De specifieke noden van de regio werden vervolgens geïdentificeerd evenals potentiële succesvolle regionale praktijken, welke daarna werden getoetst aan elders gevestigde praktijken en standaarden.

Deze gedetailleerde beoordelingen, die bijzonderheden die specifiek waren voor de landen weerspiegelen, dienden als basis voor het modelbeleid en de modelwetteksten die het vooruitzicht boden van een wetgevingslandschap waarop de hele regio trots kan zijn. Het project zal zeker andere regio's tot voorbeeld strekken bij hun pogingen de katalytische kracht van ICT bruikbaar te maken voor het bespoedigen van economische integratie en sociale en economische ontwikkeling.

Ik maak gebruik van deze gelegenheid om dank uit te brengen aan de Europese Commissie en het ACP-Secretariaat voor hun financiële bijdrage. Ik breng ook dank uit aan het Secretariaat van de Caribische Gemeenschap (CARICOM) en het Secretariaat van de Caribische Telecommunicatie-Unie (CTU) voor hun bijdrage aan dit werk. Zonder de politieke wil van de zijde van de begunstigde landen zou niet veel zijn bereikt. Ik breng daarom mijn hartgrondige dank uit aan alle ACP-regeringen voor hun politieke wil welke dit project tot een groot succes heeft gemaakt.

Brahima Sanou
BDT, Directeur

Dankwoord

Dit document vertegenwoordigt een van de resultaten van de regionale activiteiten uitgevoerd in het kader van het HIPCAR-project “Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT” officieel van start gegaan in Grenada in december 2008.

In reactie op zowel de uitdagingen als de kansen voortvloeiende uit de bijdrage van de informatie- en communicatietechnologie (ICT) aan de politieke, sociale, economische en ecologische ontwikkeling, hebben de Internationale Telecommunicatie-Unie (ITU) en de Europese Commissie (EC) hun krachten gebundeld en een overeenkomst getekend voor het geven van “Assistentie bij de vaststelling van geharmoniseerde beleidsregels voor de ICT-markt in de ACP”, als onderdeel van het Programma “ACP-Informatie- en Communicatietechnologie (@CP-ICT)” in het kader van het 9e Europees Ontwikkelingsfonds (EDF), i.e. het ITU-EC-ACP-project.

Dit wereldwijd ITU-EC-ACP-project wordt geïmplementeerd via drie aparte subprojecten die zijn afgestemd op de specifieke behoeften van elke regio: het Caribisch Gebied (HIPCAR), sub-Sahara Afrika (HIPSSA) en de Stille Zuidzee Eilandstaten (ICB4PAC).

De HIPCAR-Stuurgroep - voorgezeten door de Caribische Telecommunicatie-Unie (CTU) - zorgde voor de begeleiding en ondersteuning van een team van adviseurs, onder wie Gilberto Martíns de Almeida, Kwesie Prescod en Karen Stephen-Dalton. Het concept document werd vervolgens bestudeerd, gefinaliseerd en met een ruime consensus aangenomen door de participanten van twee consultatieworkshops voor de HIPCAR-Werkgroep Kwesties de Informatiemaatschappij rakende, gehouden te Saint Lucia van 8-12 maart 2010 en Barbados van 23-26 augustust 2010 (zie Bijlagen). De toelichting bij de modelwettekst in dit document is opgesteld door Gilberto Martíns de Almeida en behandelt onder andere de punten die tijdens de tweede workshop naar voren werden gebracht.

ITU wil een bijzonder woord van dank uitbrengen aan de delegaties van de Caribische ministeries belast met ICT en telecommunicatie die hebben deelgenomen aan de workshops, alsook aan vertegenwoordigers van ministeries van justitie en juridische zaken en andere lichamen uit de publieke sector, regelgevende lichamen, de academische wereld, het maatschappelijk middenveld, aanbieders van diensten en regionale organisaties, voor hun harde werk en toewijding bij het produceren van de inhoud van dit rapport. Door deze brede participatie van de publieke sector vertegenwoordigende verschillende sectoren heeft het project kunnen profiteren van een dwarsdoorsnede van standpunten en belangen. De bijdragen vanuit het Secretariaat van de Caribische Gemeenschap en de Caribische Telecommunicatie-Unie worden ook met dank gememoreerd.

Zonder de actieve betrokkenheid van al deze belanghebbenden, zou het niet mogelijk zijn geweest documenten zoals deze te produceren, welke niet alleen de algemene vereisten en voorwaarden van de Caribische regio weergeven maar ook de internationale beste praktijk vertegenwoordigen.

De activiteiten zijn ten uitvoer gelegd door Kerstin Ludwig, verantwoordelijk voor de coördinatie van activiteiten in het Caribisch Gebied (HIPCAR-Projectcoördinator), en Sandro Bazzanella, verantwoordelijk voor het beheer van het volledig project voor de landen in Afrika ten zuiden van de Sahara, het Caribisch Gebied en de Stille Oceaan (ITU-EC-ACP-Projectmanager), met algemene ondersteuning van Nicole Darmanie, HIPCAR-Projectassistent, en van Silvia Villar, ITU-EC-ACP-Projectassistent. Het werk is uitgevoerd onder de algemene leiding van Cosmas Zavazava, Hoofd, afdeling Projectondersteuning en Kennisbeheer (PKM). Het document is verder verbeterd aan de hand van de commentaren van de ITU Telecommunication Development Bureau’s (BDT) ICT-applicaties en Cybersecurity Divisie (CYB), evenals van Michael Tetelmann. Philip Cross van het ITU Regionaal Kantoor voor het Caribisch gebied verleende ondersteuning. De vooropmaak werd verzorgd door Pau Puig Gabarró. Het team van ITU’s Publication Composition Service (dienst samenstelling publicaties) is verantwoordelijk voor de publicatie.

Inhoudsopgave

Bladzijde

Inleiding

1.1. HIPCAR-Project – Doelstellingen en begunstigden

Het door de EU-ITU gefinancierd HIPCAR – project[1] met een looptijd van drie jaar werd door de Internationale Telecommunicatie Unie (ITU) en de Europese Unie (EU) gelanceerd in september 2008, in nauwe samenwerking met het Secretariaat van de Caribische Gemeenschap (CARICOM) en de Caribische Telecommunicatie Unie (CTU). Het maakt deel uit van een globaal ITU-EU-project voor de ACP-staten en omvat tevens de landen in Afrika ten zuiden van de Sahara en in de Stille Oceaan.

Het doel van HIPCAR is CARIFORUM[2]-landen in het Caribisch gebied te assisteren bij het harmoniseren van hun beleid en procedures voor wet- en regelgeving op het vlak van informatie- en communicatietechnologie (ICT) met het oog op het scheppen van een gunstig klimaat voor ICT-ontwikkeling en connectiviteit, om zo de marktintegratie te bevorderen, de investering in verbeterde ICT-capaciteit en -diensten aan te moedigen en de bescherming van de belangen van ICT-gebruikers in de hele regio te vergroten. Het uiteindelijk doel van het project is het versterken van het concurrentievermogen en de sociaal-economische en culturele ontwikkeling in het Caribisch gebied door middel van ICT.

Overeenkomstig artikel 67 van het Herziene Verdrag van Chaguaramas, kan HIPCAR worden beschouwd als een integrerend deel van het streven van de regio om de CARICOM Interne Markt & Economie (CSME) te ontwikkelen via de progressieve liberalisatie van zijn ICT-dienstensector. Het project biedt ook ondersteuning aan de CARICOM-Agenda voor Connectiviteit en de verplichtingen van de regio tegenover de Wereldtop over de informatiemaatschappij (WSIS), de Algemene Overeenkomst van de Wereldhandelsorganisatie inzake de Handel in Diensten (WTO-GATS) en de Millenniumdoelstellingen voor Ontwikkeling (MDG's). Het houdt tevens rechtstreeks verband met het bevorderen van het concurrentievermogen en een grotere toegang tot diensten in de context van verdragsverplichtingen zoals de Economische Partnerschapsovereenkomst van de CARIFORUM-landen met de Europese Unie (EU-EPA).

De begunstigde landen van het HIPCAR-project zijn Antigua en Barbuda, de Bahama's, Barbados, Belize, Gemenebest Dominica, de Dominicaanse Republiek, Grenada, Guyana, Haïti, Jamaica, St. Kitts en Nevis, St. Lucia, St. Vincent en de Grenadines, Suriname, en Trinidad en Tobago.

---

1 De volledige titel van het HIPCAR-project is "Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT". HIPCAR is deel van een mondiaal ITU-EC-ACP-project ondersteund en gefinancierd door de Europese Unie met EUR 8 miljoen en een aanvulling van USD 500,000 van de Internationale Telecommunicatie Unie (ITU). Het wordt uitgevoerd door de Internationale Telecommunicatie Unie (ITU) in samenwerking met de Caribische Telecommunicatie Unie (CTU) en met betrokkenheid van andere organisaties in de regio.
(zie **www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html**).

2 Het CARIFORUM is een regionale organisatie van vijftien onafhankelijke staten in het Caribisch gebied (Antigua en Barbuda, Bahama's, Barbados, Belize, Dominica, de Dominicaanse Republiek, Grenada, Guyana, Haïti, Jamaica, Saint Christopher en Nevis, Saint Lucia, Saint Vincent en de Grenadines, Suriname, en Trinidad en Tobago). Deze staten zijn alle ondertekenaars van de ACP-EU-verdragen.

1.2. Stuurcomité en Werkgroepen van het project

HIPCAR heeft een Stuurcomité voor het project ingesteld om te zorgen voor de nodige begeleiding en supervisie. Het Stuurcomité bestaat onder andere uit vertegenwoordigers van het Secretariaat van de Caribische Gemeenschap (CARICOM), de Caribische Telecommunicatie Unie (CTU), de Oost-Caribische Telecommunicatie Autoriteit (ECTEL), de Caribische Associatie van Nationale Telecommunicatie Organisaties (CANTO), de Caribische ICT-Virtuele Gemeenschap (CIVIC), en de Internationale Telecommunicatie Unie (ITU).

Om de inbreng van de belanghebbenden en de relevantie voor elk land te garanderen, werden ook HIPCAR-Werkgroepen geïnstalleerd bestaande uit leden die zijn aangewezen door de respectieve overheden van de landen – met inbegrip van specialisten van ICT-agentschappen, justitie en juridische zaken en andere publieke sector lichamen, nationale regelgevende instanties, nationale ICT-contactpersonen en personen verantwoordelijk voor het ontwikkelen van nationale wetgeving. Door deze brede participatie van de publieke sector uit verschillende sectoren heeft het project kunnen profiteren van een dwarsdoorsnede van standpunten en belangen. De Werkgroepen bestaan verder uit vertegenwoordigers van relevante regionale lichamen (CARICOM-Secretariaat, CTU, ECTEL en CANTO) en waarnemers van overige belanghebbende entiteiten in de regio (zoals het maatschappelijk middenveld, de particuliere sector, aanbieders van telecommunicatiediensten, de academische wereld, enz.).

De Werkgroepen waren verantwoordelijk voor het uitdiepen van de volgende twee werkgebieden:

1. *ICT-Beleidskader en Wetgevingskader voor Kwesties de Informatiemaatschappij rakende, omvattende zes deelgebieden: e-commerce (transacties en bewijs), persoonlijke levenssfeer & gegevensbescherming, aftappen van berichten, cybercriminaliteit, en toegang tot publieke informatie (vrijheid van informatie)*.
2. *ICT-Beleidskader en Wetgevingskader voor Telecommunicatie, omvattende drie deelgebieden: universele toegang/diensten, interconnectie, en vergunningenbeleid.*

De rapporten van de Werkgroepen gepubliceerd in deze documentenreeks zijn opgebouwd rond deze twee voornaamste werkgebieden.

1.3. Projectuitvoering en – inhoud

De aanzet tot de projectactiviteiten werd gegeven door middel van een rondetafelbespreking voor de lancering van het project gehouden in Grenada, van 15 tot 16 december 2008. Tot heden hebben alle begunstigde landen van het HIPCAR-project – uitgezonderd Haïti – samen met de als partners van het project optredende regionale organisaties, regelgevende instanties, aanbieders van telecommunicatiediensten, academische wereld en het maatschappelijk middenveld actief geparticipeerd in de HIPCAR-evenementen, met inbegrip van – naast de projectlancering in Grenada – regionale workshops in Trinidad & Tobago, St. Lucia, St. Kitts en Nevis, Suriname en Barbados.

De inhoudelijke activiteiten van het project staan onder leiding van teams van regionale en internationale deskundigen die samenwerken met de leden van de Werkgroepen die zich concentreren op de twee bovengenoemde werkgebieden.

Tijdens *Fase I* van het project – net afgerond – heeft HIPCAR:

1. een beoordeling gemaakt van de bestaande wetgeving van de begunstigde landen vergeleken met de internationale beste toepassing in de praktijk en in de context van harmonisatie in de gehele regio; en
2. model beleidsregels en model wetteksten opgesteld voor de bovengenoemde werkgebieden, waaruit het nationaal ICT-beleid en de nationale ICT-wetgeving/regelgeving kunnen worden ontwikkeld.

Het is de bedoeling dat deze voorstellen worden bekrachtigd of onderschreven door CARICOM/CTU en de autoriteiten van de landen in de regio als basis voor de volgende fase van het project.

Fase II van het HIPCAR-project is erop gericht begunstigde landen die daar belangstelling voor hebben assistentie te verlenen bij het omzetten van de eerder genoemde modellen in nationaal ICT-beleid en nationale ICT-wetgeving aangepast aan hun specifieke eisen, omstandigheden en prioriteiten. HIPCAR heeft fondsen gereserveerd om te kunnen inspelen op de verzoeken van de landen voor technische bijstand – met inbegrip van capaciteitsopbouw – nodig voor dit doel.

1.4. Overzicht van de zes HIPCAR-richtlijnen voor model beleid en wetteksten inzake kwesties de informatiemaatschappij rakende

Wereldwijd zijn landen, ook in het Caribisch gebied, op zoek naar manieren om wettelijke kaders te ontwikkelen voor het aanpakken van de behoeften van de informatiemaatschappij met het oog op het gebruikmaken van de groeiende aanwezigheid van het wereldwijde web als een kanaal voor de levering van diensten, ter garantie van een veilige omgeving en ter verhoging van de verwerkingskracht van informatie-systemen voor zakelijke efficiëntie en effectiviteit.

De informatiemaatschappij is gebaseerd op het uitgangspunt van toegang tot informatie en diensten en het gebruik van geautomatiseerde verwerkingssystemen ter verbetering van de levering van diensten aan markten en personen *overal in de wereld*. Voor zowel gebruikers als bedrijven biedt de informatiemaatschappij in het algemeen en de beschikbaarheid van informatie- en communicatietechnologie (ICT) unieke kansen. Terwijl de belangrijkste vereisten van de handel ongewijzigd blijven, creëert de directe overdracht van commerciële informatie mogelijkheden voor verbeterde zakelijke relaties. Dit gemak van uitwisseling van commerciële informatie brengt ook nieuwe paradigma's met zich mee: ten eerste, waar informatie wordt gebruikt om transacties met betrekking tot fysieke goederen en traditionele diensten te ondersteunen, en ten tweede, waar informatie zelf het product is dat wordt verhandeld.

De beschikbaarheid van ICT en nieuwe netwerk-gebaseerde diensten bieden een aantal voordelen voor de samenleving in het algemeen, met name voor ontwikkelingslanden. ICT-toepassingen, zoals e-overheid, e-handel, e-onderwijs, e-gezondheidszorg en e-milieu, worden gezien als faciliterend voor ontwikkeling, aangezien zij een efficiënt kanaal bieden voor de levering van een breed scala aan basisdiensten in afgelegen en landelijke gebieden. ICT-toepassingen kunnen de vervulling van de millennium ontwikkelingsdoelstellingen vergemakkelijken, armoede terugdringen en de gezondheids- en milieuomstandigheden in ontwikkelingslanden verbeteren. Onbelemmerde toegang tot informatie kan de democratie ondersteunen, als de informatiestroom buiten de controle valt van overheidsinstanties (zoals is gebeurd, bij voorbeeld in Oost-Europa). Met de juiste aanpak, context en uitvoeringsprocessen, kunnen investeringen in ICT-toepassingen en -instrumenten resulteren in productiviteit en kwaliteitsverbetering.

Echter, het transformatieproces gaat gepaard met uitdagingen aangezien het bestaande wettelijk kader niet noodzakelijk de specifieke eisen van een snel veranderende technische omgeving dekt. In gevallen waar informatie de handel in traditionele goederen en diensten ondersteunt, moet er duidelijkheid zijn in de manier waarop traditionele commerciële veronderstellingen worden toegepast, en in het geval waarin informatie het product is dat wordt verhandeld, moet de maker/ eigenaar van het product worden beschermd. In beide gevallen, moet er vastgesteld worden hoe het misdrijf aan het licht wordt gebracht, vervolgd en stopgezet in de realiteit van grensoverschrijdende transacties op basis van een immaterieel product.

De zes met elkaar verbonden model kaders

Het HIPCAR-project heeft zes (6) met elkaar verbonden model kaders ontwikkeld die een alomvattend wettelijk kader vormen voor de aanpak van de hierboven genoemde veranderende omgeving van de informatiesamenleving door het begeleiden en ondersteunen van de invoering van geharmoniseerde wetgeving in de HIPCAR begunstigde landen.

In de eerste plaats werd een juridisch kader ontwikkeld om het recht van gebruikers te beschermen in een veranderende omgeving en daarmee, naast andere aspecten, te zorgen voor vertrouwen van de consument en beleggers in rechtszekerheid en bescherming van privacy, en HIPCAR model wetteksten werden ontwikkeld om overwegingen aan te pakken met betrekking tot: **de toegang tot publieke informatie (Vrijheid van Informatie)** - gericht op het stimuleren van de juiste cultuur van transparantie in regelgeving in het voordeel van alle belanghebbenden; en **privacy en gegevensbescherming** - gericht op het waarborgen van de bescherming van de privacy en persoonlijke gegevens naar tevredenheid van het individu. Dit laatste kader is gericht op passende geheimhoudingspraktijken binnen zowel de publieke als private sector.

In de tweede plaats, werd een HIPCAR model wettekst ontwikkeld voor **elektronische handel (transacties)**, met inbegrip van elektronische handtekeningen voor het vergemakkelijken van de harmonisatie van de wetten met betrekking tot de standaardverwachtingen en rechtsgeldigheid van contract formuleringspraktijken. Dit kader is erop gericht om te voorzien in de gelijkwaardigheid van papieren en elektronische documenten en contracten en voor het leggen van een basis voor het aangaan van handel in cyberspace. Een wettekst over **Elektronische Handel (Bewijs)** - de bijbehorende tekst voor het kader voor elektronische handel (transacties) werd toegevoegd ter regulering van het wettig bewijs, in zowel civiele en criminele procedures.

Om ervoor te zorgen dat ernstige schendingen van de vertrouwelijkheid, integriteit en beschikbaarheid van ICT en de gegevens kunnen worden onderzocht door de rechtshandhaver, werden model wetteksten ontwikkeld om wetgeving te harmoniseren op het gebied van het strafrecht en het strafprocesrecht. De wetstekst inzake **cybercriminaliteit** definieert strafbare feiten, onderzoeksinstrumenten en de strafrechtelijke aansprakelijkheid van de belangrijkste actoren. Een wettekst over het aftappen **van elektronische communicatie** verschaft een passend kader dat het wederrechtelijk aftappen van communicatie verbiedt en heeft een minieme mogelijkheid geschapen zodat de rechtshandhaver in staat wordt gesteld om rechtmatig communicatie af te tappen, indien aan bepaalde duidelijk omschreven voorwaarden is voldaan.

Ontwikkelen van de model wetteksten

De model wetteksten werden ontwikkeld rekening houdend met de belangrijkste elementen van internationale trends, alsmede juridische tradities en beste praktijken uit de regio. Dit proces werd ondernomen zodat de kaders het beste beantwoorden aan de realiteit en de behoeften van de regio van HIPCAR begunstigde landen waarvoor en waarmee zij zijn ontwikkeld. Daarom was er tijdens het proces veel interactie met belanghebbenden in elk stadium van de ontwikkeling.

De eerste stap in dit complexe proces is een evaluatie van de bestaande juridische kaders binnen de regio door middel van een beoordeling van de wetgeving betreffende alle relevante gebieden. Naast uitgevaardigde wetgeving, werd in het overzicht opgenomen, indien relevant, wetsontwerpen die waren voorbereid, maar die nog niet het proces van afkondiging hadden voltooid. In een tweede stap werden de beste internationale praktijken (bijvoorbeeld van de Verenigde Naties, OESO, EU, het Gemenebest, UNCITRAL en CARICOM), alsmede geavanceerde nationale wetgeving (bijvoorbeeld uit het Verenigd Koninkrijk, Australië, Malta en Brazilië, onder andere) geïdentificeerd. Deze beste praktijken werden gebruikt als maatstaf.

Voor elk van de zes gebieden, werden complexe juridische analyses opgesteld, die de bestaande wetgeving in de regio vergeleek met deze maatstaven. Deze rechtsvergelijkende analyse leverde een momentopname van de mate van vooruitgang op belangrijke beleidsterreinen binnen de regio. Deze bevindingen waren leerzaam, en toonden aan dat er een meer geavanceerde ontwikkeling was in wetgevingskaders met betrekking tot elektronische transacties, cybercriminaliteit (of "computermisbruik") en toegang tot publieke informatie (vrijheid van informatie) dan is gebleken in de andere kaders.

Inleiding

Op basis van de resultaten van de rechtsvergelijkende analyses, hebben de regionale belanghebbenden “bouwstenen” ontwikkeld voor basisbeleid, die - zodra deze zijn goedgekeurd door de betrokken partijen - de basis bepalen voor de verdere beraadslaging over het beleid en ontwikkeling van de wettekst. Deze bouwstenen voor het beleid bevestigden een aantal gemeenschappelijke thema's en trends in de internationale precedenten, maar identificeerden ook bepaalde overwegingen die moeten worden opgenomen binnen de context van een regio die bestaat uit soevereine kleine eiland-ontwikkelingslanden. Een voorbeeld van een belangrijke overweging betreffende de situatie die de beraadslagingen beïnvloedde in deze fase en in andere fasen van het proces was de kwestie van institutionele capaciteit om adequaat beheer van deze nieuwe systemen te faciliteren.

De beleidsbouwstenen werden vervolgens gebruikt om aangepaste model wetteksten te ontwikkelen die zowel aan de internationale normen en de vraag van de HIPCAR begunstigde landen voldoen. Elke model tekst werd vervolgens opnieuw geëvalueerd door de betrokken partijen vanuit het perspectief van de levensvatbaarheid en de mogelijkheid om te worden vertaald naar de regionale context. Als zodanig, heeft de groep belanghebbenden - bestaande uit een mix van wetgevingsjuristen en beleidsdeskundigen uit de regio - teksten ontwikkeld die het beste het samenvallen van de internationale normen met lokale overwegingen weerspiegelen. Een brede betrokkenheid van vertegenwoordigers van bijna alle 15 HIPCAR begunstigde landen, regelgevers, aanbieders van telecommunicatiediensten, regionale organisaties, het maatschappelijk middenveld en de academische wereld heeft ervoor gezorgd dat de wetteksten verenigbaar zijn met de verschillende wettelijke normen in de regio. Het werd echter ook erkend dat elke begunstigde staat misschien specifieke voorkeuren heeft met betrekking tot de uitvoering van sommige bepalingen. Daarom bieden de model teksten ook een keuze in de benadering binnen de algemeenheid van een geharmoniseerd kader. Deze aanpak is gericht op het faciliteren van brede acceptatie van de documenten en het verhogen van de mogelijkheid van een tijdige uitvoering in alle begunstigde rechtsgebieden.

Interactie en het overlappen van de model teksten

Als gevolg van de aard van de kwesties die worden overwogen, weerspiegelen alle zes kaders een aantal algemene aspecten.

In eerste instantie moet aandacht worden besteed aan de kaders die zorgen voor het gebruik van elektronische middelen in communicatie en uitvoering van handel: **Elektronische handel (transacties), elektronische handel (bewijs), cybercriminaliteit** en **aftappen van communicatie**. Alle vier kaders handelen over kwesties in verband met de behandeling van berichten verzonden via telecommunicatienetwerken, de vaststelling van passende testen om de geldigheid van documenten of andere bescheiden te bepalen en de integratie van systemen gericht op de gelijke behandeling van papieren en elektronisch materiaal bij bescherming tegen onheuse behandeling, consumentenzaken en procedures voor geschillenbeslechting.

Als zodanig, zijn er verschillende gemeenschappelijke definities in deze kaders die rekening moeten houden met, waar nodig, overwegingen betreffende een uiteenlopende reikwijdte van de toepasbaarheid. Gemeenschappelijke concepten zijn onder meer: “elektronisch telecommunicatienetwerk" - wat moet worden afgestemd op de bestaande definitie van het rechtsgebied in de heersende telecommunicatiewetten; "elektronisch document" of "elektronische bescheiden" - die een brede interpretatie moeten hebben zodat bijvoorbeeld audio- en videomateriaal daaronder vallen; en "elektronische handtekeningen", "geavanceerde elektronische handtekeningen", "certificaten", "geaccrediteerde certificaten", "certificaat dienstverleners" en "certificatie-instanties" - die allemaal te maken hebben met de toepassing van encryptietechnieken voor elektronische validatie van authenticiteit en de erkenning van de technologische en economische sector, die is opgezet rond het verlenen van dergelijke diensten.

In deze context, legt **elektronische handel (transacties)**, onder andere, kernbeginselen neer van de erkenning en toekenning die nodig zijn voor de effectiviteit van de andere kaders. De nadruk ligt op het definiëren van de fundamentele beginselen die gebruikt moeten worden bij het bepalen van de gevallen van een civiele of commerciële aard. Dit kader is ook van essentieel belang bij het bepalen van een geschikte marktstructuur en een realistische strategie voor de sector toezicht in het belang van het publiek en het vertrouwen van de consument. Beslissingen over de kwesties gerelateerd aan een dergelijk administratief systeem hebben vervolgens een invloed op hoe elektronische handtekeningen procedureel worden gebruikt ten behoeve van bewijsvoering, en hoe de verantwoordelijkheden en verplichtingen in de wet gedefinieerd op de juiste manier kunnen worden toegeschreven.

Deze veronderstelling van gelijkwaardigheid geeft de overige kaders de mogelijkheid op adequate wijze om te gaan met de vertrekpunten betreffende de passende behandeling van elektronische informatieoverdracht. Het kader voor **cybercriminaliteit**, bij voorbeeld, definieert strafbare feiten met betrekking tot het aftappen van communicatie, verandering van communicatie- en computer-gerelateerde fraude. Het kader voor **elektronische handel (bewijs)** voorziet in een basis die elektronisch bewijsmateriaal introduceert als een nieuwe categorie van bewijs.

Een belangrijke rode draad die **e-transacties** en **cybercriminaliteit** aan elkaar verbindt is de vaststelling van de passende aansprakelijkheid en verantwoordelijkheid van dienstverleners van wie diensten worden gebruikt in situaties van elektronisch gepleegde misdrijven. Speciale aandacht werd besteed aan de samenhang bij het bepalen van de doelpartijen voor deze relevante delen en te zorgen voor de juiste toepassing van de verplichtingen en de handhaving daarvan.

In het geval van de kaders gericht op het verbeteren van gereglementeerd overzicht en vertrouwen van de gebruiker, behandelen de model teksten ontwikkeld door HIPCAR de twee uitersten van hetzelfde probleem: terwijl het model **toegang tot publieke informatie** de bevordering van de openbaarmaking van publieke informatie bevordert op specifieke uitzonderingen na, stimuleert het model **privacy en gegevensbescherming** de bescherming van een subset van deze informatie, die onttrokken is aan het vorige model. Belangrijk is dat beide kaders zijn gericht op het stimuleren van beter documentbeheer en archiveringspraktijken binnen de publieke sector en - in het geval van het laatstgenoemde kader - een aantal aspecten van de particuliere sector. Het is echter opmerkelijk dat - in tegenstelling tot de andere vier modelteksten - deze kaders niet uitsluitend van toepassing zijn op het elektronisch medium, noch voor het creëren van een gunstig kader waarbij overwegingen van een nieuw medium worden overgebracht naar bestaande procedures. Om te zorgen voor consistentie, zijn de kaders gericht op het reguleren van een passend beheer van informatiebronnen, in zowel elektronische en niet-elektronische vorm.

Er zijn een aantal structurele en logistieke overlappingen die bestaan tussen deze twee wettelijke kaders. Onder andere in de definitie van de belangrijkste concepten van "overheidsinstantie" (de personen op wie de kaders van toepassing zouden zijn), "informatie", "data" en "document", en de relatie tussen deze. Een andere belangrijke vorm van overlapping betreft het gepaste toezicht op deze kaders. Beide kaders vereisen de instelling van toezichthoudende instanties, die voldoende onafhankelijk van invloeden van buitenaf moeten zijn om zo het publiek te verzekeren van de integriteit van hun beslissingen. Deze onafhankelijke instanties moeten ook de capaciteit hebben om boetes en/of sancties op te leggen tegen partijen die activiteiten ondernemen om de doelstellingen van een van deze kaders te frustreren.

Conclusie

De zes HIPCAR model wetteksten voorzien de begunstigde landen van het project met een uitgebreid kader om het meest relevante gebied van regelgeving aan te pakken met betrekking tot vraagstukken van de informatiemaatschappij. In de formulering werden zowel de meest actuele internationale normen, alsook de eisen van kleine eiland-ontwikkelingslanden in het algemeen en - meer specifiek - die van de begunstigde HIPCAR-landen opgenomen. De brede betrokkenheid van de belanghebbenden uit deze

begunstigde landen in alle fasen van de ontwikkeling van de model wetteksten zorgt ervoor dat zij probleemloos en tijdig kunnen worden aangenomen. Hoewel de nadruk ligt op de behoeften van de landen in het Caribisch gebied, zijn de genoemde model wetteksten reeds geïdentificeerd als mogelijke richtsnoeren door bepaalde landen in andere regio's van de wereld.

Gezien de specifieke en nauw met elkaar verbonden aard van de HIPCAR model teksten, zal het voor de begunstigde projectlanden het voordeligst zijn wetgeving te ontwikkelen en introduceren op basis van deze modellen op een gecoördineerde wijze. De modellen voor de elektronische handel (transacties en bewijs) zullen het meest effectief functioneren in geval van gelijktijdige ontwikkeling en adoptie van de kaders voor cybercriminaliteit en aftappen van communicatie, aangezien die zo nauw verbonden en afhankelijk van elkaar zijn voor het aanpakken van de zorgpunten betreffende de ontwikkeling van een gedegen regelgeving. De kaders voor toegang tot publieke informatie en privacy en gegevensbescherming bevatten ook dergelijke synergieën in de administratieve kaders en kerncompetentie vereisten dat de gelijktijdige aanname slechts beide kaders kan versterken in de uitvoering ervan.

Op deze manier zal er een optimale mogelijkheid gecreëerd worden om de holistische kaders te benutten die zijn ingesteld in de regio.

1.5. Dit rapport

Dit rapport handelt over aftappen van communicatie, een van de werkterreinen van de Werkgroep inzake ICT-Beleidskader en Wetgevingskader voor Kwesties de Informatiemaatschappij rakende. Het omvat de Richtlijnen voor Model beleid en een Model Wettekst met Memorie van Toelichting die de landen in het Caribisch gebied zouden kunnen gebruiken wanneer zij hun eigen nationaal beleid en wetgeving op dit gebied ontwikkelen of bijwerken.

Voorafgaand aan het formuleren van dit document, heeft een team van deskundigen van HIPCAR – in nauwe samenwerking met de bovenstaande leden van de Werkgroep – een evaluatie voorbereid en beoordeeld van bestaande wetgeving in de vijftien begunstigde HIPCAR-landen in de regio die zich op zes gebieden heeft geconcentreerd: Elektronische Transacties, Elektronisch Bewijs bij e-Commerce, Bescherming van Privacy en Gegevens, Aftappen van Communicatie, Cybercriminaliteit, en Toegang tot Publieke Informatie (Vrijheid van Informatie). Deze evaluatie hield rekening met geaccepteerde internationale en regionale beste praktijken.

Deze regionale evaluatie – apart gepubliceerd als bijbehorend document voor het huidige rapport[3] – betrof een vergelijkende analyse van de huidige wetgeving met betrekking tot Elektronisch bewijs in e-handel in de begunstigde HIPCAR-landen en de identificatie van eventuele lacunes met betrekking hiertoe, waardoor de basis werd gelegd voor de ontwikkeling van een raamwerk voor model beleid en wetteksten dat hierin wordt gepresenteerd. Doordat de nationale, regionale en internationale beste toepassing in de praktijk en standaarden[4] worden weerspiegeld, terwijl tegelijkertijd de compatibiliteit met de juridische tradities in het Caribisch gebied zijn gegarandeerd, beantwoorden de model documenten in dit rapport aan de specifieke vereisten van de regio.

De model wettekst inzake aftappen van communicatie werd in drie fasen ontwikkeld: (1) het opstellen van een evaluatierapport; (2) de ontwikkeling van richtlijnen voor model beleid; en (3) het formuleren van een model wettekst. Het evaluatierapport werd voorbereid in twee fasen door HIPCAR-consultants. De eerste fase werd uitgevoerd door Mw. Karen Stephen-Dalton, en de tweede fase door dhr. Gilberto

[3] Zie "ICT-Beleidskader en Wetgevingskader voor Kwesties de Informatiemaatschappij rakende – Elektronische Transacties: Evaluatierapport inzake de huidige situatie in het Caribisch gebied" beschikbaar op www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

[4] Zoals weerspiegeld in de gereedschapskist voor Wetgeving inzake Cybercriminaliteit en het Begrijpen van Cybercriminaliteit: Een gids voor ontwikkelingslanden, de *Model Wet inzake Elektronisch Bewijsmateriaal van de Gemenebest* (LMM(02)1), Directief 2002/58/EC, en nationale benaderingen zowel binnen als buiten de regio.

Martíns de Almeida. Hierna, werden de concept richtlijnen voor model beleid voorbereid door dhr. Martíns de Almeida, en daarna bekeken, besproken en aangenomen door de HIPCAR-Werkgroep inzake Kwesties de Informatiemaatschappij rakende tijdens de eerste consultatie workshop voor bovenstaande werkgroep gehouden te Saint Lucia van 8-12 maart 2010. Op basis van de richtlijnen voor model beleid heeft de HIPCAR-consultant Dr. Marco Gercke de concept model wettekst opgesteld, die ook is bekeken, besproken en afgerond door de bovengenoemde werkgroep tijdens de tweede consultatie workshop van het project gehouden in Barbados van 23-26 augustus 2010 (zie Bijlagen). De Memorie van Toelichting bij de model wettekst is opgesteld door Dr. Gercke waarin onder andere de zaken die naar voren zijn gebracht in de tweede workshop worden behandeld. De documenten zijn aangenomen met een brede consensus tijdens deze workshops. Het HIPCAR-project stuurcomité en project managementteam heeft toezicht gehouden op het proces om deze documenten te ontwikkelen.

Volgend op dit proces werden de documenten afgerond en verspreid onder alle belanghebbenden ter overweging van de overheden van de HIPCAR begunstigde landen.

1.6. Het belang van doeltreffend beleid en doeltreffende wetgeving inzake aftappen van communicatie

In het kader van de informatiemaatschappij, waar communicatie[5] een belangrijke rol speelt, is het aftappen of het aftappen van communicatie - onder bepaalde omstandigheden - een essentieel mechanisme in de bescherming van staten en individuen.

In het licht van het feit dat de uitoefening ervan kan botsen met de privacy en andere belangrijke rechten, vereist de definitie van de criteria die het gebruik daarvan bepalen of omschrijven een goede beleidsvorming en wetgevingsformulering.

In overeenstemming met de ITU gereedschapskist voor wetgeving[6] inzake cybercriminaliteit, wordt “aftappen” gedefinieerd als "het verwerven, het bekijken, vastleggen, of het kopiëren van de inhoud of een deel daarvan van alle communicatie, met inbegrip van de inhoudelijke gegevens, computergegevens, verkeersgegevens, en/of elektronische uitzending daarvan, ook via bedrading, draadloze, elektronische, optische, magnetische, mondelinge, of op andere wijze, *tijdens de overdracht* door het gebruik van elk elektronisch, mechanisch, optisch, golf-, elektromechanisch, of ander apparaat."[7]

Een dergelijke definitie verklaart de brede reikwijdte van "aftappen", alsook van de "communicatie" eraan onderworpen, waaronder "inhoud" (de informatie meegedeeld) en "verkeer" (gegevens met betrekking tot de communicatie)[8]. Het geeft ook verschillende communicatiemiddelen aan die kunnen worden onderschept. Natuurlijk, op internet gebaseerde communicatie - en vooral cybercriminilateit - vormt een belangrijk deel van de aftapactiviteiten van een kwantitatief standpunt en qua complexiteit.

---

5 Deze uitdrukking is gedefinieerd in de Europese richtlijn 02/58/EC, in artikel 2 onder “d” als “informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronische-telecommunicatiedienst. Dit omvat niet de informatie die via een omroepdienst over een elektronische-telecommunicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt.”

6 Beschikbaar op www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf , en ontwikkeld samen met de Commissie van de Amerikaanse Advocatenvereniging *“American Bar Association’s Privacy & Computer Crime Committee”*, Afdeling Wetenschap- & Technologiewetten.

7 Artikel 1 – Definities, onder “k”.

8 Het verdrag van Boedapest beheerd door de Raad van Europa heeft “verkeersgegevens” gedefinieerd in artikel 1 onder “d”, als “computergegevens die verband houden met een met behulp van een computersysteem gevoerde communicatie die en worden voortgebracht door een computersysteem dat een onderdeel vormt van een communicatieketen en de herkomst, de bestemming, de route, de tijd, de datum, de omvang, de duur of de aard van de betrokken dienst aanduiden”; daarop zijn “computergegevens” op hun beurt gedefinieerd onder “b” van artikel1, als "iedere weergave van feiten, informatie, of begrippen in een vorm die geschikt is voor verwerking in een computersysteem, met inbegrip van een programma dat geschikt is om een computersysteem een functie te laten verrichten”. Verkeersgegevens zijn ook gedefinieerd in artikel 2 onder “b” van de Europese richtlijn 02/58/EC als “gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronische-telecommunicatienetwerk of voor de facturering ervan.”

Inleiding

Europese Directieven 02/58/EC en 06/24/EC verschaffen ook relevante inbreng om te begrijpen hoe uitgebreid het aftappen van communicatie kan zijn. De concepten "data"[9] en "locatiegegevens"[10] zijn van bijzonder belang in hierbij.

Aftappen van communicatie kan juridisch toelaatbaar en uitvoerbaar zijn. In het algemeen, bestaat legaal aftappen uit het verkrijgen van communicatiegegevens naar aanleiding van een rechtmatig mandaat ten behoeve van analyse of als bewijs. Rechtmatig mandaat op dit gebied heeft vaak betrekking op de cyberbeveiliging en bescherming van de communicatie-infrastructuur. Legaal aftappen speelt een cruciale rol om wetshandhavingsinstanties, regelgevende of administratieve instanties en inlichtingendiensten te helpen bij de bestrijding van criminaliteit, gelet op de toenemende finesse van de criminelen van vandaag. Legaal aftappen is een *onmisbaar middel om informatie te vergaren tegen de meedogenloze criminelen*.[11]

De veranderingen in de telecommunicatie- en postmarkt en de grote expansie in de aard en omvang van de beschikbare diensten in de meeste staten zijn opmerkelijk. Mobiele telefoons hebben zich ontwikkeld als een massagoed vandaag de dag, communicatie via het internet is sterk gegroeid in de afgelopen jaren en gaat nog voort, en de postsector ontwikkelt zich snel met de groei van het aantal bedrijven die pakketten en document bezorgen. Criminelen (waaronder terroristen) zijn er snel bij om deze buitengewone veranderingen in de communicatiesector voor hun criminele activiteiten uit te buiten, terwijl de wetgeving in veel landen geen gelijke tred heeft gehouden met deze veranderingen en dus het risico wordt gelopen dat de capaciteit van de rechtshandhaving, veiligheids- en inlichtingendiensten wordt aangetast.

De serieuze criminele en veiligheidsdreigingen die uitgaan naar de mondiale gemeenschap hebben er in veel landen voor gezorgd – waaronder Australie, de Verenigde Staten, het Verenigd Koninkrijk, Saint Lucia en Jamaica – dat er wetgeving is geïntroduceerd die vereist van elektronische telecommunicatiedienstverleners dat zij in staat zijn legaal aftappingen uit te voeren en die het aftappen van communicatieactiviteiten reguleert.

Om rechtmatig communicatie af te tappen moet dit worden gedaan in overeenstemming met de nationale wetten, die zowel particulier als officieel aftappen van communicatie reguleren. De rechtmatigheid van particulier aftappen van communicatie wordt beperkt tot een gelimiteerd aantal situaties waarbij, bij voorbeeld, wordt inbegrepen elektronische monitoring van personeel op de werkplek. Nationale wetten kunnen particulier aftappen van communicatie behandelen in het kader van arbeidsverhouding, het recht op privacy of anderszins.

Cloud computing, remailing technieken, cryptografie en steganografie zijn voorbeelden van technologische middelen die gebruikt kunnen worden door criminelen waardoor het moeilijk of zelfs onmogelijk wordt om communicatie af te tappen of om deze te analyseren. Daarom is het gebruik van dergelijke technologieën voor illegale doeleinden een punt van zorg.

Aan de andere kant, is het vereiste evenwicht tussen aftapverzoeken en recht op privacy een andere uitdaging waarvoor de uitvoering van het aftappen van communicatie zich geplaatst ziet, aangezien het is onderworpen aan een beoordeling van een geval tot geval, ondanks het snel toenemende volume van de orders, sommigen van hen afkomstig uit andere delen van de wereld.

9 Gedefinieerd in artikel 2 onder "a" van de Europese richtlijn 06/24/EC als "verkeers- en locatiegegevens, en de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren;"

10 Gedefinieerd in artikel 2 onder "c" van de Europese richtlijn 06/24/EC als "gegevens verwerkt in een elektronisch telecommunicatienetwerk, dat de geografische positie aanduidt van de eindgebruikersapparatuur van een publiek beschikbaar elektronische telecommunicatiedienst".

11 Aantekeningen inzake het wetsontwerp van de OECS inzake aftappen van communicatie, bladzijde 6 kan worden gevonden op www.//unpan1.un.org/intradoc/groups/public/documents/TASF/UNPAN024635.pdf

Problemen bij het uitvoeren van aftappen zijn ook geassocieerd met complex beheer. Grote hoeveelheden verzamelde gegevens en meerdere parameters voor het houden en verwijderen van opslag illustreren dat het aftappen van communicatie niet alleen een complexe juridische kwestie is, maar ook een ingewikkelde administratieve taak.

Verschillende juridische systemen en verschillende stadia van ontwikkeling en implementatie van ICT-beleid vertegenwoordigen additionele complicaties voor het harmoniseren van nationale wetgeving. Bovendien, hebben de landen ook diverse wet- en regelgevingskaders op het nationaal vlak.

Hoewel landen in het Caribisch gebied partij kunnen zijn bij regionale en internationale verdragen - en in de meeste gevallen lid zijn van de Caribische Gemeenschap - is er geen regionale soevereine macht met de bevoegdheid om wetten te maken namens hen als een groep en om naleving te waarborgen, zoals het geval is met de Europese Gemeenschap.

Neem het voorbeeld van de lidstaten van de Organisatie van Oost-Caribische Staten (OECS), de model wet inzake aftappen van communicatie opgesteld door de OECS wetgevingsfaciliteit in 2003 werd in datzelfde jaar goedgekeurd door de Commissie Juridische Zaken - die bestaat uit de Advocaten-Generaal (die rechtstreeks verantwoordelijk zijn voor de uitvoering van het beleid inzake aftappen) - voor bekrachtiging in alle OECS lidstaten. Echter, tot op heden, heeft slechts Saint Lucia in de OECS een Wet inzake aftappen van communicatie uitgevaardigd (gevolgd door een soortgelijke wet in Jamaica).

Voor verdere informatie betreffende de uitdagingen waarvoor men zich geplaatst ziet bij de ontwikkeling van beleid en wetgeving die betrekking heeft op aftappen van communicatie worden hoofdstukken 3.2 en 3.3 van “Understanding Cybercrime: a Guide for Developing Countries”[12] (Cybercriminaliteit uit de doeken gedaan: een gids voor ontwikkelingslanden) aanbevolen.

[12] Beschikbaar van www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf.

Deel I:
Richtlijnen voor model beleid – aftappen van communicatie

Hieronder volgen de richtlijnen voor model beleid die een land kan overwegen met betrekking tot aftappen van communicatie.

1. CARICOM/CARIFORUM-LANDEN ZULLEN ZICH EROP RICHTEN OM DE NODIGE GEZAMENLIJKE INTERPRETATIES VAST TE STELLEN VOOR SLEUTELBEGRIPPEN DIE WORDEN GEASSOCIEERD MET AFTAPPEN VAN COMMUNICATIE

- Er zal een passende definitie zijn van “aftappen”, “communicatie”, “gegevens”, “inhoud”, “verkeer”, “inhoudelijke gegevens”, “verkeersgegevens”, “locatiegegevens”.
- Er zal een voldoende ruime formulering van de definitie van deze termen zijn gekoppeld aan een lijst van illustratieve voorbeelden.
- Er zal een duidelijke definitie zijn van de soort informatie (tekst, visueel, geluid) en de reikwijdte van media onderhevig aan het aftappen van communicatie, zodat daarbij zijn inbegrepen elektronische en niet-elektronische documenten, bandopnamen, films, geluidsopnamen, beelden, enzovoort, geproduceerd door een overheids- of een particuliere partij, op enig moment.
- Voor zover verenigbaar met de zorgpunten van nationale veiligheid, wordt er een publiekscampagne gevoerd die gericht is op het ontwikkelen van bewustzijn over communicatie onderhevig aan aftappen, en het verklaren van overheidsbeleid die dit rechtvaardigen en behandelen.

2. CARICOM/CARIFORUM-LANDEN ZULLEN HET VASTSTELLEN VAN HET NODIGE RAAMWERK NASTREVEN OM DE PUBLIEKE OF PARTICULIERE OORSPRONG EN DE ROL VAN DE PARTIJEN TE DEFINIEREN DIE VERANTWOORDELIJK ZIJN VOOR HET BEHEER VAN HET AFTAPPEN VAN COMMUNICATIE[13]

- Er moeten bepalingen worden neergelegd bij wet waarin expliciet wordt bepaald wat de rol is van "de overheid" (zoals rechtshandhavingsagentschappen) en van "particuliere instanties" (zoals internetproviders en telecommunicatiebedrijven) in het kader van het aftappen van communicatie.
- Er zal een bepaling zijn die vaststelt dat van particuliere instanties wordt verwacht dat zij samenwerken met de overheid bij het aftappen van communicatie zoals bepaald in de toepasselijke wetgeving (procedurele strafrechtelijke wetten, nationale veiligheidswetten), in de mate toegestaan door de wet.
- Er zal regelgeving zijn welke ruimte biedt voor de erkenning en integratie van algemeen aanvaarde technische standaarden die elektronische en/ of telefonische monitoring behandelen, en die behulpzaam zijn bij het aftappen van communicatie.

[13] Er zal een overheidsbeleid zijn dat institutionele samenwerking aanmoedigt (bij voorbeeld, met de industrie en handel) voor de ontwikkeling of het gebruik, waar nodig (en zover als nodig, het delen) van databanken en andere mechanismen of opslag of publicatie van gegevens die relevant zijn voor het bereiken van de doelstellingen van aftappen van communicatie.
Er zal constante monitoring plaatsvinden betreffende nieuwe uitdagingen bij het aftappen van communicatie (zoals steganografie, cloud computing, enzovoort).

- Er zal een overheidsbeleid zijn voor het harmoniseren van het aftappen van communicatie en het recht of privacy, vrijheid van informatie, intellectuele eigendom, en ander overheidsbeleid die te maken hebben met het bevorderen van productie, het houden en vrijgeven van informatie.
- Er zullen formele criteria worden vastgesteld over hoe verzoeken en gerechtelijke bevelen worden behandeld en voor het aftappen van communicatie die afkomstig zijn uit het buitenland.
- Er zullen formele criteria worden vastgesteld en training voor het uitvoeren van aftappen van communicatie op een wijze zodat het als elektronisch bewijsmateriaal kan worden geaccepteerd.

3. CARICOM/CARIFORUM-LANDEN ZULLEN DE WETTELIJKE MANDATEN EN NORMEN VASTSTELLEN WAARAAN AFTAPPEN VAN COMMUNICATIE ONDERWORPEN IS

- De wet moet faciliterend zijn van aard en de bepalingen dienen niet al te dicterend te zijn.
- De wet zal vastleggen dat communicatie slechts zal worden onderschept indien er een publiek belang mee is gemoeid, en indien het wordt gedaan in overeenstemming met wettelijke procedures, normen en praktijken.
- De wet /het wettelijk mandaat zal definiëren wat de constitutionele gronden zijn voor aftappen van communicatie om het gewicht daarvan te kunnen vaststellen in vergelijking met andere constitutionele rechten of beginselen.
- De wet /het wettelijk mandaat zal criteria neerleggen die de selectie moeten sturen van elektronische zoekopdrachten van af te tappen communicatie.
- De wet /het wettelijk mandaat zal vaststellen wat de aanvaardbare patronen zijn voor de implementatie van het aftappen van communicatie, waarbij rekening wordt gehouden met de duur van de zoekopdracht, reikwijdte van de zoekopdracht, filtermechanismen, de maximale tijd voor het bewaren van onderschepte communicatie, veiligheid bij het opslaan van onderschepte communicatie, het op de juiste wijze wegdoen daarvan en andere procedures.
- De wet /het wettelijk mandaat kan verschillende behandeling vaststellen voor inhoudelijke gegevens, verkeersgegevens en locatiegegevens.
- De wet /het wettelijk mandaat zal vaststellen dat het beheer van het aftappen van communicatie wordt geleid door de doelstellingen van naleving van juridische beginselen, doeltreffendheid, doelmatigheid en het naspeuren van bescheiden.
- De wet /het wettelijk mandaat kan vaststellen welke communicatie (zoals terrorisme, contraspionage) onderhevig zal zijn aan speciale aftapprocedures en administratieve structuren.

4. CARICOM/CARIFORUM-LANDEN ZULLEN UITZONDERINGEN VASTSTELLEN VOOR HET NALEVEN VAN AFTAPPEN VAN COMMUNICATIE

- De wet zal uitzonderingen neerleggen die duidelijk en zorgvuldig zijn afgebakend, zodat breed opgezette uitzonderingen worden vermeden, die de doelstellingen van aftappen van communicatie zou kunnen te niet doen.
- De wet zal vaststellen dat communicatie (zoals bank, medisch en anderszins) worden vrijgesteld van aftappen, tenzij er een gerechtelijk bevel is dat een volmacht verleend voor aftappen.
- De wet zal bewustzijn ontwikkelen met betrekking tot criteria die het aftappen van communicatie en andere soorten geheimen (bank, belasting, post, professioneel, gerechtelijk en anderszins) harmoniseren.

- De wet zal aangeven dat waar het publiek belang om een communicatie geheim te houden groter is dan het publiek belang van het aftappen daarvan, het aftappen zal worden verondersteld niet toegestaan te zijn.
- De wet zal vaststellen dat aftappen van communicatie in overeenstemming is met het overheidsbeleid inzake de vrijheid om communicatie te coderen (en om andere middelen te gebruiken om de weg die de communicatie aflegt, zoals remailing, te verhullen).

5. CARICOM/CARIFORUM-LANDEN ZULLEN PROCEDURES VASTSTELLEN VOOR HET TOEZICHT OP, DE NALEVING VAN, HET HERZIEN VAN EN HET BEROEP AANTEKENEN MET BETREKKING TOT het AFTAPPEN VAN COMMUNICATIE

- De wet /het wettelijk mandaat zal procedures neerleggen voor het toezicht op, de naleving van, het herzien van en het beroep aantekenen met betrekking tot het aftappen van communicatie.
- De wet /het wettelijk mandaat zal vaststellen dat zowel de verzoeker als de overheidsinstantie het recht zullen hebben beroep aan te tekenen bij de rechter tegen de beslissingen van een administratief lichaam.
- De wet /het wettelijk mandaat zal een tijdlijn vaststellen, zodat de reactie op een verzoek en de verstrekking van informatie niet op onredelijke wijze worden vertraagd.
- De wet /het wettelijk mandaat zal sancties neerleggen voor het niet naleven van de rechten en verplichtingen die verband houden met het aftappen van communicatie.

6. CARICOM/CARIFORUM-LANDEN ZULLEN EEN KADER VASTSTELLEN VOOR HET AFTAPPEN VAN COMMUNICATIE IN SAMENHANG MET OVERHEIDSBELEID INZAKE AANVERWANTE ZAKEN

- De wet /het wettelijk mandaat zal het aftappen van communicatie reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake nationale veiligheid.
- De wet /het wettelijk mandaat zal het aftappen van communicatie reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake cybercriminaliteit.
- De wet /het wettelijk mandaat zal het aftappen van communicatie reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake vrijheid van informatie.
- De wet /het wettelijk mandaat zal het aftappen van communicatie reguleren op een wijze die consistent is met het overheidsbeleid inzake privacy en gegevensbescherming.
- De wet /het wettelijk mandaat zal het aftappen van communicatie reguleren op een wijze die in overeenstemming is met het relevante overheidsbeleid inzake censuur.
- De wet /het wettelijk mandaat zal het aftappen van communicatie reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake informatiebeveiliging.
- De wet /het wettelijk mandaat zal het aftappen van communicatie reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake intellectuele eigendom.
- De wet /het wettelijk mandaat zal het aftappen van communicatie reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake de zendvrijheid.
- De wet /het wettelijk mandaat zal het aftappen van communicatie reguleren op een wijze die in overeenstemming is met het overheidsbeleid op *habeas data,* waar van toepassing.

Deel II:
Model wettekst –
aftappen van communicatie

Onderstaand volgt een model wettekst die een land in overweging kan nemen bij de ontwikkeling van nationale wetgeving die betrekking heeft op aftappen van communicatie. Deze model tekst is gebaseerd op de richtlijnen voor model beleid hierboven aangegeven.

Indeling van de artikelen

Deel II

Deel II

HOOFDSTUK I – INLEIDING

Citeertitel

1. Deze wet wordt aangehaald als de "Wet inzake aftappen van Communicatie", en wordt van kracht en treedt in werking [op xxx/ na publicatie in het Staatsblad].

Doelstelling

2. [Dit is een wet voor de ontwikkeling van een wettelijk kader voor het legaal aftappen van communicatie en voor het beschermen en behouden van het recht op anonimiteit, codering en geheimhouding van communicatie].

Definities

3. (1) Agentschap: een [aftappeninstantie] of [ander handhavingslichaam].

(2) Gemachtigde officier:

a. de [commissaris van politie];

b. de [directeur van de financiele inlichtingendienst];

c. een persoon die voorlopig legaal de functies vervult van een persoon aangehaald in leden (a) of (b);

d. een persoon schriftelijk bevoegd te handelen namens een persoon aangehaald in de leden (a, (b) of (c).

(3) Communicatiemiddelen

a. alles waaronder spraak, muziek, geluid, visuele beelden of data van welke omschrijving dan ook, waaronder inhoudelijke gegevens, computergegevens, verkeersgegevens, en/ of elektronische uitzending daarvan; of

b. signalen dienende voor het doorgeven van iets tussen personen, tussen een persoon en een ding, of tussen dingen of voor het activeren of beheersen van enig apparaat,

overgebracht via een elektronisch telecommunicatienetwerk of een deel daarvan met het gebruik van enig elektronisch, mechanisch, optisch golf-, elektromechanisch of ander apparaat.

(4) Aanbieder van telecommunicatiediensten: een persoon die een telecommunicatienetwerk beheert of die een telecommunicatiedienst verleent aan meer dan [aantal] klanten.

(5) Telecommunicatienetwerk: een faciliteit of infrastructuur gebruikt door een persoon voor het verlenen van telecommunicatiediensten en waarbij is inbegrepen een netwerk waarmee een persoon communicatie kan verzenden of ontvangen van of naar –

a. elke plek in de staat;

b. elke plek buiten de staat.

(6) Telecommunicatiedienst: een dienst verleend door middel van een telecommunicatienetwerk, ongeacht of die wel of niet wordt beheert door de persoon die de dienst verleent.

(7) Aangewezen persoon: de [Minister] of enige persoon voorgeschreven voor de doelstellingen van deze wet door de [Minister] krachtens een besluit gepubliceerd in het [naam van de publicatie] afhankelijk van parlementaire? bekrachtiging.

(8) Bevel tot openbaarmaking: een bevel uitgevaardigd krachtens artikel 30 waarmee toegang tot opgeslagen communicatiegegevens wordt geëist.

(9) Aftappen: het verwerven, bekijken, vastleggen, monitoren of kopieren van de inhoud of een deel daarvan, van elke communicatie tijdens transmissie door het gebruik van een aftapapparaat of -methode.

(10) Onderschepte communicatie: elke communicatie die is onderschept tijdens de verzending.

(11) Aftapapparaat: een elektronisch, mechanisch, optisch, golf-, elektromechanisch, instrument, apparatuur of apparaat dat wordt gebruikt, of kan worden gebruikt, ongeacht of dat op zichzelf is of in combinatie met enig ander instrument, apparatuur, programma of apparaat voor het aftappen van communicatie, maar het betekent niet enig instrument, apparatuur of apparaat of enig onderdeel daarvan:

a. verstrekt aan een klant door een aanbieder van telecommunicatiediensten in de normale gang van zaken en gebruikt door de klant bij de normale uitoefening van zijn of haar bedrijf;

b. verstrekt door een klant voor de aansluiting op de faciliteiten van dergelijke telecommunicatiedienst en gebruikt door de klant bij de normale uitoefening van zijn bedrijf; of

c. gebruikt door een aanbieder van telecommunicatiediensten in de normale uitoefening van zijn bedrijf.

(12) Bevel tot aftappen: een machtiging uitgegeven krachtens artikel 8.

(13) Beschermde* apparatuur: apparatuur waarvan is afgekondigd dat het beschermde* apparatuur is krachtens artikel 25, en daarbij is inbegrepen elke onderdeel van dergelijke apparatuur.

(14) Minister: de [Minister] [naam van het ministerie].

[(15) Persoon omvat een lichaam met rechtspersoonlijkheid of een lichaam zonder rechtspersoonlijkheid.].

(16) Opgeslagen communicatiegegevens: communicatie die of nog niet is begonnen, of is afgelopen, en verlopen is via een communicatiesysteem.

Toepassing 4. (1) Niets in deze wet zal worden geïnterpreteerd op dusdanige wijze dat het de anonimiteit of codering van communicatie vereist of verbied.

(2) Deze wet is niet van toepassing indien aftappen van communicatie is voorzien krachtens enige andere wet in [Staat].

HOOFDSTUK II – AFTAPPEN VAN COMMUNICATIE

Verbod op aftappen van communicatie 5. (1) Een persoon die met opzet enige communicatie onderschept tijdens de verzending daarvan pleegt een overtreding die strafbaar is bij veroordeling met een boete niet meer dan [bedrag], of met een gevangenisstraf voor een duur niet langer dan [periode], of met beiden.

(2) Een persoon pleegt geen overtreding krachtens lid (1), indien:

a. De communicatie werd onderschept in overeenstemming met een bevel tot aftappen uitgegeven krachtens artikel 8 door een [rechter];

b. Behoudens lid (3), heeft die persoon redelijke gronden te geloven dat de persoon aan wie of van wie die communicatie wordt verzonden instemt met het aftappen;

c. De communicatie opgeslagen communicatiegegevens zijn en is verworven in overeenstemming met de bepalingen van enige andere wet;

d. De communicatie wordt onderschept als een gewoon incident bij de levering van telecommunicatiediensten of bij de handhaving van enige wet die betrekking heeft op het gebruik van die diensten;

e. Het aftappen wordt gemaakt van een communicatie die is gedaan door een telecommunicatienetwerk dat is opgezet voor het gemakkelijk toegang geven tot de communicatie voor het algemeen publiek; of

f. het aftappen van een communicatie is verzonden en verstuurd binnen een intern netwerk dat wordt gebruikt om de behoeften van een bedrijf of huishouden te dienen en wordt uitgevoerd door een persoon die:

   i. het recht heeft de bediening of het gebruik van het netwerk te beheersen; of

   ii. uitdrukkelijk of stilzwijgend toestemming heeft van een persoon waarnaar wordt verwezen in lid f onder (i).

(3) Een persoon pleegt geen overtreding krachtens lid (1) indien:

a. De communicatie is verstuurd of bestemd voor een persoon die heeft ingestemd met het aftappen; en

b. een bevoegde officier gelooft dat het aftappen van communicatie nodig is met als gevolg van een noodsituatie, het voorkomen van een dood of ongeval, of om enige schade aan de fysieke of mentale gezondheid van een persoon te beperken of in het belang van de nationale veiligheid.

Opmerking: Een land kan de strafbaarstelling beperken door aanvullende eisen te stellen.

Aanvraag van bevel tot aftappen

6. (1) Een [bevoegde officier] [Procureur-Generaal namens een bevoegde officier] kan *ex parte* bij de [rechter] een aanvraag indienen voor een bevel tot aftappen van communicatie in ieder geval waar er redelijke aanwijzingen zijn om te geloven dat aan de voorwaarden waarnaar wordt verwezen in lid 1 van artikel 8 wordt voldaan.

(2) Behoudens artikel 14, moet de aanvraag voor een bevel tot aftappen schriftelijk worden gedaan en vergezeld zijn van een beëdigde verklaring waarin het volgende staat:

a. De naam van de bevoegde officier [namens wie de aanvraag wordt gedaan];

b. Feiten en andere gronden op basis waarvan de aanvraag wordt gedaan;

c. De periode waarvoor het bevel van kracht zal zijn en waarom het noodzakelijk wordt geacht dat het bevel tijdens die periode van kracht is;

d. Voldoende informatie voor een [rechter] voor het uitvaardigen van een bevel tot aftappen op basis van de voorwaarden neergelegd in lid (1) van artikel 8;

e. De gronden waarnaar verwezen wordt in lid (1) van artikel 8 op basis waarvan de aanvraag wordt gedaan;

f. De volledige bijzonderheden van alle feiten en omstandigheden die worden verondersteld door de bevoegde officier namens wie de aanvraag wordt gedaan, waaronder;

   i. indien praktisch, een beschrijving van de aard en locatie van de faciliteiten van waar, of de panden en erven waar de communicatie onderschept dient te worden; en

   ii. de basis om aan te nemen dat het bewijs met betrekking tot de grond waarop de aanvraag is ingediend zal worden verkregen door het aftappen;

g. Indien van toepassing, of andere onderzoeksprocedures zijn toegepast en het noodzakelijke bewijsmateriaal hebben opgeleverd of de reden waarom andere onderzoeksprocedures die redelijkerwijze onwaarschijnlijk lijken succes te zullen hebben indien toegepast, of waarschijnlijk te gevaarlijk zullen zijn om toe te passen voor het verkrijgen van het gewenste bewijsmateriaal;

h. Of enige vorige aanvraag die is gedaan voor het uitvaardigen van een bevel tot aftappen met betrekking tot dezelfde persoon, dezelfde faciliteit of dezelfde panden en erven omschreven in de aanvraag, en indien dergelijke voorgaande aanvraag bestaat, zal de huidige status van die aanvraag worden aangegeven;

i. Alle andere instructies door de [rechter] uitgevaardigd.

(3) Waar een bevel tot aftappen wordt aangevraagd op basis van nationale veiligheid, zal de aanvraag vergezeld gaan van een schriftelijke machtiging getekend door de [Minister].

(4) Behoudens lid (5), zullen de bescheiden die betrekking hebben op een bevel tot aftappen of de vernieuwing of wijziging daarvan;

a. in een verzegeld pakket worden gedaan door de [rechter] aan wie de aanvraag is gericht direct na de vaststelling van de aanvraag; en

b. in bewaring worden gehouden door de rechter in een plaats die niet toegankelijk is voor het publiek of in een plaats op instructie van de [rechter].

(5) De bescheiden waarnaar wordt verwezen in lid (5) kunnen worden geopend indien de [rechter] het beveelt en slechts

a. met als doel het behandelen van een aanvraag voor verdere machtiging; of

b. voor vernieuwing van de machtiging; tenzij anders geïnstrueerd door de rechter.

(6) Een persoon die in een aanvraag of beëdigde verklaring krachtens deze wet een verklaring doet waarvan hij weet dat die onwaar is met betrekking tot enig materieel feit begaat een overtreding en kan veroordeeld worden bij kort geding tot een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

Openbaarmaking aanvraag

7. (1) Elke persoon die het bestaan van een aanvraag voor een bevel tot aftappen openbaar maakt, met uitzondering van de bevoegde officier, begaat een overtreding die strafbaar is, bij veroordeling, met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

(2) Het zal een verdediging zijn in enig proces tegen een persoon om aan te tonen

a. dat de openbaarmaking werd gedaan bij een advocaat met als doel het inwinnen van juridisch advies;

b. dat de persoon aan wie, of afhankelijk van het geval, door wie de openbaarmaking waarnaar wordt verwezen onder lid (1) werd gedaan, de cliënt was of een vertegenwoordiger van de cliënt.

(3) Het zal een verdediging zijn in een proces tegen een persoon voor een overtreding onder lid (1) om aan te tonen dat de openbaarmaking werd gedaan door een advocaat;

a. in de planning van, of in relatie tot een juridisch proces; en

b. voor de doelstellingen van het proces.

(4) Lid (2) of lid (3) zal niet van toepassing zijn in het geval van een openbaarmaking gedaan in een strafrechtelijk proces.

(5) In een proces tegen een persoon voor een overtreding onder dit lid (1), zal het een verdediging voor die persoon zijn om aan te tonen dat de openbaarmaking beperkt was tot een openbaarmaking toegestaan door een bevoegde officier.

Het uitvaardigen van het bevel tot aftappen

8. (1) Een [rechter] zal machtiging geven tot aftappen en een bevel tot aftappen uitvaardigen indien hij of zij ervan overtuigd is dat:

a. het bevel tot aftappen noodzakelijk is

   i. in het belang van nationale veiligheid; of

   ii. ter voorkoming of ter opsporing van enige overtreding die is neergelegd in de bijlage, indien er redelijke gronden zijn om te geloven dat een dergelijke overtreding is, wordt of kan worden gepleegd; of

   iii. met als doel, in de omstandigheden die voor de [rechter] gelijkaardig lijken aan die waarin hij of zij een bevel tot aftappen zou uitvaardigen krachtens lid a onder (ii) om uitvoering te geven aan bepalingen van enige overeenkomst of wet inzake wederzijdse rechtsbijstand;

b. informatie verkregen van het aftappen zeer waarschijnlijk zullen helpen bij onderzoek met betrekking tot enige zaak die wordt genoemd in lid (a), en

c. andere procedures:

i. niet of niet waarschijnlijk succesvol zullen zijn in het verkrijgen van de informatie waarvan men denkt die te verkrijgen door middel van het bevel tot aftappen;

ii. te gevaarlijk zijn om in deze omstandigheden te gebruiken, of

iii. die gezien het spoedeisend karakter van de zaak niet praktisch lijken te zijn;

en

d. het in het belang is voor de rechtsbedeling om het bevel tot aftappen uit te vaardigen.

(2) Een [rechter] die een aanvraag voor een bevel tot aftappen in overweging heeft kan eisen van een bevoegde officier dat die verdere informatie verschaft in verband met de aanvraag naar gelang hij of zij dat nodig acht.

Reikwijdte en vorm van het bevel tot aftappen

9. (1) Een bevel tot aftappen wordt schriftelijk uitgevaardigd en zal toestaan dat de bevoegde officier:

a. communicatie onderschept tijdens de verzending;

b. een aanbieder van telecommunicatiediensten kan gebieden communicatie af te tappen tijdens de verzending;

c. het aftappen kan uitvoeren door middel van een telecommunicatienetwerk of telecommunicatiedienstverleners zoals beschreven in het bevel tot aftappen;

d. de onderschepte communicatie openbaar maakt die is verkregen of vereist door het bevel tot aftappen aan die personen en op dusdanige wijze als neergelegd in het bevel tot aftappen.

(2) Een bevel tot aftappen zal het aftappen toestaan van:

a. communicatie die wordt verzonden door telecommunicatienetwerken of aanbieders naar of van:

i. een bepaald individu gespecificeerd in het bevel tot aftappen;

ii. een bepaald adres gespecificeerd in het bevel tot aftappen;

b. communicatie verzonden door telecommunicatienetwerken of aanbieders van een bepaalde verbinding gespecificeerd in het bevel tot aftappen;

c. iedere andere communicatie, indien van toepassing, zoals nodig mocht blijken voor het aftappen van communicatie die valt onder lid (a).

(3) Een bevel tot aftappen kan de toegang machtigen tot panden en erven gespecificeerd in het bevelschrift zoals beschreven in artikel 18 voor het installeren, onderhouden, gebruiken of terughalen van alle apparatuur die is gebruikt voor het aftappen van communicatie gespecificeerd in het bevelschrift.

(4) Een bevel tot aftappen zal:

a. de identiteit specificeren van de bevoegde officier namens wie de aanvraag is gedaan;

b. de persoon identificeren die het bevel tot aftappen zal uitvoeren;

c. de aanbieder van telecommunicatiediensten identificeren aan wie het bevel tot aftappen geaddresseerd zou moeten zijn en moeten specificeren of de aanbieder van telecommunicatiediensten geautoriseerd is om communicatie af te tappen, indien van toepassing; en

d. wanneer een bevel tot aftappen de toegang tot panden en erven toestaat krachtens lid (3),

   i. moet het specificeren of de toegang is geautoriseerd op elk tijdstip van de dag of nacht of slechts tijdens specifieke uren;

   ii. kan het bijkomende maatregelen specificeren die genomen moeten worden voor het garanderen en uitoefenen van de toegang tot de panden en erven.

(5) Een bevel tot aftappen kan hulpbepalingen bevatten die nodig zijn om te verzekeren dat het wordt uitgevoerd in overeenstemming met deze wet.

(6) Een bevel tot aftappen kan voorwaarden specificeren of beperkingen die verband houden met het aftappen van communicatie die daarin wordt toegestaan.

Opmerking: Landen kunnen – afhankelijk van hun rechtstradities – bijkomende procedurele waarborgen vereisen.

(7) Voor het doeleinde van dit artikel omvat "adres" de panden en erven, het emailadres, telefoonnummer of enig nummer of aanwijzing gebruikt met als doel het identificeren van telecommunicatienetwerken, aanbieders of apparatuur.

Duur en vernieuwing van bevel tot aftappen

10. (1) Een bevel tot aftappen zal geldig zijn voor een duur, niet meer dan [90] dagen, zoals de [rechter] zal specificeren in het bevelschrift, maar kan op elk moment vernieuwd worden voor het aflopen van die periode, met betrekking tot een aanvraag gedaan ingevolge leden (3) en (4).

(2) Een [rechter] kan, met betrekking tot een aanvraag voor vernieuwing van een bevel tot aftappen gedaan door een [bevoegde officier] [*leidinggevende van het Openbaar Ministerie* namens een bevoegde officier] op enig moment voordat het bevelschrift (of enige geldende vernieuwing van het bevel tot aftappen) komt te vervallen, deze vernieuwen.

(3) Een aanvraag voor vernieuwing van een bevel tot aftappen onder lid (2) dient schriftelijk te worden gedaan en zal worden vergezeld van een beëdigde verklaring waarin wordt getuigd wat de omstandigheden zijn die de vernieuwing van het bevel tot aftappen rechtvaardigen.

(4) Iedere aanvraag voor de vernieuwing van een bevel tot aftappen zal worden gedaan op de wijze voorzien in artikel 6 en geeft:

a. de reden en de periode waarin de vernieuwing wordt vereist; en

b. de volledige bijzonderheden samen met de tijdstippen en data van alle aftappingen gedaan of geprobeerd onder het bevelschrift, en een verwijzing naar de aard van de informatie die is verkregen bij elke aftapping.

(5) Elke aanvraag voor vernieuwing van het bevel tot aftappen zal worden ondersteund door zulke andere informatie die de [rechter] kan vereisen.

(6) Een vernieuwing van een bevel tot aftappen kan worden verleend krachtens dit artikel indien de [rechter] ervan is overtuigd dat de omstandigheden waarnaar wordt verwezen in lid (1) van artikel 8 nog steeds gelden.

(7) Elke vernieuwing van een bevel tot aftappen zal slechts geldig zijn voor een periode niet langer dan [*90*] dagen, zoals de [rechter] zal specificeren in de vernieuwing.

(8) Indien op enig moment voor het eind van de periode waarnaar wordt verwezen in lid (1) en (7) van artikel 10 blijkt volgens de bevoegde officier aan wie het bevelschrift is uitgevaardigd, of een persoon die namens hem of haar handelt, dat een bevel tot aftappen niet langer noodzakelijk is, zal hij of zij een aanvraag indienen bij [de rechter] voor het herroepen van het bevel tot aftappen.

Wijziging van bevel tot aftappen

11. (1) Een [rechter] kan alle bepalingen van een bevel tot aftappen wijzigen op om het even welk moment, na de [*bevoegde officier/leidinggevende van het Openbaar Ministerie* handelend namens een bevoegde officier] te hebben gehoord en indien hij of zij overtuigd is dat er een wijziging is in de omstandigheden die de gevraagde wijzigingen noodzakelijk maken of opportuun.

(2) Een aanvraag voor wijziging van het bevel tot aftappen zal worden gedaan in overeenstemming met artikel 6 en zal de informatie bevatten waarnaar wordt verwezen onder lid (2) van artikel 6.

Herroepingvan het bevel tot aftappen

12. (1) Een [rechter] die een bevel tot aftappen heeft uitgevaardigd [of, indien hij of zij niet beschikbaar is, elke andere [rechter] die bevoegd is een dergelijk bevelschrift uit te vaardigen] kan het bevel tot aftappen herroepen, indien

a. de bevoegde officier er niet in slaagt een rapport in te dienen in overeenstemming met artikel 15, indien van toepassing; of
b. de [rechter] bij ontvangst van een rapport ingediend krachtens artikel 15 ervan is overtuigd dat de doelstellingen van het bevel tot aftappen zijn bereikt; of
c. de gronden waarop het bevel tot aftappen was uitgevaardigd niet langer geldig zijn; of
d. de voorwaarden van de toepassing waarnaar wordt verwezen in lid (1) van artikel 8 gewijzigd zijn op dusdanige wijze dat een aanvraag niet meer mogelijk zou zijn.

(2) Wanneer een [rechter] een bevel tot aftappen herroept ingevolge lid (1), zal hij of zij direct schriftelijk de bevoegde officier in kennis stellen van de herroeping.

(3) Indien het bevel tot aftappen wordt herroepen, zal een bevoegde officier, zo snel als mogelijk, na in kennis te zijn gesteld van de herroeping, alle aftapapparatuur, die was geïnstalleerd krachtens lid (3) van artikel 9, verwijderen of laten verwijderen uit de panden en erven waarop het bevel tot aftappen betrekking had krachtens hetzelfde lid.

Gevolgen van een herroeping

13. In het geval dat een bevel tot aftappen dat werd uitgevaardigd in overeenstemming met deze wet wordt herroepen krachtens artikel 12 zal de inhoud van alle communicatie die is onderschept onder dat bevel tot aftappen niet toelaatbaar zijn als bewijsmateriaal in enig strafrechtelijk proces of civiel proces dat mocht worden beoogd, tenzij de rechter van mening is dat het toelaten van dergelijk bewijsmateriaal het proces niet onrechtvaardig maakt of anderszins nadelig is voor de rechtsbedeling.

Spoedaanvraag

14. (1) Wanneer een rechter is overtuigd dat de urgentie van de omstandigheden het vereist –

a. Kan hij of zij ontheffing verlenen met betrekking tot de vereisten van een schriftelijke aanvraag en een beëdigde verklaring en overgaan tot het horen van een mondelinge aanvraag voor een bevel tot aftappen; en

b. Zal indien hij is overtuigd dat een bevel tot aftappen noodzakelijk is een bevel tot aftappen uitvaardigen in overeenstemming met deze wet.

(2) Een aanvraag volgens lid (1) onder (a) moet

a. de informatie bevatten waarnaar wordt verwezen in lid (2) van artikel 6;

b. de bijzonderheden van de urgentie in dit geval aangeven of de andere uitzonderlijke omstandigheden, die naar mening van de bevoegde officier het doen van een mondelinge aanvraag rechtvaardigen.

(3) Een [rechter] kan, op een mondelinge aanvraag die bij hem of haar is gedaan, een bevel tot aftappen uitvaardigen, indien hij of zij ervan overtuigd is dat

a. er redelijke gronden zijn om te geloven dat het bevel tot aftappen zal worden uitgevaardigd; en

b. het niet redelijkerwijs mogelijk is gezien de urgentie van het geval of het bestaan van exceptionele omstandigheden voor de [bevoegde officier] [leidinggevende van het Openbaar Ministerie die namens de bevoegde officier de aanvraag doet] om een schriftelijke aanvraag te doen voor het uitvaardigen van het bevel tot aftappen, waarvoor men de aanvraag doet.

(4) In het geval dat de [rechter] de aanvraag voor een nood bevel tot aftappen toewijst, zal de [rechter] direct een schriftelijke aantekening maken waarin de bijzonderheden van de aanvraag worden vastgelegd. De [rechter] zal ook een aantekening maken van de voorwaarden van het bevelschrift.

(5) Een bevel tot aftappen dat is uitgevaardigd naar aanleiding van de mondelinge aanvraag dient dezelfde reikwijdte te hebben als aangegeven in artikel 9.

(6) Elk nood bevel tot aftappen zal geldig zijn voor [*48*] uren vanaf het moment dat het wordt verleend, en zal dan komen te vervallen.

(7) In het geval dat een bevel tot aftappen wordt uitgevaardigd onder dit artikel, zal de [bevoegde officier] *[leidinggevende van het Openbaar Ministerie* namens de bevoegde officier] binnen [*48*] uur te rekenen

vanaf de uitvaardiging een schriftelijke aanvraag en beëdigde verklaring indienen bij de [rechter] in overeenstemming met de bepalingen van artikel 6.

(8) Na het verstrijken van [*48*] uren na het moment van uitvaardiging van het bevel tot aftappen; zal de [rechter] krachtens dit artikel zijn of haar beslissing inzake het verlenen van het bevel tot aftappen heroverwegen.

(9) Bij de heroverweging van zijn of haar beslissing krachtens lid (8), zal de [rechter] bepalen of het bevel tot aftappen nodig blijft krachtens artikel 8.

(10) Indien de [rechter] overtuigd is dat het bevel tot aftappen nodig blijft, zal hij of zij een bevelschrift maken waarin de uitvaardiging daarvan wordt bevestigd.

(11) Indien de [rechter] niet overtuigd is dat het bevel tot aftappen noodzakelijk blijft, zal hij of zij een bevelschrift maken voor de herroeping daarvan.

(12) In het geval dat een bevel tot aftappen uitgevaardigd of vernieuwd krachtens dit artikel wordt herroepen onder lid (11), zal het bevelschrift niet meer van kracht zijn vanaf de herroeping.

(13) In het geval dat de uitvaardiging van een bevel tot aftappen wordt bevestigd krachtens lid (10) van dit artikel, zullen de bepalingen van artikel 10 van toepassing zijn met betrekking tot de duur ervan alsof de datum van het bevelschrift waarmee de uitvaardiging van het bevel tot aftappen wordt bevestigd de datum is waarop het bevelschrift eerst werd uitgevaardigd.

Voortgangsrapport

15. Een [rechter] die een bevel tot aftappen heeft uitgevaardigd kan op het tijdstip van uitvaardiging daarvan of op enig moment voor de vervaldatum daarvan van de bevoegde officier namens wie de relevante aanvraag voor het bevel tot aftappen was gemaakt, eisen schriftelijk te rapporteren aan hem of haar inzake :

a. de voortgang die is gemaakt bij het behalen van de doelstellingen van het bevel tot aftappen; en

b. enige andere zaak die de [rechter] noodzakelijk acht.

Eindrapport

16. (1) Zo snel als mogelijk nadat een bevel tot aftappen is vervallen, zal de bevoegde officier die het had aangevraagd, een schriftelijk rapport indienen bij de [rechter] die het bevel tot aftappen had verleend, of indien die [rechter] niet in staat is te handelen bij een andere [rechter], met betrekking tot de wijze waarop de machtiging verleend door het bevel tot aftappen is uitgevoerd en de resultaten verkregen door de uitvoering van die bevoegdheid.

(2) Elk rapport dat is gemaakt voor de doelstellingen van lid (1) zal de volgende informatie bevatten:

a. waar het aftapapparaat was geplaatst;

b. het aantal aftappingen uitgevoerd met het aftapapparaat;

c. of enig relevant bewijsmateriaal was verkregen door middel van het aftapapparaat;

d. of enig relevant bewijsmateriaal was, of zal, worden gebruikt in een strafrechtelijke vervolging; en

e. of enige bescheiden van een communicatie onderschept ingevolge het bevel tot aftappen zijn vernietigd in overeenstemming met artikel 23, en indien niet, waarom die niet zijn vernietigd.

HOOFDSTUK III – UITVOERING VAN HET AFTAPPEN

Uitvoering van bevel tot aftappen

17. (1) Een bevoegde officier die een bevel tot aftappen uitvoert mag communicatie gespecificeerd in het bevelschrift aftappen en volgens de voorwaarden van het bevel tot aftappen tijdens de verzending daarvan door middel van een aftapapparaat.

(2) Een bevoegde officier kan van een persoon eisen dat die communicatie onderschept, indien dat is gespecificeerd in het bevelschrift.

(3) Een bevoegde officier of persoon, die ingevolge een bevel tot aftappen communicatie onderschept of bijstaat in het aftappen daarvan moet alle redelijke stappen ondernemen voor het minimaliseren van de invloed van aftappen op derden.

(4) Een bevoegde officier of persoon die handelt ingevolge of in naleving van een bevel tot aftappen of die in goed vertrouwen een persoon helpt waarvan hij op redelijke gronden gelooft dat die handelt in overeenstemming met dergelijke machtiging stelt zich niet bloot aan enige strafrechtelijke of civiele aansprakelijkheid voor iets dat redelijkerwijs is gedaan ten behoeve van het bevel tot aftappen.

Betreding van panden en erven voor de uitvoering van een bevel tot aftappen

18. Indien een bevel tot aftappen een toestemming omvat dat een bevoegde officier panden en erven kan betreden krachtens lid (3) van artikel 9, kan een bevoegde officier op enig tijdstip gespecificeerd in het bevel tot aftappen de panden en erven betreden en handelingen verrichten waarvoor hij of zij toestemming heeft om die uit te voeren in overeenstemming met het bevel tot aftappen.

Plicht om bijstand te verlenen

19. (1) Een persoon die telecommunicatiediensten verleent zal toestaan aan, en bijstand verlenen indien vereist en redelijk, een bevoegde officier dat die het bevel tot aftappen kan uitvoeren.

(2) Indien een bevoegde officier van plan is een persoon te bevelen communicatie af te tappen, dan zal de [rechter] die persoon verplichten het aftappen uit te voeren in naleving van het bevel tot aftappen uitgegeven in overeenstemming met lid (1) van artikel 8 of artikel 14.

Nalaten bijstand te verlenen

20. Een persoon, die opzettelijk en zonder rechtmatig excuus of rechtvaardiging nalaat een bevoegde officier toe te staan of bij te staan bij het uitvoeren van het aftappen zoals gespecificeerd in leden (1) en (2) van artikel 19 begaat een strafbaar feit dat bij veroordeling wordt bestraft met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beiden.

Confidentialité de la

21. (1) Een bevoegde officier zal de volgende regelingen treffen die nodig zijn voor het verzekeren van de geheimhouding van het aftappen:

communication interceptée

a. tot een minimum dat nodig is voor de doelstellingen waarvoor het bevel tot aftappen werd uitgegeven, beperken:

i. de mate waarin de onderschepte communicatie openbaar wordt gemaakt;

ii. het aantal personen aan wie enige van de communicatie wordt onthuld;

iii. de mate waarin enige van die communicatie werd gekopieerd; en

iv. het aantal kopieën dat wordt gemaakt van enige communicatie;

en

b. om te verzekeren dat elke kopie gemaakt van de communicatie wordt

i. opgeslagen op een veilige manier voor zolang de bewaring daarvan nodig is, en

ii. vernietigd krachtens de bepalingen van artikel 23.

(2) Elke persoon die gemachtigd is communicatie af te tappen of bijstand te verlenen voor het uitvoeren van aftappen zal de volgende informatie geheimhouden:

a. het bestaan en de inhoud van het bevel tot aftappen;
b. bijzonderheden van de uitvaardiging van het bevel tot aftappen en van enige vernieuwing of wijziging van een van beide;
c. het bestaan en de inhoud van enige vereiste om bijstand te verlenen;
d. stappen genomen voor het uitvoeren van het bevel tot aftappen;
e. alle onderschepte materialen met alle daaraan gerelateerde communicatiegegevens.

Nalaten om informatie inzake aftappen geheim te houden

22. Een persoon die opzettelijk en zonder rechtmatig excuus of rechtvaardiging iets openbaar maakt waarvan hij of zij wordt geacht dat geheim te houden ingevolge de bepalingen van artikel 21 begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

Destruction des enregistrements

23. (1) Een bevoegde officier zal verzekeren dat bescheiden die niet zijn gerelateerd aan de doelstelling van het bevel tot aftappen direct worden vernietigd.

(2) Alle bescheiden van de informatie die is verkregen van het aftappen van communicatie krachtens een bevel tot aftappen, waaronder informatie die geheel of gedeeltelijk en direct of indirect is gerelateerd aan de doelstelling van het bevel tot aftappen zal zodra blijkt dat geen proces, of geen verder proces, zal worden gevoerd waarin de informatie waarschijnlijk vereist zal worden te worden overlegd als bewijsmateriaal, vernietigd worden.

(3) Niets in lid (2) zal van toepassing zijn op enige bescheiden of enige informatie aangehaald in het proces voor enige rechter.

(4) Elk rapport uitgebracht aan een [rechter] in overeenstemming met artikel 16 zal aangeven of er wel of niet is voldaan aan lid (2), en indien niet, dan zal de [rechter] dergelijke instructies geven die verband houden met de mogelijke vernietiging van de bescheiden zoals nodig geacht door de [rechter] om naleving met dat lid te garanderen, waaronder de vereiste dat de [rechter] in kennis wordt gesteld wanneer de bescheiden zijn vernietigd.

Nalaten bescheiden te vernietigen

24. Een persoon die opzettelijk en zonder rechtmatig excuus of rechtvaardiging nalaat de vereisten van leden (1) en (2) van artikel 23 na te leven begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beide.

HOOFDSTUK IV – AFTAPAPPARATUUR

Lijst van apparatuur met aftapcapaciteiten

25. [(1) De [*Minister*] zal, bij kennisgeving gepubliceerd in de [*Staatscourant*], alle draad, draadloze, elektronische, optische, magnetische, of ander instrumenten, apparaten, of apparatuur, die voornamelijk zijn ontworpen met als doel het aftappen van communicatie, onder de voorwaarden en omstandigheden gespecificeerd in de kennisgeving, bestempelen als beschermde apparatuur met aftapcapaciteiten.

(2) Een kennisgeving kan op elk moment worden gewijzigd of ingetrokken.

(3) De eerste kennisgeving onder lid (1) zal worden uitgegeven door de [Minister] binnen [*drie maanden*] na de datum van inwerkingtreding van deze wet.

(4) Voordat de [Minister] de bevoegdheid onder lid (1) uitoefent, zal het concept van de voorgestelde kennisgeving worden gepubliceerd in de [*Staatscourant*], samen met een kennisgeving om alle belanghebbenden uit te nodigen binnen een gespecificeerde periode schriftelijk hun commentaar en voorstellen in te dienen met betrekking tot de voorgestelde kennisgeving.

(5) Een periode van *[een maand*] zal verstrijken tussen de publicatie van de conceptkennisgeving en de kennisgeving ingevolge lid (1).

(6) Lid (4) is niet van toepassing indien:

a. de [Minister], in navolging van commentaren en voorstellen ontvangen ingevolge lid (4) besluit een kennisgeving te publiceren waarnaar wordt verwezen in lid (1) in een gewijzigde vorm;

b. een afkondiging ingevolge lid (1) met betrekking waartoe de [Minister] van mening is dat in het openbaar belang deze zonder vertraging gemaakt dient te worden.

(7) Elke kennisgeving ingevolge lid (1) zal voorafgaand aan de publicatie daarvan in de [*Staatscourant*] worden gedaan middels een positieve beslissing.]

Verbod op de productie, het bezit en het gebruik van beschermde apparatuur met aftapcapaciteiten

26. [(1) Behoudens lid (2) van dit artikel en artikel 27 zal geen enkele persoon beschermde apparatuur in elkaar zetten, bezitten, verkopen, kopen en gebruiken.

(2) Lid (1) is niet van toepassing in geval van een toestemming verleend ingevolge artikel 28.]

Utilisation d'un équipement sans autorisation

27. [(1) Een persoon die opzettelijk en zonder rechtmatig excuus of rechtvaardiging handelt in strijd met of nalaat de vereisten van artikel 26 na te leven, begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beiden.

(2) In geval een persoon wordt veroordeeld wegens een misdrijf tegen lid (1) kan de rechter als onderdeel van de uitspraak de opdracht geven dat de apparatuur met aftapcapaciteiten in beslag wordt genomen.

Opmerking: Een land kan een bepaling opnemen die toestaat dat een vergunning wordt beëindigd in geval de aanbieder van telecommunicatiediensten opzettelijk en zonder rechtmatig excuus of rechtvaardiging de bepaling van artikel 26 overtreedt of nalaat die na te leven.].

Machtiging tot het gebruik van beschermde apparatuur met aftapcapaciteiten

28. [(1) De [Minister] kan, bij aanvraag, iedere persoon, privé-lichaam of rechtshandhavingsinstantie vrijstellen van een of alle verboden handelingen genoemd onder lid 1 van artikel 26 voor een periode en op voorwaarden vast te stellen door de [Minister].

(2) De [Minister] kan slechts een vrijstelling verlenen ingevolge lid (1) indien hij of zij ervan overtuigd is dat —

a. dergelijke vrijstelling in het openbaar belang is;

b. de doelstelling waarvoor de beschermde apparatuur zal worden gemaakt, in elkaar gezet, in bezit worden gehouden, verkocht, gekocht of geadverteerd redelijkerwijs nodig is; en

c. er speciale omstandigheden zijn die een dergelijke vrijstelling rechtvaardigen.

(3) Een vrijstelling ingevolge lid (1) zal worden verleend door een vrijstellingscertificaat te verlenen aan de betrokken persoon waarin zijn of haar naam of de naam daarvan en de reikwijdte, duur en voorwaarden van de vrijstelling zijn gespecificeerd.

(4) Een vrijstellingscertificaat verleend ingevolge lid (3) zal worden gepubliceerd in de [*Staatscourant*] en zal geldig zijn vanaf de dag van de publicatie daarvan.

(5) Een vrijstellingscertificaat kan op enig tijdstip op een gelijkaardige wijze worden gewijzigd of ingetrokken door de [Minister].

(6) Een vrijstellingscertificaat vervalt in geval van

a. beëindiging van de periode waarvoor het verleend was; en

b. intrekking ingevolge lid (5)].

Deel II

HOOFDSTUK V – OPENBAARMAKING VAN OPGESLAGEN COMMUNICATIEGEGEVENS

Verbod op toegang tot opgeslagen computerdata

29. (1) wederrechtelijke toegang tot opgeslagen communicatie is verboden.

(2) Een persoon die opzettelijk en zonder rechtmatig excuus of rechtvaardiging zich toegang verschaft tot opgeslagen communicatie, of die een andere persoon machtigt, toelaat of toestemt zich toegang te verschaffen tot opgeslagen communicatie begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beiden.

(3) Een rechtmatig excuus is gegeven indien:

a. toegang tot opgeslagen communicatie is gebaseerd op een bevel tot openbaarmaking; of

b. toegang tot opgeslagen communicatie is gebaseerd op een bevel tot aftappen; of

c. toegang tot opgeslagen communicatie is gebaseerd op a ingevolge bevelschriften en instructies uitgegeven in overeenstemming met procedurele wetgeving.

Openbaarmaking van opgeslagen communicatiegegevens

30. (1) In het geval dat de [aangewezen persoon] [rechter] de indruk heeft dat een persoon die telecommunicatiediensten verleent in het bezit is of kan zijn van, of in staat is in het bezit te komen van, enige communicatiegegevens, kan de [aangewezen persoon] [rechter] ingevolge een bevel tot openbaarmaking eisen van de aanbieder van telecommunicatiediensten:

a. aan een bevoegde officier alle data openbaar te maken die hij of zij in haar bezit heeft of die door hem of haar daarop verkregen zal worden, of

b. indien de aanbieder niet reeds in het bezit is van de data, om de data te verkrijgen en openbaar te maken aan de bevoegde officier.

(2) Een [aangewezen persoon] [rechter] kan geen bevel tot openbaarmaking uitvaardigen met betrekking tot communicatiegegevens tenzij hij of zij ervan overtuigd is dat het nodig is de data te verkrijgen en de data openbaar te maken aan een bevoegde officier.

(3) Een [aangewezen persoon] [rechter] kan geen bevel tot openbaarmaking uitvaardigen ingevolge lid (2) met betrekking tot communicatiegegevens tenzij hij of zij ervan overtuigd is dat het nodig is die data te verwerven;

a. in het belang van de nationale veiligheid;

b. met als doel het voorkomen of opsporen van misdrijven of voor het voorkomen van publieke onrust;

c. in het belang van de openbare veiligheid;

d. met als doel het beschermen van de openbare gezondheid;

e. met als doel in een noodgeval het voorkomen van de dood, een ongeval, of enige schade aan de fysieke en mentale gezondheid van een persoon, of voor het verlichten van een ongeval of schade aan de fysieke of mentale gezondheid van een persoon.

(4) Een bevel tot openbaarmaking ingevolge dit artikel omvat:

a. de communicatiegegevens met betrekking waartoe het van toepassing is;

b. de bevoegde officier aan wie de openbaarmaking wordt gedaan;

c. de manier waarin de openbaarmaking zal worden gedaan;

d. de zaken die vallen binnen lid (3) onder verwijzing waarnaar het bevelschrift is uitgevaardigd; en

e. de datum waarop het is uitgevaardigd.

(5) Een bevel tot openbaarmaking vereist niet dat;

a. enige communicatiegegevens zal worden openbaar gemaakt aan het eind van de periode van een maand beginnend op de datum waarop het bevelschrift is uitgevaardigd; of

b. na het eind van die periode, enige communicatiegegevens openbaar wordt gemaakt die niet in het bezit was van de aanbieder van telecommunicatiediensten, of waarvan werd vereist dat hij of zij die verwierf, tijdens die periode.

(6) Behoudens lid (7), zal een aanbieder van telecommunicatiediensten, aan wie een bevel tot openbaarmaking is uitgevaardigd ingevolge dit artikel, aan geen enkele persoon het bestaan onthullen van of de werking van het bevelschrift, of enige informatie waaruit het bestaan of de werking daarvan redelijkerwijs kan worden afgeleid.

(7) De openbaarmaking waarnaar wordt verwezen in lid 6 kan worden gedaan aan:

a. een officier of agent van de dienstverlener met als doel er voor te zorgen dat het bevel tot openbaarmaking wordt nageleefd;

b. een advocaat met als doel het verkrijgen van juridisch advies of vertegenwoordiging met betrekking tot het bevel tot openbaarmaking,

en een persoon waarnaar wordt verwezen in leden (a) of (b) zal het bestaan of de werking van het bevel tot openbaarmaking niet onthullen, behalve aan de bevoegde officier gespecificeerd in de kennisgeving met als doel;

i. het verzekeren dat de kennisgeving wordt nageleefd, of het verkrijgen van juridisch advies of vertegenwoordiging met betrekking tot het bevel tot openbaarmaking, in geval van een officier of agent van de dienstverlener; of

ii. het geven van juridisch advies of het maken van verklaringen met betrekking tot het bevel tot openbaarmaking in geval van een advocaat.

Nalaten om informatie over het bevel tot openbaarmaking geheim te houden

31. Een persoon die opzettelijk en zonder rechtmatig excuus of rechtvaardiging iets openbaar maakt waarvan hij of zij wordt vereist dat geheim te houden ingevolge lid (6) van artikel 20 begaat een strafbaar feit dat bij veroordeling bestraft wordt met een boete van niet meer dan [bedrag] of een gevangenisstraf voor een periode van niet langer dan [periode], of beiden.

HOOFDSTUK VI – KOSTEN VOOR AFTAPPEN

Toewijzing van kosten

32. (1) Kosten die worden opgelopen door een aanbieder van telecommunicatiediensten die de aanbieder van telecommunicatiediensten in staat stelt communicatie af te tappen en/ of op te slaan, waaronder de investerings-, technische, onderhouds- en operationale kosten moeten worden gedragen door die aanbieder van telecommunicatiediensten.

(2) Een land kan een model vaststellen voor de terugbetaling van directe kosten die zijn opgelopen door de aanbieder van telecommunicatiediensten met betrekking tot het personeel en de administratie die vereist zijn voor het verlenen van bijstand in de uitvoering van een bevel tot aftappen.

HOOFDSTUK VII – WAARBORGEN

Beroepsgeheim

33. [Indien het bewijsmateriaal verkregen door middel van aftappen van communicatie geprivilegieerd is krachtens de [wet] ter bescherming van:

a. [medisch beroepsgeheim];

b. [communicatie van professionele aard tussen een advocaat en een cliënt];

c. [bankgeheim];

d. [financieel geheim];

e. [enig ander geheim dat een land wenst te beschermen bij wet]

dan blijft dat bewijsmateriaal geprivilegieerd en zal niet voor de rechtbank worden gepresenteerd, behalve met de instemming van de persoon die recht heeft op het afstand doen van dat privilege].

Monitoren van aftappen van communicatie

34. [(1) Een Onafhankelijke Monitoringsautoriteit zal worden ingesteld met de bevoegdheid in richtlijnen en controles te voorzien om te verzekeren dat het aftappen van communicatie wordt uitgevoerd in overeenstemming met de juridische machtiging.

(2) In plaats van het creëren van een aparte Onafhankelijke Monitoringsautoriteit, kan een land een autoriteit die:

a. niet actief betrokken is in het opsporingsproces; en

b. de capaciteit heeft de nodige functies uit te voeren voor het toezien op het aftappen de functies toekennen van de Onafhankelijke Monitoringsautoriteit.

(3) Een bevoegde officier zal niet meer dan [7] dagen na het indienen van een Eindrapport (artikel 16) de volgende informatie aan de Onafhankelijke Monitoringsautoriteit overleggen met als doel het bijhouden van een register van bevelen tot aftappen:

a. datum van uitgifte van het bevelschrift;

b. [rechter] die het bevelschrift had uitgevaardigd;

c. agentschap waaraan het bevelschrift was uitgevaardigd; en

d. periode waarvoor het bevelschrift in werking was.

(4) De Onafhankelijke Monitoringsautoriteit:

a. houdt het register van bevelen tot aftappen bij, waarbij informatie wordt bijgehouden gespecificeerd in lid (3) van artikel 34; en

b. overlegt iedere [6] maanden een rapport inzake het Monitoren van het Aftappen van Communicatie aan de Onafhankelijke Commissaris inzake Aftappen van Communicatie.

(5) De Onafhankelijke Monitoringsautoriteit kan, door middel van een schriftelijke kennisgeving afgegeven aan de [leidinggevende functionaris van de in aanmerking komende instantie], eisen dat de [in aanmerking komende instantie] informatie overlegt die nodig is om te verzekeren dat het aftappen van communicatie wordt uitgevoerd in overeenstemming met deze wet.

(6) In het geval, dat als gevolg van het monitoren de Onafhankelijke Monitoringsautoriteit gelooft dat een bevoegde officier een bepaling van deze wet heeft overtreden, kan de Onafhankelijke Monitoringsautoriteit deze schending opnemen in het rapport inzake het Monitoren van het Aftappen van Communicatie].

Onafhankelijke commissaris inzake het aftappen van communicatie

35. [(1) De Onafhankelijke Commissaris inzake het Aftappen van Communicatie zal worden aangesteld door het Parlement.

(2) De Onafhankelijke Commissaris zal zijn functie bekleden voor een periode van niet meer dan [5] jaar, zoals aangegeven in zijn of haar benoemingsakte, maar komt in aanmerking voor herbenoeming.

(3) De Onafhankelijke Commissaris, wanneer het doel een inspectie is:

a. kan, na het in kennis stellen van de leidinggevende functionaris van de [instantie], op elk redelijk tijdstip de panden en erven ingenomen door de [instantie] betreden]; en

b. heeft het recht op volledige en vrije toegang op elk redelijk tijdstip tot alle bescheiden van de [instantie] betreffende aftappingen; en

c. heeft het recht op het maken van kopieën van, en extra beschikbare te nemen van, bescheiden van de instantie of het register van bevelen tot aftappen; en

d. kan een functionaris van de [instantie] verzoeken de Onafhankelijke Commissaris die informatie te verstrekken die het register van bevelen tot aftappen nodig vindt, welke informatie is die in het bezit is van de functionaris, of waartoe de functionaris toegang heeft, en die relevant is voor de inspectie.

(4) De [leidinggevende functionaris] van [een instantie] zal verzekeren dat de functionarissen van de [instantie] de Onafhankelijke Commissaris die bijstand verlenen in verband met het uitvoeren of uitoefenen van de functie of bevoegdheden van de Onafhankelijke Commissaris ingevolge dit artikel die redelijkerwijs vereist worden door de Onafhankelijke Commissaris.

(5) Alle verzoeken gedaan door de Onafhankelijke Commissaris terwijl die zijn taken uitoefent ingevolge leden (3) en (4) zullen worden beantwoord binnen [*7*] dagen.

(6) In het geval dat als gevolg van de inspectie de Onafhankelijke Commissaris gelooft dat een bevoegde officier of [instantie] een bepaling van deze wet heeft overtreden, kan de Onafhankelijke Commissaris zijn eigen onderzoek in die zaak initiëren.

(7) In het geval dat als gevolg van een onderzoek gedaan ingevolge lid (6) de Onafhankelijke Commissaris een overtreding van deze wet ontdekte, kan hij of zij een bindende uitspraak doen die vereist dat de schending wordt beëindigd en de activiteit die deze wet schendt wordt stopgezet.

(8) De bindende uitspraak uitgevaardigd ingevolge lid (7) moet worden uitgevaardigd in schriftelijke vorm en is dwingend voor een bevoegde officier, instantie of particulier lichaam.

(9) Indien een bevoegde officier, instantie of particulier lichaam nalaat de uitspraak na te leven uitgevaardigd ingevolge lid (7) binnen [*14*] dagen nadat de uitspraak is ontvangen, dan kan de Onafhankelijke Commissaris een verzoek doen aan de rechter de uitspraak af te dwingen.

(10) Individuen of overheidsinstanties hebben het recht in beroep te gaan tegen de beslissingen van de Onafhankelijke Commissaris.].

HOOFDSTUK VIII – TOELAATBAARHEID VAN BEWIJSMATERIAAL

Toelaatbaarheid van onderschepte communicatie als bewijsmateriaal

36. [(1) Slechts communicatiegegevens onderschept in overeenstemming met deze wet zal toelaatbaar zijn als bewijsmateriaal in overeenstemming met de wet inzake de toelaatbaarheid van bewijsmateriaal.

(2) Bijzonderheden van communicatie onderschept krachtens een bevel tot aftappen of een nood bevel tot aftappen zal niet toelaatbaar zijn als bewijsmateriaal in een rechtszaak tegen een persoon tenzij de partij die van plan is het aan te halen de persoon redelijkerwijs voorafgaande kennisgeving heeft gegeven van de intentie om dit te doen, samen met

a. een transcriptie van de privé communicatie waar in de persoon het wil aanhalen in de vorm van een opname, of een geschreven verklaring waarin de volledige bijzonderheden uiteengezet worden van de communicatie waar die persoon van plan is dat mondeling bewijs ervan aan te halen; en

b. een verklaring van de tijd, plaats (indien bekend), en datum van de communicatie, en de namen en adressen van de partijen bij de communicatie, indien die bekend zijn.

(3) Zelfs als de communicatie was onderschept ingevolge een bevel tot aftappen of een nood bevelschrift, zal bewijsmateriaal van onderschepte communicatie door middel van een aftapbewijs, of van de inhoud, betekenis of doel ervan, niet verstrekt worden in enige rechtszaak, tenzij het bewijsmateriaal betrekking heeft op het misdrijf dat is gespecificeerd in de bijlage.

Ontoelaatbaarheid van onderschepte communicatie als bewijsmateriaal

37. In het geval dat een communicatie wordt onderschept door middel van een aftapapparaat anderszins dan ingevolge een aftapbewijs of nood aftapbewijs uitgevaardigd ingevolge artikel 14 of enige bevoegdheid verleend door of ingevolge enige andere bepaling ter kennis is gekomen van een persoon als direct of indirect gevolg van die aftapping of de openbaarmaking daarvan, geen bewijsmateriaal van die communicatie op die wijze verkregen, of van de inhoud, betekenis, of doel, en geen ander bewijsmateriaal verkregen als direct of indirect resultaat van het aftappen of openbaarmaking daarvan, zal worden verstrekt aan enige persoon, behalve in een proces dat betrekking heeft op het wederrechtelijke aftappen van communicatie door middel van een aftapapparaat of de wederrechtelijke openbaarmaking van communicatie die wederrechtelijk was onderschept op die wijze.].

HOOFDSTUK IX – BIJLAGE

Wijziging van bijlage

38. (1) De Minster kan, bij besluit, overtredingen toevoegen of verwijderen van de lijst van overtredingen vervat in de bijlage.

(2) Een besluit gemaakt ingevolge lid (1) zal onderworpen zijn aan parlementaire goedkeuring.

Regelgeving

39. (1) De minister kan regelgeving instellen voor het implementeren van de doelstelling van deze wet.

(2) Regelgeving neergelegd ingevolge lid (1) zal onderworpen zijn aan parlementaire goedkeuring.

Deel II

BIJLAGE

(Artikel 8 (1) (a) (ii))

(1) [Moord of doodslag of hoogverraad].

(2) [Ontvoering].

(3) [Money laundering] in strijd met de [Wet inzake [het tegengaan van] Opbrengsten van misdrijven en money laundering].

(4) [Produceren, samenstellen, aanleveren of anderszins handelen in alle gevaarlijke drugs] in overtreding van de [Wet inzake Gevaarlijke Drugs].

(5) [Importeren of exporteren van gevaarlijke drugs] in overtreding van de [Wet inzake Gevaarlijke Drugs].

(6) [Import, export of doorvoer van alle wapens of munitie] in overtreding van de [Wapenwet].

(7) [Vervaardigen van, of handel drijven in wapens of munitie] in overtreding van de [Wapenwet].

(8) [Illegaal bezit van een verboden wapen of enig ander vuurwapen of ammunitie] in strijd met de [artikel van de Wapenwet].

(9) Een overtreding in strijd met [artikel van de wet inzake preventie van corruptie].

(10) [Brandstichting].

(11) [Internationale verdrag inzake vliegtuigkaping, terroristische daden, etc.].

(12) [Wet inzake het voorkomen van terrorisme].

(13) Poging of samenzweren tot het plegen, of het helpen of bijstaan, advies geven of het opdracht geven tot een overtreding die valt onder een van de voorgaande leden.

Deel III:
Memorie van toelichting bij de model wettekst inzake aftappen van communicatie

INLEIDING

1. Deze wettekst legt een model juridisch kader neer voor het legaal aftappen van communicatie. De belangrijkste doelstellingen van deze wettekst zijn het verbieden van wederrechtelijk aftappen van communicatie, zodat een beperkt aantal omstandigheden kan worden gedefinieerd voor het toestaan van aftappen, voor het vastleggen van normen voor het geven van dergelijke machtiging en voor de uitvoering daarvan, en voor het in evenwicht brengen van de macht van de staat en individuele privacy; en voor het beschermen van geheimhouding en de vrijheid van communicatie.
2. Deze wettekst is voorbereid en aangenomen in overeenstemming met de Richtlijnen voor model beleid van de Eerste consultatieworkshop van de HIPCAR werkgroep 1 inzake kwesties de informatiemaatschappij rakende.
3. Deze toelichting is bedoeld om de inhoud van deze wet toe te lichten, en moet worden gelezen in samenhang daarmee. Het belang van de bepalingen van deze wet wordt toegelicht en, in voorkomend geval, wordt de aandacht gevestigd op bepaalde besprekingen van de HIPCAR14 werkgroep15 en de Richtlijnen voor model beleid van de eerste consultatie workshop van de HIPCAR werkgroep 1. Ze zijn niet, en zijn niet bedoeld, een gedetailleerde beschrijving van deze wet te geven. Dus, waar een artikel of een deel van een artikel geen uitgebreide toelichting, commentaar of verwijzing behoeft, of wanneer er geen discussie was over een bepaalde bepaling, wordt geen gedetailleerde uitleg gegeven.
4. De wettekst bestaat uit negen hoofdstukken:
   - **Hoofdstuk I** geeft de definities en legt de doelstelling van de wettekst neer;
   - **Hoofdstuk II** verbiedt wederrechtelijk aftappen en stelt een beperkt aantal voorwaarden voor wanneer aftappen verondersteld wordt legaal te zijn. Het omvat tevens bepalingen die de procedure neerleggen voor het verkrijgen van een machtiging voor het aftappen van communicatie. Als laatste, verschaft het ook een basis voor het verlenen aan relevante instanties van een bevel tot aftappen, evenals de regels voor de duur, hernieuwing en terugtrekking van bevelen;

14 De volledige naam van het HIPCAR-project is “Versterking van het Concurrentievermogen in het Caribisch Gebied door de Harmonisatie van Beleid, Wetgeving en Regelgevingsprocedures op het stuk van ICT”. Het project met een looptijd van drie jaar werd gelanceerd in september 2008 in het kader van overkoepelend project voor de ACP-landen en wordt gefinancierd door de Europese Unie (EU) en de Internationale Telecommunicatie Unie (ITU). Het project wordt geïmplementeerd door de Internationale Telecommunicatie Unie (ITU) in samenwerking met de Caribische Gemeenschap (CARICOM) en de Caribische Telecommunicatie Unie (CTU).

15 De leden van de HIPCAR Werkgroepen bestaan uit vertegenwoordigers van Ministeries en regelgevende lichamen aangewezen door hun nationale overheden, relevante regionale lichamen en waarnemers – zoals aanbieders en andere geïnteresseerde belanghebbenden. De opdracht voor de werkgroepen zijn beschikbaar op: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/docs/ToR%20HIPCAR%20WGs.pdf.
De tweede consultatie workshop (Fase B) voor HIPCAR Werkgroep 1 inzake het ICT wettelijk kader – inzake kwestie de informatiemaatschappij rakende werd gehouden in Barbados, van 23-26 augustus 2010. Participanten hebben met een brede consensus de concept model wetteksten herzien, besproken en aangenomen betreffende het betrokken werkgebied. Waar het woord “werkgroep” wordt gebruikt in dit document, verwijst het naar de voorgaande workshop.

- **Hoofdstuk III** ontwikkelt een kader voor de uitvoering van aftappen van communicatie;
- **Hoofdstuk IV** behandelt de kwestie van het verbod op apparatuur die aftapcapaciteiten heeft en geeft ook de regeling waarmee het gebruik van dergelijke apparatuur wordt gereguleerd;
- **Hoofdstuk V** geeft aanbevelingen over de implementatie van de bepalingen inzake de openbaarmaking van opgeslagen communicatiegegevens;
- **Hoofdstuk VI** handelt over de kwestie van de toewijzing van kosten die men oploopt bij het aftappen;
- **Hoofdstuk VII** geeft aanbevelingen betreffende waarborgen voor het beschermen van bevoorrechte communicatie en geeft een optie voor het implementeren van maatregelen voor monitoring en toezicht;
- **Hoofdstuk VIII** bevat aanbevelingen betreffende de kwestie van de toelaatbaarheid van bewijsmateriaal**;**
- **Hoofdstuk IX** geeft een schematisch overzicht van de ernstige misdrijven waarnaar wordt verwezen in Hoofdstuk 1 van deze wettekst.

COMMENTAAR OP DE ARTIKELEN

HOOFDSTUK I – INLEIDING

5. Hoofdstuk I legt de inleidende bepalingen neer, zoals de titel, definities, doelstelling en de bepaling inzake de inwerkingtreding.

6. Artikelen 2 en 3 gaven aanleiding tot discussie binnen de HIPCAR werkgroep met betrekking tot de wijze waarop wetten worden opgesteld in de verschillende rechtsgebieden. Er werd besproken of het artikel met de definities geplaatst moet worden voor het artikel dat de doelstellingen van de model wettekst neerlegt. Er was een consensus dat deze kwestie zou worden overgelaten aan het oordeel van de individuele staten.

Artikel 3. Definities

7. Termen die in vierkante haken staan geven de keuze aan die de individuele staten hebben binnen de implementatie van de wetgeving. Als gevolg van bestaande bepalingen of het nationale rechtssysteem, kan een land ervoor kiezen een andere term te selecteren voor de woorden die in vierkante haken staan.

8. De definitie van agentschap gegeven in lid (1) stelt de begunstigde staten in staat het agentschap te determineren dat het aftappen zal uitvoeren. Er was een discussie binnen de werkgroep of er aanbevelingen zullen zijn met betrekking tot de lichamen waaraan dergelijke bevoegdheden zullen worden verleend. Echter, men was het erover eens dat elke staat zelf moet beslissen welk agentschap de bevoegdheid moet worden gegeven om af te tappen.

9. Dezelfde keuze wordt gegeven in lid (2), waarin de definitie van een gemachtigde officier wordt gegeven. Hoewel het belangrijk is om vast te stellen en definiëren, wie in staat moet zijn om een bevel tot aftappen aan te vragen en aftapprocedures uit te voeren, wordt de keuze overgelaten aan de begunstigde staten, die hun eigen lijst van personen zullen bepalen aan wie toestemming wordt verleend een machtiging aan te vragen voor het aftappen van communicatie.

10. Lid (3) definieert wat communicatie betekent voor het neerleggen van een kader dat aftappen reguleert. Voor de wettekst die aftappen van communicatie verbiedt, is het erg belangrijk, ten eerste, om de definitie van technologisch neutraal te formuleren, en ten tweede, om elke beperking te vermijden die relevante soorten communicatie kunnen uitsluiten van het verbod op aftappen. Dat is waarom de definitie van communicatie is opgesteld met als doel zowel data en

signalen daarbij te incorporeren die worden overgebracht over een elektronisch telecommunicatienetwerk of enig deel daarvan met behulp van elektronische, mechanische, optische, golf-, elektromagnetische of andere apparaten.

11. De definitie van aanbieder van telecommunicatiediensten is neergelegd in lid (4) met als doel het opleggen van de verplichting om communicatie af te tappen. Aangezien deze wet de mogelijkheid biedt aanbieders van telecommunicatiediensten te verplichten communicatie af te tappen in overeenstemming met het bevel, zal om kleine aanbieder van telecommunicatiedienstens te beschermen, die niet in staat zijn een aftapping te doen, een land het aantal klanten vaststellen die worden bediend door een aanbieder van telecommunicatiediensten zodat de rechter de mogelijkheid heeft een aanbieder van telecommunicatiediensten (aanbieder) te verplichten het aftappen uit te voeren.

12. Er was een belangrijke discussie met betrekking tot de definitie van telecommunicatienetwerk. Ten eerste, werd besproken of in deze definitie de verzending van informatie wordt begrepen, of het verlenen van telecommunicatiediensten. Ten tweede, werd besproken of het telecommunicatienetwerk voornamelijk verwijst naar de diensten of faciliteiten en infrastructuur. Ten derde, besprak de werkgroep of er een noodzaak is of er aparte definities moeten worden gegeven voor publieke en particuliere telecommunicatienetwerken met als doel het scheppen van een kader dat het aftappen van communicatie reguleert.

13. Het werd overeengekomen dat de definitie van telecommunicatienetwerk wordt geformuleerd zodat er een duidelijk onderscheid wordt gemaakt tussen faciliteiten, infrastructuur en diensten. Op dezelfde manier, heeft de werkgroep besloten telecommunicatienetwerk te definiëren als elke faciliteit of infrastructuur gebruikt door een persoon voor het verlenen van telecommunicatiediensten.

14. Verder werd besloten dat er geen noodzaak is om een onderscheid te maken tussen publieke en particuliere netwerken waar het aftappen betreft. Dit is ten eerste van toepassing op het verbod op aftappen: communicatie zal gelijkelijk worden beschermd ongeacht via welk netwerk de communicatie verloopt. Bovendien, met als doel het verlenen van de bevoegdheid om af te tappen, worden identieke waarborgen en procedures toegepast op beide soorten netwerken met als doel het evenveel beschermen van de rechten van individuen die verschillende soorten netwerken gebruiken. Zo wordt er dan geen onderscheid gemaakt tussen publieke en particuliere netwerken voor de doelstelling van deze wet.

15. De werkgroep besprak tevens de definitie van communicatie met betrekking tot de reikwijdte van de wettekst. De vraag die werd opgeworpen was of de wettekst het aftappen zou moeten reguleren van elke soort communicatie, waaronder post, of slechts elektronische communicatie. Hoewel veel van de participanten aangaven dat post- en elektronische communicatie niet anders moet worden behandeld met betrekking tot aftappen (b.v. aftappen zou verboden moeten worden, degelijke waarborgen moeten worden geïmplementeerd), was de werkgroep het erover eens dat het mandaat van de groep het aftappen van post niet dekte.

16. De definitie van telecommunicatiedienst gegeven in lid (6) is belangrijk voor het maken van een onderscheid tussen telecommunicatienetwerk en telecommunicatiediensten. Het legt vast dat voor de doelstelling van deze wettekst telecommunicatiedienst een dienst omvat die wordt verleend zowel door een persoon die een netwerk exploiteert en de persoon die slechts de dienst verleent zonder dat die het netwerk beheert.

17. Definities van aangewezen persoon en bevel tot openbaarmaking worden gegeven in respectievelijk leden (7) en (8), voor de doelstelling van Hoofdstuk V – openbaarmaking van opgeslagen communicatiegegevens. Deze definities zullen slechts door een lidstaat worden opgenomen indien het de aanpak volgt die wordt voorgesteld in Hoofdstuk V en de bepaling implementeert die toegang reguleren tot communicatiegegevens die nog niet zijn begonnen of reeds door een telecommunicatienetwerk zijn overgebracht.

18. Lid (9) legt een van de belangrijkste definities van deze wettekst neer. Om vast te stellen wat is verboden en wat wordt gereguleerd door deze wettekst, legt dit lid neer dat aftappen betekent het verwerven, bekijken, vastleggen, monitoren of kopiëren van de inhoud of een deel daarvan, van elke communicatie tijdens de verzending door middel van een aftapapparaat of -methode. Deze definitie brengt twee sleutelelementen naar voren bij de definitie van wat het werkwoord 'aftappen' inhoudt. Ten eerste, omvat het alle verschillende acties die kunnen worden uitgevoerd om af te tappen, zoals bekijken, monitoren, kopiëren en vastleggen. Ten tweede, stelt het vast dat binnen het kader van aftappen dit allemaal slechts toepasbaar is op de communicatie tijdens de verzending daarvan. Het werd besproken in de werkgroep dat aangezien de betekenis van aftapapparaat ook wordt gegeven in de wettekst, er geen noodzaak is een uitgebreide uitleg te geven voor aftapapparaat of -methode binnen de definitie van aftappen.

19. Lid (10) werd ontwikkeld voor het definiëren van onderschepte communicatie zodat het kan worden onderscheiden van, bij voorbeeld, opgeslagen communicatiegegevens. Zelfs indien communicatie wordt opgeslagen nadat een aftapping is uitgevoerd, is de belangrijkste benadering om het te definiëren als onderschept, dat het is vastgelegd tijdens de verzending daarvan. De definitie van onderschepte communicatie is ook relevant om bepalingen toe te passen die geheimhouding van onderschepte data beschermen en verplichtingen om alle bescheiden te vernietigen.

20. Aangezien de definitie van aftappen een verwijzing bevat naar de term “aftapapparaat”, wordt de laatste gedefinieerd in lid (11). De definitie van aftapapparaat werd ontworpen voor het omvatten van elk elektronisch, mechanisch, optisch, golf-, elektromechanish instrument, apparatuur of apparaat wat is gebruikt of kan worden gebruikt, ongeacht of dat op zichzelf is of in combinatie met enig ander instrument, apparatuur, programma of apparaat voor het aftappen van communicatie. Er was een discussie tijdens de plenaire sessie van de consultatieworkshop of de definitie van aftapapparaat software moet omvatten. Er werd opgemerkt door sommige van de participanten dat software kan worden gebruikt voor het uitvoeren van aftappen. Echter, men was het erover eens dat software op zichzelf niet kan worden gebruikt voor het aftappen van communicatie, zonder hardware, en de definitie van aftapapparaat bestrijkt elk soort hardware. Dus werd overeengekomen dat er geen noodzaak is software in deze definitie op te nemen.

21. Voor het beschermen van normale bedrijfsactiviteit, sluit lid (11) uit elk instrument, apparatuur of apparaat, of enig onderdeel daarvan dat wordt geleverd en wordt gebruikt in de normale bedrijfsuitoefening door klanten of door aanbieders van telecommunicatiediensten.

22. Lid (12) geeft de definitie van bevel tot aftappen door een verwijzing te maken naar lid 8. De belangrijkste discussie met betrekking tot de keuze van de term bevel in plaats van de term richtlijn is opgenomen in deze memorie van toelichting (artikel 8).

23. Voor de doelstelling van het aftappen van communicatie kader, geeft lid (13) aan wat beschermde apparatuur* is. Het moet worden opgemerkt dat de term beschermde apparatuur verschilt van aftapapparaat. Terwijl aftapapparaat een apparaat is (waaronder apparatuur voor tweeërlei gebruik) dat kan worden gebruikt voor het uitvoeren van een aftapping, verwijst beschermde apparatuur naar het speciale stelsel dat is ontwikkeld voor het beperken van het gebruik van apparatuur dat voornamelijk is ontworpen voor het doel van aftappen. Een land wordt geadviseerd de definitie van beschermde apparatuur slechts op te nemen indien het de benadering volgt voorgesteld in artikel 25 van deze wettekst.

24. De definitie van Minister wordt gegeven om staten een mogelijkheid te bieden een ministerie te definiëren die regelgeving zal ontwikkelen met betrekking tot het aftappen van communicatie. Dit kan bij voorbeeld het Ministerie van Nationale Veiligheid zijn, of enig ander ministerie dat de bevoegdheid heeft zich met deze aftapvraagstukken bezig te houden.

25. De definitie van een Persoon gegeven in lid (15) werd opgesteld door de werkgroep zodat zowel lichamen met als zonder rechtspersoonlijkheid worden inbegrepen.

26. De term opgeslagen communicatiegegevens is opgenomen in de lijst van definities aangezien het onderscheid tussen communicatie tijdens de transmissie en communicatie die of nog niet is begonnen, of is afgelopen, en verlopen is via een communicatiesysteem relevant is voor het aftekenen van een duidelijke lijn tussen aftappen en de openbaarmaking van opgeslagen communicatiegegevens. Deze model wettekst voorziet in verschillende kaders die het mogelijk maken communicatie af te tappen die wordt verzonden en voor het toegang verlenen tot opgeslagen communicatie. Het is essentieel een duidelijke lijn te trekken tussen deze twee procedures en twee verschillende soorten communicatie voor wat aftappen betreft.

1.7. Artikel 4: Toepassing

27. Het belangrijkste doel van dit artikel is om vast te stellen wat de reikwijdte is van de model wettekst, zodat niets in dit specifieke stuk wetgeving dat slechts van toepassing zou moeten zijn binnen de context van het aftappen van communicatie kan worden gebruikt in het geval van ernstige misdrijven voor het beperken van het recht van het individu. Lid (1) voorziet er dan in dat niets in deze wettekst kan worden geïnterpreteerd op dusdanige wijze dat het de anonimiteit of codering van communicatie vereist of verbied. Deze bepaling is ontwikkeld om de mogelijkheid te vermijden dat de wettekst wordt gebruikt als de basis voor een verbod op de codering van communicatie. Dit betekent niet dat de wettekst een begunstigde staat verbiedt dergelijk verbod in te stellen. Echter, dit moet apart worden gedaan van deze wettekst.

28. Lid (1) gaf aanleiding tot wezenlijke discussies in de Werkgroep en tijdens de plenaire sessie van de consultatie workshop over of de encryptie van communicatie een recht was van individuen, en of een dergelijk recht moet worden beperkt onder de noemer van het aftappen van communicatie kader. Terwijl beleidssturing benadrukt dat het ontwerp van de model wettekst niet het recht van het individu moet belemmeren voor anonimiteit en codering, uitte een deel van de deelnemers aan de workshop de bezorgdheid dat het recht om de communicatie te coderen het doel van aftappen op zichzelf kan belemmeren. Er werd benadrukt dat het verbod op codering op een ander niveau zal worden besproken aangezien het niet onder het mandaat valt van de Werkgroep. Echter, indien de wettekst geen bepaling zou bevatten die de invloed van de wet zou beperken betreffende het recht op anonieme en gecodeerde communicatie, dan zou deze wetgeving waarschijnlijk geïnterpreteerd kunnen worden als de basis voor een verbod op codering. Na intensieve besprekingen werd overeengekomen dat een expliciete beperking van codering buiten de reikwijdte van deze model wettekst lag, en dat elke wet die gebaseerd is op de model wettekst niet moet worden uitgelegd as het hebben van een invloed op enig recht op anonimiteit of codering van communicatie.

29. Lid (2) is opgesteld om een onderscheid te maken tussen aftappen van communicatie krachtens deze wettekst en regelgeving neergelegd door andere wetgeving voor bepaalde specifieke gevallen zoals aftappen uitgevoerd door inlichtingendiensten. De werkgroep was het erover eens dat lid (2) van artikel 4 omschrijft dat de wettekst niet van toepassing is indien communicatie onderworpen is aan speciale aftapprocedures en administratieve structuren krachtens een andere wet. Dit betekent dat indien er andere regelgeving van toepassing is op aftappen door inlichtingendiensten, of tijdens terrorismebestrijdingsactiviteiten, of in gelijkaardige situaties, of, zoals was aangegeven tijdens de werkgroep, wetgeving voor het aftappen van postdiensten bestaat, dan is de wettekst niet van toepassing op deze speciale aftapprocedures.

Deel III

HOOFDSTUK II – AFTAPPEN VAN COMMUNICATIE

30. Dit deel van de model wettekst streeft de belangrijkste doelen na van het document: ten eerste het verbieden van wederrechtelijk aftappen van communicatie en ten tweede het neerleggen van een beperkt aantal omstandigheden en strikte voorwaarden waaronder aftappen kan worden toegestaan.

31. De benadering van een verbod op het aftappen van communicatie ingenomen door deze wettekst is gelijk aan de vele regionale en nationale benaderingen op dit vlak, zoals de model wet van de OECS16, de wetgeving van Australië, Hong Kong, Zuid-Afrika en het Verenigd Koninkrijk. De strafbaarstelling van wederrechtelijk aftappen in de bovengenoemde nationale rechtsgebieden wordt meestal gevolgd door bepalingen die een wettig excuus vormen voor het aftappen en de regulering van het machtigingsproces.

32. Alle nationale benaderingen beschouwen het aftappen van communicatie als een uitzonderlijke maatregel die is beperkt tot het onderzoek van ernstige misdrijven. Verder, vereist aftappen voorafgaande judiciële machtiging – voornamelijk door middel van een rechterlijk bevel, alhoewel sommige landen zoals het Verenigd Koninkrijk het recht hebben vastgesteld om af te tappen zonder voorafgaande machtiging door de rechter. Tenslotte, kan aftappen worden toegestaan voor een beperkte tijd. Volgens deze benadering, naast het vaststellen van de overtreding van wederrechtelijk aftappen, geeft dit hoofdstuk:

- een uitleg van de omstandigheden waaronder aftappen legaal is;
- een aantal voorwaarden die nodig zijn voor het aanvragen van bevelen tot aftappen;
- de reikwijdte, vorm en duur van het bevel tot aftappen als een grond voor de verlenging en herroeping daarvan.

33. Verder, legt dit hoofdstuk ook een aantal degelijke waarborgen neer voor het beschermen van de privacy van communicatie en het voorkomen van het misbruik van de macht af te tappen. Elk artikel dat een machtiging verleent voor inmenging wordt gevolgd door een reeks bijkomende beperkingen en controles om te verzekeren dat aftappen nodig is en niet kan worden vermeden in bepaalde omstandigheden.

Artikel 5: Verbod op aftappen van communicatie

34. Artikel 5 maak wederrechtelijk aftappen een overtreding en verklaart de omstandigheden die de rechtmatigheid van het aftappen kan rechtvaardigen. Deze benadering maakt het mogelijk eerst strikte waarborgen in te voeren en dan het aftappen te beperken tot ernstige strafbare feiten en kwesties die nationale veiligheid raken.

35. Het belangrijkste doel van lid (1) is om de privacy van de gebruikers van telecommunicatiediensten te beschermen door het strafbaarstellen van alle communicatie tijdens de verzending anders dan in overeenstemming met de bepalingen van de wettekst. Strafbaarstelling van wederrechtelijk aftappen is een noodzakelijke maatregel om de communicatie te beschermen tegen inbreuken daarop. In de eerste plaats, vormt aftappen van communicatie een ernstige inbreuk op de persoonlijke levenssfeer die het gebruik van strafrechtelijke sancties rechtvaardigt. Het verbieden van het aftappen van communicatie door middel van strafrechtelijke sancties zorgt ervoor dat het slachtoffer hulp krijgt van wetshandhavingsinstanties bij het identificeren van de bron van crimineel gedrag. Bovendien, heeft het slachtoffer geen verhaal in het burgerlijk recht, indien het aftappen van de communicatie werd uitgevoerd zonder ongeoorloofde toegang tot privé panden en erven. Ten slotte voldoet de criminalisering van wederrechtelijk aftappen ook aan de redelijke verwachtingen van de partijen die deelhebben in de communicatie: elke inbraak moet worden verboden, tenzij toegestaan in overeenstemming met de wet.

16 Organisatie van Oost-Caribische Staten

36. Lid (2) geeft de reeks van bepaalde enge uitzonderingen. Deze reeks van uitzonderingen is heel belangrijk voor het garanderen dat aftappen rechtmatig kan zijn wanneer het is geautoriseerd en voor het rechtvaardigen van aftappen in bepaalde gevallen wanneer judiciële machtiging niet nodig is.

37. Lid (2) (a) garandeert het recht op aftappen in overeenstemming met de autorisatie gekregen van de rechter. Deze model wettekst reguleert het proces voor het verkrijgen en uitvoeren van dergelijke autorisatie.

38. Lid (2) (b) legt vast dat aftappen rechtmatig is wanneer er redelijk grond is om te geloven dat de partij bij de communicatie daarmee heeft ingestemd. Deze bepaling is van belang voor het uitsluiten van aftappen met wederzijdse instemming van de reikwijdte van de wettekst. Deze model wettekst concentreert zich op de gevallen waarin de partijen bij de communicatie niet instemmen met het aftappen, slechts omdat in dit geval het aftappen inbreuk doet op het recht op privacy. Er is geen aftappen indien de partijen ermee instemmen. De meeste bestaande benaderingen reguleren geen aftappen met wederzijds goedvinden en het monitoren van communicatie door de deelnemers, omdat het recht op het aftappen de eigen communicatie de privébelangen van de persoon beschermt, in het bijzonder in de handels- en bedrijfscontext. Een partij bij de communicatie zal het risico nemen van openbaarmaking van communicatie door een andere partij. Daarbij, zal het recht van de partij goede notities te maken van een conversatie en dan deze notities te reproduceren kan overeenkomen met het recht de eigen communicatie af te tappen, zoals bekend in bepaalde rechtsgebieden.

39. Lid (2) (c) sluit opgeslagen communicatiegegevens uit die verkregen zijn in het kader van enige andere wet. Deze bepaling maakt een duidelijk onderscheid tussen aftappen - het vastleggen van communicatie bij hun verzending - en het verkrijgen van opgeslagen communicatiegegevens die niet begonnen zijn of al door het telecommunicatienetwerk zijn heengegaan.

40. Lid (2) (d) maakt het wettig om communicatie af te tappen als een gewoon incident bij het verlenen van telecommunicatiediensten of voor de handhaving van enige wet die van kracht is met betrekking tot het gebruik van die diensten. Deze uitsluiting is essentieel voor het veiligstellen van normale handelsactiviteiten van aanbieders van telecommunicatiediensten. Bij voorbeeld, het kan van communicatie dienstverleners vereist worden dat zij radiostoringen opsporen en elimineren en om te verzekeren dat er naleving is van de vergunningsvoorwaarden of om communicatieapparatuur te testen en meten om na te gaan of die overeenstemmen met de eisen onder de regelgeving of de voorwaarden van de vergunning waaronder die worden gehouden. Dit kan aftappen omvatten. Aangezien dit soort aftappen nodig is om te verzekeren dat het telecommunicatiesysteem goed werkt, worden aftappen om deze reden uitgesloten van strafbaarstelling.

41. Verder, zullen communicatie dienstverleners een plicht hebben om de kwaliteit van de dienstverlening in het telecommunicatienetwerk te onderhouden. Zij kunnen ook worden verplicht om te voldoen aan de vergunningsvoorwaarden. Bij voorbeeld, zij moeten aftappingen uitvoeren om ervoor te zorgen dat ruis in het telecommunicatienetwerk wordt gehouden op een aanvaardbaar niveau. Daarom moet dienstverleners ook worden toegestaan telecommunicatie af te tappen voor het leveren van telecommunicatiediensten of het uitvoeren van mechanische of dienstverleningskwaliteitscontrole. Lid (2) onder (d) beschermt dit recht.

42. Lid (2) onder (e) beperkt de strafbaarstelling met betrekking tot het aftappen van communicatie via een telecommunicatienetwerk dat is geconfigureerd op een manier die communicatie gemakkelijk toegankelijk moet maken voor het grote publiek. Dit is belangrijk ter bescherming van de persoon die communicatie onderschept die in eerste instantie niet worden gewaarborgd door privacy-recht, omdat zij gemakkelijk toegankelijk zijn voor het publiek.

43. Lid (2) onder (f) maakt een uitzondering voor het aftappen van communicatie ontvangen en verzonden binnen het netwerk dat in de behoeften voorziet van een particulier bedrijf of huishouden indien het aftappen wordt uitgevoerd door de persoon die het recht heeft om de

werking of het gebruik van het netwerk te beheersen of met uitdrukkelijke of stilzwijgende toestemming van deze persoon. Deze bepaling is met name relevant voor een persoon die het recht heeft een telecommunicatienetwerk binnen een bedrijf of huishouden te beheersen en laat het aftappen van hun eigen netwerken toe zonder dat dit kwalificeert als het plegen van een strafbaar feit. Dit kan onder meer inhouden, bij voorbeeld monitoren van telefoongesprekken met behulp van een tweede telefoonhoorn in een huis, of het opnemen van gesprekken met klanten in de banken zodat er een vastlegging is van de transacties, het opnemen van telefoongesprekken naar de klantenservice in grote bedrijven, etc.

44. De werkgroep heeft besproken of het nodig is 'netwerk' te definiëren waarnaar wordt verwezen in lid (2) onder (f) als een particulier netwerk en de definitie op te nemen in het inleidende deel van de model wettekst. Er werd overeengekomen dat er geen reden is voor het onderscheid maken tussen publieke en particuliere netwerken met betrekking tot aftappen. Een persoon die een telecommunicatienetwerk gebruikt, heeft het recht beschermd te worden tegen wederrechtelijk aftappen, ongeacht of het netwerk publiek is of privé. Communicatie moet gevrijwaard worden van aftappen in beide netwerken. De werkgroep heeft besloten de interne bedrijfsnetwerken en huishoudelijke netwerken alleen in dit lid te definiëren voor de toepassing van deze bepaling.

45. Lid (3) biedt een extra reeks van uitzonderingen. Op basis van lid (3) onder (a), wordt het aftappen van communicatie verzonden door of bestemd voor een persoon, die toestemming heeft gegeven voor het aftappen als geoorloofd beschouwd. Deze bepaling volgt de aanpak van uitsluiting van aftappen met wederzijds goedvinden van strafbaarstelling. Het verschil tussen de leden (2) (b) en lid (3) (a) is dat de laatste handelt over het geval waarbij toestemming duidelijk is kenbaar gemaakt.

46. Lid (3) onder (b) voorziet in een wettig excuus voor het aftappen in geval van nood. Deze bepaling is belangrijk om het recht veilig te stellen om alle redelijke maatregelen te nemen om dood of letsel of schade aan de fysieke of mentale gezondheid van een persoon te vermijden, of om enig letsel of schade aan de lichamelijke of geestelijke gezondheid van een persoon te verminderen of in het belang van de nationale veiligheid wanneer er geen mogelijkheid is machtiging van te voren aan te vragen. Er moet echter speciaal worden benadrukt dat deze bepaling alleen gevallen van echte noodzaak dekt.

Artikel 6. Aanvraag van bevel tot aftappen

47. Artikel 6 is erop gericht de procedure vast te stellen voor de eerste aanvraag om aftappen toe te staan.

48. Lid (1) definieert dat een bevoegde officier ex parte bij de [rechter] een bevel kan aanvragen voor het aftappen van communicatie in elk geval waarbij er redelijke gronden zijn om te geloven dat aan de voorwaarden voor het uitvaardigen van het bevel tot aftappen is voldaan. Deze bepaling bevat een aantal belangrijke implicaties voor de procedure voor het goedkeuren van het aftappen: (1) het aftappen wordt gegeven onder het systeem van bevelen; (2) het aftappen wordt goedgekeurd door de rechter; (3) de aanvraag wordt ex parte gedaan.

49. Het systeem van bevelen is een essentieel conventioneel mechanisme dat is aangenomen in veel landen waarmee inbreuken zoals huiszoeking en aftappen van communicatie worden toegestaan. Ten eerste, vereist het de goedkeuring door een onafhankelijke autoriteit voorafgaand aan de inbreuk. Ten tweede, verstrekt het de indringer met een schriftelijke toestemming die hij of zij slechts kan overleggen onder bepaalde voorwaarden. Verder, is een systeem van bevelen slechts belangrijk wanneer de inbreuk de technische bijstand vereist van een derde. Dit is de gebruikelijke situatie wanneer aftappen van communicatie wordt uitgevoerd door een telecommunicatienetwerk op instructie van de rechter. Tenslotte, heeft het systeem van bevelen voordelen in gevallen die een fysieke indringing in de panden en erven inhouden.

50. Wanneer voor het indringen geen externe hulp nodig is en geen toegang tot gebouwen is vereist, wordt het belang van het bevel bepaald door de ernst van de inbreuk zoals het aftappen van communicatie. Als het systeem van bevelen alleen wordt geïmplementeerd voor sommige soorten van aftappen, kan het het gebruik van aftapactiviteiten aanmoedigen zonder het vereiste bevel. Voor de implementatie van een geïntegreerde aanpak, vereist deze model wettekst een daartoe bevoegde officier een verzoek voor een bevelschrift in te dienen voor elk geval waarbij aftappen van belang wordt geacht.

51. Dit artikel introduceert de term 'bevel tot aftappen' met betrekking tot de goedkeuring om communicatie af te tappen. De werkgroep besprak het gebruik van de term 'bevelschrift' in plaats van de term 'instructie'. Men was het erover eens dat hoewel beide opties mogelijk waren, dat de term 'bevelschrift' de voorkeur had binnen het kader van deze wettekst aangezien het de gevallen dekt waar de toestemming voor het betreden van panden en erven noodzakelijk is. De rechter kan een speciale toegangsclausule opnemen in het bevelschrift. Indien de rechter in plaats daarvan een "aftapinstructie" uitvaardigt dan is er een noodzaak om een additioneel toegangsbevel uit te vaardigen. Daarom was het overeengekomen dat de term "bevel tot aftappen" zal worden gebruikt voor deze wettekst.

52. De uitvaardiging van de toestemming door de rechter is heel belangrijk, omdat de additionele onafhankelijkheid die wordt toegestaan door een rechterlijke uitspraak de nodige checks-and-balances met betrekking tot de ernst van de inbreuk. Volgens de model wettekst, worden alle bevelschriften die aftappen toestaan slechts uitgevaardigd door de rechter, waarbij geen onderscheid wordt gemaakt tussen bevelschriften die met rechtshandhaving en met nationale veiligheid hebben te maken. Hoewel sommige landen een onderscheid maken tussen bevelschriften die betrekking hebben tot misdrijven (voor de rechterlijke macht) of voor openbare veiligheid (voor de uitvoerende macht), is de alomvattende aanpak waarbij er een evenwicht wordt gezocht is tussen de openbare belangen en de rechten van het individu om te eisen dat alle toestemmingen worden goedgekeurd door de rechter.

53. De implementatie van de vereiste om aftappen door het hof te eisen is belangrijk voor het houden van een evenwicht met betrekking tot de rechten van het individu en de belangen van de staat. Het is essentieel voor het behoud van het vertrouwen van het grote publiek in het systeem dat er een onafhankelijke goedkeuring is van de handelingen op een dergelijk gevoelig gebied als het aftappen van communicatie. Dat zou niet bereikt worden door hooggeplaatste publieke functionarissen toe te staan deze aanvragen goed te keuren die worden ingediend door een ander deel van de administratie. De beste manier om te verzekeren dat er efficiënte checks-and-balances zijn is door de rechter te introduceren als een onafhankelijke scheidsrechter bij de noodzaak voor aftappen. De betrokkenheid van de rechterlijke macht in het proces van toestemming verlenen voor het aftappen garandeert dat een bevoegde officier die een bevelschrift aanvraagt de zaak grondig dient te overwegen. Dit zal ook de mogelijkheid voor machtsmisbruik verminderen.

54. Met betrekking tot het aanvraagproces, heeft de werkgroep lid 6 onder (1) gewijzigd door toe te voegen dat een aanvraag ex parte wordt gedaan. Deze wijziging is nodig voor het in staat stellen van een bevoegde officier om een bevel tot aftappenschrift aan te vragen geheel op basis van bewijsmateriaal dat door hem of haar wordt overlegd zonder de persoon van wie de communicatie wordt onderschept op de hoogte te stellen.

55. Er was tevens een behoorlijke discussie in de werkgroep over de bevoegdheid van de bevoegde officier voor het aanvragen van een bevel tot aftappen. Veel internationale benaderingen, waaronder regionale wetsvoorstellen (zoals de OECS model wet inzake het aftappen van communicatie) eisen dat de aanvraag wordt ingediend door de leidinggevende van het openbaar ministerie namens de bevoegde officier, zodat er een additioneel mechanisme in plaats is van checks-and-balances. Echter, de deelnemers aan de werkgroep gaven als mening dat landen, afhankelijk van hun nationale juridische tradities, een optie gegeven moeten worden om een bevoegde officier in staat te stellen een aanvraag te doen zonder tussenkomst van de leidinggevende van het openbaar ministerie. Men kwam overeen dat elke land deze optie moet

hebben terwijl zij aftapwetgeving implementeren. Daarom is het aan een land om te beslissen of de aanvraag zal worden gedaan door een bevoegde officier of door de leidinggevende van het openbaar ministerie namens de bevoegde officier.

56. Lid (2) van artikel 6 geeft aan dat een aanvraag voor een bevel tot aftappen schriftelijk moet worden gedaan en vergezeld moet zijn van een beëdigde verklaring waarin de omstandigheden waaronder de aanvraag wordt gedaan wordt gemaakt. Het doel van dit lid is om de vereisten vast te stellen voor de vorm van de aanvraag en een aantal eisen waaraan elke aanvraag moet voldoen. Dit is nodig om te verzekeren dat het aanvraagproces voor de toestemming beantwoordt aan bepaalde vereisten, en, aangezien alle documenten schriftelijk moeten worden aangeleverd, en om transparantie te garanderen voor het aanvraagproces.

57. In overeenstemming met lid (2) onder (a)-(i), moeten aanvragen schriftelijk worden gedaan en de redenen voor de toestemming tot aftappen geven. Deze bepaling verzekert dat er een feitelijke basis is voor het verlenen van het bevel tot aftappen. aftappen mag slechts de specifieke verdachte dekken of veronderstelde contactpersonen. Een schriftelijke aanvraag vergezeld van een beëdigde verklaring garandeert dat een “verkennende” of algemene aftappen niet wordt toegestaan.

58. De vorm van het ondersteunend bewijsmateriaal (beëdigde verklaring) werd intensief besproken. De meeste nationale benaderingen vereisen een voorafgaande toestemming van de rechter om een aftappen van communicatie in te stellen. Echter, het aanvraagproces verschilt van rechtsgebied tot rechtsgebied. Hoewel het gros van de landen het erover eens zijn dat aanvragen schriftelijk dienen te worden ingediend, variëren de normen betreffende ondersteunend bewijsmateriaal aanzienlijk. Sommige landen vereisen dat bewijsmateriaal wordt gepresenteerd in de vorm van een beëdigde schriftelijke verklaring (Canada, de VSA, Australië, OOSC Model wet) terwijl andere rechtsgebieden de benadering volgen van het horen van viva voce getuigenis (b.v. Denemarken, Finland, Slovenië).

59. Lid (2) van artikel 6 is gebaseerd op het indienen van schriftelijk ondersteunend bewijsmateriaal. Dit model werd gekozen door de werkgroep, ten eerste, omdat het wijdverbreid is in de common-law landen. Ten tweede, zijn bepalingen voor het indienen van schriftelijke verklaringen geïmplementeerd als gevolg van het mogelijke verschil bij het reguleren van het opnemen en de transcriptie van mondeling bewijsmateriaal. De verplichting om ondersteunend bewijsmateriaal op schrift in te dienen is een noodzakelijke maatregel voor het verzekeren van transparantie bij de aanvraag en om de mogelijkheid tot misbruik te voorkomen.

60. Om de rechter de mogelijkheid te geven een geïnformeerde beslissing te nemen over of een bevelschrift wordt uitgevaardigd of niet, verplichten leden (2) onder (a) – (2) onder (i) de bevoegde officier om de rechter van informatie te voorzien die aantoont dat aftappen nodig is met de beoogde doelstelling. Om te garanderen dat aftappen slechts voor een bepaalde zaak wordt gegeven, is in de wetgeving opgenomen de vereiste om een gedetailleerde beëdigde verklaring in te dienen, waarin alle bijzonderheden van de zaak zijn neergelegd, waaronder de feiten en andere gronden waarop de aanvraag wordt ingediend; de periode waarvoor het bevelschrift wordt gevraagd van toepassing te zijn; de basis waarom men gelooft dat het bewijsmateriaal inzake de grondslag waarop de aanvraag wordt gemaakt, verkregen zal worden via aftappen. Bovendien, de vereiste van lid (2) onder (g) benadrukt de noodzaak om een rechtvaardiging te geven voor het aftappen als een maatregel als “laatste uitweg”. Dit lid vereist dat bijzonderheden worden gegeven over de moeilijkheden die zouden zijn opgekomen indien het onderzoek beperkt wordt tot conventionele methoden of waarom conventionele methoden hebben gefaald.

61. Lid (3) geeft de bijkomende vereisten voor de zaak wanneer een aanvraag wordt gemaakt op basis van nationale veiligheid. In dit geval, moet het vergezeld zijn van een schriftelijke toestemming getekende door [Minister]. Deze bepaling heeft als doel het veiligstellen dat de bijzonderheden van de zaak betreffende nationale veiligheid worden verstrekt aan de rechter.

62. Voor het ontwikkelen van garanties voor de geheimhouding van de aanvraag voor het onderscheppeingsbevel, brengen leden (4) en (5) een aantal maatregelen naar voor die de toegang tot een aanvraag voor bevel tot aftappen beperken. Zij leggen de vereisten neer voor de geheimhouding van de aanvraag en de procedures die het niet openbaar maken van de informatie in de aanvraag garanderen. Dit is belangrijk want het behandelen van aanvragen en het beheren van de bescheiden door de rechter kunnen problemen opleveren bij het geheim houden van de informatie tijdens het aanvraagproces, indien de toegang tot de aanvraag niet wordt beperkt tot een bepaald aantal functionarissen. De rechter moet garanderen dat alle documenten die betrekking hebben op aanvragen voor bevelschriften in bewaring worden genomen. Het is essentieel dat dergelijke documenten (waaronder de bevelschriften zelf) geheim worden gehouden. Het hele concept van aftappen als geheim onderzoek kan worden ondermijnd indien enige informatie over de aanvragen wordt openbaar gemaakt.

63. De werkgroep besliste om een bijkomende bepaling aan artikel 6 toe te voegen – lid 6 waarbij het bewust maken van een valse getuigenis door de persoon in de aanvraag voor het bevel tot aftappen of de beëdigde verklaring strafbaar wordt gesteld. Deze bepaling is een beveiliging om te voorkomen dat er enige mogelijk misbruik wordt gemaakt van het ex parte aanvraagproces wanneer de beslissing van de rechter volledig is gebaseerd op het bewijsmateriaal dat wordt overlegd door de aanvrager. De persoon van wie de communicatie wordt onderschept heeft geen kans het ondersteunend bewijsmateriaal in twijfel te trekken op het moment van de aanvraag. Daarom, wanneer een bevoegde officier de beëdigde verklaringen afneemt, zal hij of zij strafbaar zijn indien valse verklaringen willens en wetens zijn verstrekt.

Artikel 7. Openbaarmaking van aanvraag

64. Om de geheimhouding van het onderzoek te beschermen en om een garantie te geven voor de geheimhouding van de aanvraag, stelt artikel 7 de openbaarmaking van het bestaan van een aanvraag voor een bevel tot aftappen strafbaar. Deze strafbaarstelling is noodzakelijk omdat een opzettelijke inbreuk op de veiligheid bij de aanvraag kan leiden naar een samenzwering voor het ondermijnen van het onderzoek en het beperken van de rechtsbedeling.

65. Echter, om een balans te behouden en om het recht van een persoon om juridisch advies in te winnen te beschermen, maken leden (2) en (3) een uitzondering met betrekking tot de reikwijdte van de strafbaarstelling van openbaarmaking aan een advocaat.

Artikel 8. Het uitvaardigen van het bevel tot aftappen

66. Het doel van dit artikel is om een kader te creëren voor het geven van toestemming voor het aftappen van communicatie nadat een bevel tot aftappen is aangevraagd. Aangezien de aanpak is het beperken van de bevoegdheid om af te tappen tot een beperkt aantal omstandigheden, verzekert dit artikel dat er robuuste waarborgen aanwezig zijn en de [rechter] tevreden is met de noodzaak voor het uitvoeren van aftappen.

67. Als een waarborg tegen de bevoegdheid om communicatie af te tappen, stelt lid (1) een aantal omstandigheden vast die zullen worden geanalyseerd en bevestigd door een [rechter] voorafgaand aan de uitvaardiging van het bevel tot aftappen. De eerste serie van vereisten neergelegd door lid (1) onder (a) (i), (ii), (iii) heeft betrekking op de aard van de criminele activiteit die de bevoegdheid om af te tappen rechtvaardigt. Een [rechter] die het aftappen goedkeurt zal tevredengesteld zijn dat het verkrijgen van de informatie in het belang is van de nationale veiligheid of voor het voorkomen of vaststellen van een bepaalde ernstige misdaad, waaronder zaken van wederzijdse rechtsbijstand, of informatie die verkregen is van het aftappen mogelijkerwijs van assistentie kunnen zijn bij onderzoek naar de zaken die hierboven zijn genoemd.

68. Nationale veiligheid – lid (1) onder (a) (i) vertegenwoordigt een bepaalde grondslag voor de inbreuk op het recht van een persoon op privacy van communicatie. Deze grondslag voor het verlenen van toestemming voor het aftappen kan de kwestie van het in evenwicht houden van belangen van de staat en de privacy van een individu opwerpen. De vrijheid van inmenging in de privacy is niet absoluut, aangezien het moet worden afgezet tegen de concurrerende publieke belangen. De beperking van deze vrijheid moet nodig zijn voor het uitoefenen van de concurrerende belangen en de nationale veiligheid is daar een van. De vereiste voor een rechterlijke toestemming kan een balans brengen en het misbruik voorkomen van aftappen op basis van nationale veiligheid.

69. De term “nationale veiligheid” is niet gedefinieerd voor de doelstelling van deze wettekst, aangezien het in overeenstemming zou moeten zijn met de wetgeving in elk nationaal rechtsgebied. Het is belangrijk een brede interpretatie te vermijden van deze grondslag en om het te beperken tot bepaalde zaken die, natuurlijk, zouden afhangen van het implementeren door de staat van deze model wettekst.

70. Lid (1) onder (a) (ii) verstrekt de tweede grondslag voor het verstrekken van een bevel tot aftappen: voorkomen of vaststellen van enige overtreding neergelegd in de bijlage, waar er redelijke gronden zijn om te geloven dat een dergelijke overtreding is, wordt of kan worden begaan. Dit lid verwijst naar de bijlage die wordt geïntroduceerd voor het vaststellen van een serie van bepaalde ernstige misdrijven die aftappen rechtvaardigen. Het leidend principe voor het uitvoeren van deze bepaling is dat de onderzoeksmiddelen in verhouding moeten staan tot de ernst van de zaak die wordt onderzocht. Aangezien aftappen van communicatie zonder toestemming van de partijen een ernstige inmenging is in de privacy, kan een dergelijke maatregel slechts worden gerechtvaardigd indien de overtreding die wordt onderzocht van ernstige aard is.

71. Lid (1) onder (a) (iii) is essentieel voor het aanpakken van de kwestie van wederzijdse rechtsbijstand bij het onderzoek naar ernstige misdrijven. Deze bepaling is essentieel aangezien de nieuwe communicatiemiddelen grensoverschrijdende verzending van data kan inhouden. Dit maakt internationale samenwerking van belang. Het land zal de mogelijkheid hebben te reageren op verzoeken voor wederzijdse rechtsbijstand waarbij het aftappen van communicatie vereist is.

72. De bepaling van lid (1) onder (b) is essentieel voor het waarborgen dat het aftappen slechts wordt goedgekeurd in relatie tot het onderzoek van een specifiek geval. Het is nodig erin te voorzien dat een rechter het aftappen slechts mag goedkeuren met betrekking tot een specifiek misdrijf, nationale veiligheidskwestie of wederzijds rechtsbijstandsverzoek en slechts als het aftappen het onderzoek ondersteunt. Er moet een grondslag zijn voor verdenking en aftappen moet niet worden goedgekeurd op basis van een kleine kans dat men een misdrijf zal ontdekken.

73. Het uitvaardigen van een bevel tot aftappen wordt verder beperkt onder lid (1) onder (c) tot de gevallen waarin andere procedures voor het verkrijgen van informatie niet of mogelijk niet succesvol zullen zijn of te gevaarlijk om toe te passen in de omstandigheden of niet praktisch zijn door de urgentie van het geval. Deze bepaling is nodig om te zorgen dat aftappen niet worden toegestaan tenzij de informatie niet op redelijke wijze beschikbaar is met behulp van minder intensieve methoden. De toestemming wordt gerechtvaardigd niet op basis van een relatief gemak van het toepassen van aftaptechnieken, maar de redelijkheid om het uit te voeren. Deze rechtvaardiging brengt evenwicht tussen doeltreffendheid en het concurrerend publiek belang bij het geven van bescherming voor de privacy van communicatie. Het garandeert dat de onderzoeksmiddelen in verhouding staan tot de urgentie en ernst van het misdrijf.

74. Lid (1) onder (d) geeft aan dat een bevel tot aftappen slechts uitgevaardigd kan worden indien het in het beste belang is van de rechtsbedeling. Het verplicht de rechter rekening te houden met deze belangen bij het verstrekken van de toestemming. Dit is een additionele waarborg voor het opleggen van striktere controle indien het rechtshandhavingsinstituut slechts informatie wenst te vergaren.

75. Als bijkomende waarborg die verzekert dat elke aanvraag wordt beslist op een individuele basis, stelt lid (2) de rechter in staat bijkomende informatie te vereisen die betrekking heeft op de aanvraag.

Artikel 9. Reikwijdte en vorm van het bevel tot aftappen

76. Artikel 9 legt regels neer met betrekking tot de reikwijdte en vorm van het bevel tot aftappen. Om te verzekeren dat de inmenging in de privacy tot een minimum blijft beperkt, is het nodig de formele vereiste vast te stellen voor de toestemming en slechts toe te staan dat het wordt uitgevoerd door een bepaalde persoon en slechts voor een bepaald adres/ persoon/ communicatie. Een serie van vereisten met betrekking tot de reikwijdte en vorm van het bevel tot aftappen is erop gericht een zeker formeel kader vast te stellen voor ieder aftapgeval, de bevoegdheid af te tappen te beperken en het effect van het aftappen op derden te verminderen.

77. Aangezien geen aftappen kan plaats hebben zonder bevel tot aftappen, moet het bevelschrift specifiek zijn met betrekking tot wat de persoon die het aftappen uitvoert kan doen. Verder, voor het waarborgen van de privacy, moet de rechter de bevoegdheid hebben die voorwaarden op te leggen waarvan hij denkt dat die passend zijn.

78. Volgens lid (1), kan een bevel tot aftappen worden uitgevaardigd in de voorgeschreven (schriftelijke) vorm. De schriftelijke vorm is essentieel voor het in evenwicht houden van twee belangrijke componenten: ten eerste, om het recht tot aftappen en om bijstand te vragen veilig te stellen en ten tweede om dit recht te beperken tot een bepaalde persoon/ adres/ communicatie. Op deze wijze vormt de schriftelijke vorm van het bevel tot aftappen een tegenwicht voor de noodzaak een bepaalde inbreuk uit te voeren met de noodzaak om mogelijk misbruik te elimineren. Het is erg belangrijk dat een bevel tot aftappen zo specifiek als mogelijk is. Lid (1) onder (a), (b), (c) en (d) geven de reikwijdte van de toestemming aan met betrekking tot de bevoegdheid van de persoon die het uitvoert.

79. Lid (2) dient als een maatregel voor het in evenwicht brengen van de bevoegdheid verleend op grond van lid (1). Voor het strikt beperken van de bevoegdheid tot slechts een bepaalde persoon en het voorkomen van enige vorm van misbruik, vereist lid (2) dat of de persoon of de specifieke panden en erven die moeten worden onderschept worden genoemd of beschreven in het bevelschrift. Om te voldoen aan deze bepaling, zal het bevel tot aftappen de communicatie identificeren die onderschept dienen te worden naar of van een bepaald individu gespecificeerd in het bevel tot aftappen of een bepaald adres gespecificeerd in het bevel tot aftappen. Dit is noodzakelijk voor het waarborgen dat het aftappen slechts kan worden toegestaan voor het onderzoek van een bepaald misdrijf en niet als een algemene monitoringsmaatregel.

80. Er was een discussie in de werkgroep met betrekking tot de identificatie van het de panden en erven of communicatieapparaten waarvan/ waarnaar de communicatie wordt verstuurd. De werkgroep was het erover eens dat de term 'adres' gebruikt moet worden voor het identificeren van een bepaald stel ruimten*, of een telefoonnummer, of een emailadres voor het aftappen. Volgend op deze discussie kwam de werkgroep overeen dat de definitie van 'adres' alsvolgt gedefinieerd moet worden: artikel 9 “adres” omvat panden en erven, emailadres, telefoonnummer of enige andere aanwijzing gebruikt voor het identificeren van telecommunicatienetwerken, -aanbieders of apparaten.

81. Lid (3) geeft de mogelijkheid voor het incorporeren van een toegangsclausule in het bevel tot aftappen. De uitvoering van het bevel tot aftappen kan het verschaffen van toegang tot privé panden en erven vereisen. In de afwezigheid van een machtiging om de panden en erven te betreden, zou een bevoegde officier een apart bevelschrift moeten aanvragen onder de bestaande nationale wetgeving die hem zou machtigen de beoogde panden en erven te betreden. Echter, aangezien het aftappen slechts kan worden gegeven voor een onderzoek van ernstige misdrijven is een aparte aanvraag niet gewenst aangezien het kan leiden tot vertraging in de uitvoering van het bevel tot aftappen.

82. Voor het beschermen van de privacy-rechten, zal de clausule die tot het betreden van de panden en erven machtigt slechts als doel hebben het aftappen en niets anders. De bepaling van lid (3) geeft de machtiging tot het betreden van alle panden en erven gespecificeerd in het bevelschrift met als doel het installeren, onderhouden, gebruiken of terughalen van alle apparatuur die is gebruikt voor het aftappen van communicatie aangegeven in het bevelschrift. Om te waarborgen dat de verwachting voor misbruik wordt geëlimineerd, vereist dit lid dat alle panden en erven precies worden omschreven in de toegangsclausule en een bevoegde officier mag die slechts betreden met dat specifiek doel.

83. Lid (4) vereist de identificatie van een bevoegde officier namens wie de aanvraag wordt gemaakt; de persoon die het bevel tot aftappen zal uitvoeren en de aanbieder van telecommunicatiediensten aan wie het bevel tot aftappen geaddresseerd moet worden. Deze bepaling is een belangrijk waarborg voor het beperken van het aantal mensen die in staat worden gesteld het aftappen uit te voeren. Verder, beantwoordt het aan het algemeen beginsel dat bevelschriften zo specifiek als mogelijk moeten zijn om de mogelijkheid tot misbruik te voorkomen.

84. De model wettekst stelt landen in staat een persoon te kiezen die werkelijk het aftappen uitvoert. Voor landen met beperkte rechtshandhavingscapaciteit, evenals in de gevallen waarbij die politie onvoldoende middelen heeft, is er een optie om te definiëren dat de aanbieder van telecommunicatiediensten verplicht is de communicatie af te tappen. Echter, de inrichting van lid (4) maakt het de rechter mogelijk te beslissen wie het aftappen zal uitvoeren in elk specifiek geval.

85. Daarnaast kan het bevel tot aftappen dat de toegangsclausule bevat de toegestane tijd van betreding specificeren evenals enige bijkomende maatregelen die moeten worden genomen voor het uitvoeren van de maatregel.

86. Aangezien het bevel tot aftappen slechts wordt uitgevaardigd op basis van specifieke gronden, die kenmerkend zijn voor elk geval, zal de [rechter] de bevoegdheid worden gegeven bijkomende voorwaarden op te leggen die de aard van de specifieke zaak zullen weergeven. Leden (5) en (6) worden geïmplementeerd om de [rechter] in staat te stellen aanvullende bepalingen, voorwaarden of beperkingen te definiëren die betrekking hebben op het aftappen van communicatie toegestaan in het bevelschrift.

Artikel 10. Duur en vernieuwing van bevel tot aftappen

87. Artikel 10 heeft betrekking op de duur en vernieuwing van een bevel tot aftappen. Het belangrijkste doel van dit artikel is het beperken van de machtiging tot aftappen tot een bepaalde tijdsduur om een aftappen zonder einde te voorkomen.

88. Verder, voorziet dit artikel in een regeling voor de vernieuwing van het bevel tot aftappen wanneer de geldigheidsduur vastgesteld door deze model wettekst en/ of aangegeven in het bevel tot aftappen te kort was voor het doel van het doen van het aftappen. De laatste optie is kritisch wanneer het nodig is het aftappen voort te zetten zonder een onderbreking veroorzaakt door een nieuwe aanvraag.

89. De beperking van de duur van het bevel tot aftappen tot een bepaald (redelijk korte) tijdsperiode is een normale aanpak in de meeste rechtsgebieden. Echter, de vastgestelde tijdsperiode varieert aanzienlijk – b.v. 3 tot 6 maanden (Australië), 6 maanden (OOSC Model wet), 3 maanden (Hong Kong).

90. De noodzakelijke duur van het aftappen werd intensief besproken en verschillende aspecten zijn overwogen. Aan de ene kant, is het nodig weer te geven dat aftappen een ernstige maatregel is die niet gebruikt dient te worden tenzij het absoluut noodzakelijk is. Dus, zal de duur van het bevelschrift worden beperkt. Verder, hoe langer de duur is van een bevelschrift, hoe groter de mogelijkheid dat persoonlijke informatie, die niet relevant is voor een onderzoek, wordt onderschept. Deze factor wordt in overweging genomen wanneer de geldigheidsperiode wordt vastgesteld.

91. Aan de andere kant, kan het onderzoek naar ernstige misdrijven tijd nemen. Indien de maximale duur te kort is, kan het leiden tot een groot aantal aanvragen voor vernieuwing en hulpbronnen blokkeren.

92. Lid (1) legt neer dat de geldigheidsduur van een bevel tot aftappen [90] dagen niet zal overschrijden. De voorgestelde duur – 90 dagen – is een gemiddelde tijdsduur die is afgeleid van nationale benaderingen. Een land kan beslissen om de tijdsduur te wijzigen binnen de implementatie. De geldigheidsduur zal worden gespecificeerd door een rechter. Dit lid behandelt tevens de aanvraag voor de vernieuwing van een bestaand bevelschrift.

93. Aangezien de machtiging van aftappen afhankelijk is van een ex parte aanvraagproces, is het noodzakelijk dezelfde waarborgen te geven voor het vernieuwen van het bevel tot aftappen die zijn geïmplementeerd met betrekking tot de initiële aanvragen. Daarom zal de vorm en inhoud van de aanvraag hetzelfde zijn. Een vernieuwing van het bevelschrift kan worden verleend door een rechter op basis van een aanvraag gedaan door een leidinggevende van het Openbaar Ministerie namens een bevoegde officier op enig moment voordat het bevelschrift (of enige huidige vernieuwing van het bevelschrift) is verlopen. Een land kan, afhankelijk van de nationale wetgeving, een bevoegde officier toestaan een aanvraag tot vernieuwing te doen zonder tussenkomst van de leidinggevende van het Openbaar Ministerie.

94. De werkgroep besprak of de aanvraag voor vernieuwing door dezelfde procedure moet gaan en dezelfde vorm moet hebben als de initiële aanvraag. De werkgroep besloot dat de procedure voor vernieuwing zoveel als mogelijk moest overeenkomen met de procedure voor de initiële aanvraag om alle waarborgen te behouden en het risico van misbruik van de macht om af te tappen te voorkomen. De aanvraag voor vernieuwing dient de omstandigheden voor vernieuwing te rechtvaardigen, de redenen geven voor de periode van vernieuwing, en aangeven wat gedaan dient te worden voor het uitvoeren van het bestaande bevelschrift. Dat is waarom leden (3) en (4) dezelfde eisen neerleggen voor de aanvraag voor vernieuwing die zijn vastgesteld voor de initiële aanvragen. Verder, om de volledige bijzonderheden van het geval te verstrekken, zal de aanvraag informatie bevatten betreffende de uitvoering van het huidige bevel tot aftappen. Dit is nodig om te verzekeren dat het aftappen redelijk is en gericht is op het onderzoeken van een bepaald misdrijf. Voor het mogelijk maken van een vlotte bestudering van elke aanvraag voor vernieuwing, geeft lid (5) de rechter de mogelijkheid bijkomende informatie te eisen voor het behandelen van de aanvraag.

95. Lid (6) legt een waarborg neer die betrekking heeft op de gronden voor aftappen: een rechter kan slechts een bevel tot aftappen vernieuwen als hij of zij tevreden is gesteld dat de omstandigheden die de grondslag vormden voor de machtiging tot aftappen nog steeds gelden.

96. Ingevolge lid (7) mag de duur van iedere vernieuwing van een bevel tot aftappen de algemene geldigheidsduur niet overschrijden (zoals voorgesteld in de wettekst [90] dagen) en zal worden gespecificeerd door de rechter in de vernieuwing. Een land kan een andere termijn voor de geldigheid van de hernieuwde aftapping specificeren.

97. Aangezien aftappen een ernstige inbreuk op de privacy betekent, is het heel belangrijk te verzekeren dat het wordt beëindigd op het moment dat er geen noodzaak meer is voor het aftappen. Om dit beginsel te garanderen, vereist lid (8) een bevoegde officier aan wie het bevelschrift wordt uitgevaardigd of een persoon die namens hem of haar handelt om de herroeping van het bevel tot aftappen aan te vragen indien blijkt dat een bevel tot aftappen niet langer nodig is.

Artikel 11: Wijziging van bevel tot aftappen

98. Artikel 11 stelt een bevoegde officier in staat een wijziging aan te vragen van een bestaand bevel tot aftappen indien de omstandigheden zijn gewijzigd. Dit kan van toepassing zijn in gevallen waar het adres van de panden en erven van de verdachte, telefoonnummers en andere identificatiecriteria gespecificeerd in het bevel tot aftappen zijn veranderd. Het aanvraagproces

blijft hetzelfde om te zorgen dat alle waarborgen van toepassing zijn. Een aanvraag voor wijziging van het bestaande bevel tot aftappen dient gedaan te worden door de leidinggevende van het Openbaar Ministerie namens de bevoegde officier of door een bevoegde officier, afhankelijk van de benadering die een land zal kiezen met betrekking tot de procedure voor de initiele aanvraag. De grondslagen voor de uitvoering van het aftappen zullen hetzelfde blijven.

Artikel 12. Herroeping van het bevel tot aftappen

99. Dit artikel is geïmplementeerd om te garanderen dat het bevel tot aftappen wordt herroepen wanneer er enig misbruik is van het recht op aftappen of indien het aftappen niet langer nodig is. Dit is een essentieel mechanisme om te garanderen dat het aftappen volledig voldoet aan de vereisten van de model wettekst. Daarnaast moet het garanderen dat de inmenging slechts wordt gebruikt als een uitzonderlijke maatregel. Dit artikel legt de grondslagen vast en de procedure voor de herroeping van de machtiging tot aftappen. De werkgroep heeft de voorgestelde term 'beëindiging' verandert in de term 'herroeping'.

100. Volgens lid (1) kan een bevel tot aftappen worden herroepen door een rechter indien een bevoegde officier nalaat een rapport in te dienen over de voortgang in overeenstemming met artikel 15; of indien de rechter bij ontvangst van dergelijk voortgangsrapport tot de slotsom komt dat de doelstellingen van het bevel tot aftappen zijn bereikt; of de grondslagen waarop het bevel tot aftappen was uitgevaardigd vervallen zijn; of de voorwaarden van de initiële aanvraag zijn veranderd op dusdanige wijze dat een aanvraag niet meer mogelijk zou zijn.

101. Voor het vaststellen van de formele vereisten met betrekking tot de herroeping en om te verzekeren dat een bevoegde officier direct in kennis wordt gesteld van de herroeping, definieert lid (2) dat de kennisgeving van de herroeping van het bevelschrift in schriftelijk vorm moet worden doorgestuurd naar de bevoegde officier.

102. De doelstelling van lid (3) is om te garanderen dat indien een bevel tot aftappen is herroepen, de uitvoering direct stopt. Van de bevoegde officier wordt vereist dat enig aftapapparaat dat was geïnstalleerd voor de uitvoering van het aftappen wordt verwijderd. Het verwijderen dient zo snel als mogelijk plaats te vinden na de ontvangst van de kennisgeving over de herroeping.

Artikel 13. Gevolgen van een herroeping

103. Dit artikel voorziet in een waarborg in geval van het herroepen van een bevel tot aftappen. Aangezien het bevel tot aftappen wordt herroepen wanneer niet langer aan de vereisten van een aftappen vastgesteld bij wet wordt voldaan, is het nodig te verzekeren dat de onderschepte data niet worden gebruikt in een strafrechtelijke procedure. Artikel 13 voorziet erin dat bewijsmateriaal dat was verzameld terwijl een bevelschrift was herroepen niet toelaatbaar is tenzij de rechter besluit dat het toelaten van dergelijk bewijsmateriaal het proces niet onrechtvaardig maakt.

Artikel 14. Spoedaanvraag

104. Artikel 14 is essentieel in dringende gevallen waarbij aftappen zo snel als mogelijk moet worden uitgevoerd omdat vertragingen het onderzoek zouden belemmeren. Het voorziet in de grondslagen en procedures voor dergelijke urgente aanvragen.

105. In die gevallen zijn mondelinge aanvragen toegestaan. Het is niet erg verwachtbaar dat een bevoegde officier in dringende gevallen de tijd heeft voor het opstellen en indienen van een schriftelijke aanvraag bij de rechter. De werkgroep heeft daarom besloten dat er een noodmechanisme dient te zijn dat een bevoegde officier in staat stelt een bevelschrift te verkrijgen in die omstandigheden.

106. Bijna alle nationale benaderingen staan in bepaalde gevallen urgente toestemming van aftappen toe. De procedures zijn opgesteld in overeenstemming met de OOSC model wet en de wetgeving van Nieuw Zeeland.

107. Volgens lid (1) kan een rechter in een dringende geval vrijstelling geven voor de vereisten van een schriftelijke aanvraag en de leidinggevende van het Openbaar Ministerie toestaan namens een bevoegde officier een mondelinge aanvraag te doen voor een bevel tot aftappen. De rechter zal het bevelschrift uitvaardigen indien hij of zij ervan overtuigd is dat er omstandigheden zijn die het verlenen van een bevel tot aftappen onder artikel 8 zou rechtvaardigen.

108. Om de formele procedure van de aanvraag te verzekeren, legt lid (2) de vereisten neer waaraan een aanvraag voor een nood bevel tot aftappen moet voldoen. Ten eerste, moet het de informatie bevatten waarnaar wordt verwezen in lid (2) van artikel 6 wat is vereist voor de aanvraag voor een bevel tot aftappen; ten tweede moet het de bijzonderheden aangeven van de urgentie van de zaak of de andere uitzonderlijke omstandigheden waarom volgens de bevoegde officier een mondelinge aanvraag gerechtvaardigd is. Een mondelinge aanvraag moet ook overeenstemmen met alle instructies die door de [rechter] kunnen worden uitgevaardigd.

109. Volgens lid (3) vaardigt een rechter een nood bevel tot aftappen slechts uit indien hij of zij ervan overtuigd is dat er redelijke gronden zijn om te geloven dat het bevel tot aftappen wordt uitgevaardigd en het redelijkerwijs niet praktisch is om een schriftelijke aanvraag in te dienen. Deze bepaling is erop gericht te garanderen dat een dringend bevelschrift slechts kan worden verleend in uitzonderlijke omstandigheden.

110. Er was een discussie in de werkgroep over de mogelijkheid regels toe te passen voor een dringende aanvraag voor de procedure van het hernieuwen van een bestaand bevel tot aftappen. De belangrijkste zorg was hoe de juiste checks-and-balances ingebracht door de clausules inzake de dringende aanvraag van toepassing zouden zijn in dit geval. De werkgroep kwam overeen geen mondelinge aanvraag toe te staan voor standaardgevallen voor hernieuwing.

111. Om te verzekeren dat de bescheiden worden bewaard voor elke aanvraag, vereist lid (4) dat de rechter een schriftelijke aantekening maakt van de bijzonderheden van de aanvraag indien een noodbevelschrift wordt uitgevaardigd.

112. Lid (5) definieert dat een bevel tot aftappen uitgevaardigd op basis van een mondelinge aanvraag dezelfde reikwijdte moet hebben als een standaard bevel tot aftappen. Deze bepaling is erop gericht dat verschillende normen worden vermeden met betrekking tot dringende aanvragen en normale procedures. De werkgroep besprak of het dringende bevelschrift schriftelijk of mondeling dient te worden uitgevaardigd. Men kwam overeen dat het bevel tot aftappen uitgevaardigd op basis van een mondelinge aanvraag moet worden gedaan in een schriftelijke vorm zoals vereist door artikel 9.

113. De geldigheidsduur voor elk nood bevel tot aftappen wordt vastgelegd in lid (6) en moet [48] uur zijn te tellen vanaf het moment dat het werd uitgevaardigd. Een land kan kiezen voor een andere geldigheidsduur voor het dringende bevel tot aftappen. Na die periode vervalt het bevelschrift. Volgens lid (7) moet een schriftelijke aanvraag en beëdigde verklaring worden ingediend in overeenstemming met de bepalingen van artikel 6 binnen [48] uur. Deze bepaling is erop gericht te verzekeren dat elke aanvraag voor een bevel tot aftappen transparant is en uiteindelijk wordt gedaan in schriftelijke vorm. Daarnaast is het erop gericht de rechter de gelegenheid te geven de noodbeslissing te herzien indien er niet voldoende bewijsmateriaal is voor het verlenen van toestemming tot aftappen.

114. Er was een discussie in de werkgroep over de procedure (schriftelijke aanvraag) volgend op de uitvaardiging van een dringend bevel tot aftappen. Sommige deelnemers aan de consultatieworkshop waren bezorgd over de noodzaak het papierwerk te doen in een korte tijdspanne. Echter, de werkgroep was het erover eens dat het nodig is een schriftelijke aanvraag te eisen om de mogelijkheid tot misbruik te elimineren. Aangezien 48 uur slechts een aanbevolen duur is van de noodbevelschriften, kan een land ervoor kiezen een langere geldigheidsduur vast te stellen voor de dringend verstrekte bevelschriften.

115. Lid (8) legt een procedure vast voor het herzien van de beslissing inzake het verlenen van een noodbevelschrift. Deze procedure is noodzakelijk om te garanderen dat de afwijking van de formele aanvraagprocedure gerechtvaardigd is of, indien niet, wordt het bevelschrift ingetrokken.

Artikel 15: Voortgangsrapport

116. Het voortgangsrapport is een maatregel die nodig is voor het toezicht op het bevel tot aftappen. Het stelt een rechter in staat die het bevelschrift heeft uitgevaardigd er zeker van te zijn dat het aftappen wordt uitgevoerd in overeenstemming met de wet en de wettelijke goedkeuring. Deze aanpak wordt bij voorbeeld gebruikt in de OOSC modelwet op aftappen van communicatie. Artikel 15 geeft een rechter, die een bevel tot aftappen heeft uitgevaardigd, de bevoegdheid de bevoegde officier namens wie de relevante aanvraag was gedaan, te bevelen om schriftelijk te rapporteren over de voortgang die is gemaakt of enige ander zaak die de rechter van belang acht. Dit bevel is bindend en kan de intrekking van het bevel tot aftappen tot gevolg hebben zoals neergelegd in artikel 12. Het verzoek onder artikel 15 kan worden gedaan door een rechter op het moment van uitvaardiging van het bevel tot aftappen, of op enig ander moment voor de vervaldatum.

117. De vereiste voor een voortgangsrapport is er ook op gericht evenwicht te brengen in de administratieve en judiciële controlesystemen.

Artikel 16: Eindrapport

118. Dit artikel is een optie die een land kan implementeren als additionele waarborg. De vereiste van een eindrapport over de resultaten van een aftapping is in sommige landen, zoals Australië en Nieuw Zeeland, ingevoerd. Het vereist dat een bevoegde officier een eindrapport indient met betrekking tot de bijzonderheden van het aftappen, waaronder de resultaten die zijn behaald. Met betrekking hiertoe, dient het eindrapport tevens als een bijkomend instrument voor het veiligstellen van naleving van de regels over geheimhouding van onderschepte communicatie, zoals voorzien in artikel 23.

119. Lid (2) voorziet in een aantal vereisten die betrekking hebben op de vorm en inhoud van het eindrapport. Het moet worden opgemerkt dat er speciale aandacht wordt besteed aan het vernietigen van irrelevante informatie als waarborg.

120. Echter, een land kan problemen ervaren bij het implementeren van deze bepaling aangezien de verplichting bijkomend papierwerk inhoudt en mogelijke zorgpunten betreffende privacy. Na een intensieve discussie kwam de werkgroep overeen dat de landen moeten beslissen of zij een eindrapport zullen eisen of niet.

Deel III

HOOFDSTUK III – UITVOERING VAN HET AFTAPPEN

121. Hoofdstuk III legt de plichten en verantwoordelijkheden vast van openbare lichamen (bevoegde officier) en personen voor het uitvoeren van het aftappen. Dit hoofdstuk schept het essentieel kader voor het proces van het uitvoeren van het aftappen. Het omvat regelingen betreffende de verplichting voor het geven van bijstand. Het bevat tevens een bepaling die handelt over de geheimhouding van de onderschepte informatie en de verplichting onderschepte bescheiden te vernietigen. Strikte regelgeving en waarborgen worden voorzien voor het garanderen dat informatie geheim wordt gehouden en irrelevante data worden vernietigd.

Artikel 17: Uitvoering van bevel tot aftappen

122. Artikel 17 is erop gericht de bevoegde officier in staat te stellen communicatie gespecificeerd in het bevelschrift af te tappen in overeenstemming met de voorwaarden daarvan. Daarnaast verleent het de bevoegde officier de bevoegdheid te eisen van een persoon die in het bevelschrift is gespecificeerd de communicatie af te tappen of te helpen bij de uitvoering van het aftappen. Deze verplichting om bijstand te verlenen is cruciaal omdat rechtshandhavingslichamen vaak afhankelijk zijn van de ondersteuning van de persoon die specifieke kennis heeft over telecommunicatienetwerken of die exploiteert. Echter de verplichting om bijstand te verlenen is beperkt tot de reikwijdte van de machtiging en de plichten gespecificeerd in het bevel tot aftappen. Deze bepaling is essentieel om te verzekeren dat er geen onredelijke eisen worden gesteld met betrekking tot de persoon van wie wordt geëist dat hij bijstand verleent. Het voorziet in het recht om een verzoek om bijstand te weigeren dat niet in overeenstemming is met het bevel tot aftappen.

123. Lid (3) is nodig omdat aftappen vaak een inbreuk doet op de privacy niet alleen van de persoon van wie de communicatie onderschept worden. Het recht van derden op privé communicatie wordt vaak ook beïnvloed door het bevel tot aftappen. Om de inbreuk op de wettelijke belangen van derden te beperken, verplicht dit lid een bevoegde officier of een persoon die onderschept of helpt bij het aftappen van communicatie om alle redelijke stappen te ondernemen voor het minimaliseren van de invloed van aftappen op derden.

124. De werkgroep heeft besloten een bijkomende bepaling toe te voegen bij artikel 17: lid (4) voorziet erin dat er geen strafrechtelijke of civiele aansprakelijkheid zal voortkomen uit de handelingen van een bevoegde officier of persoon indien zij handelen in overeenstemming met een bevel tot aftappen. Hetzelfde geldt voor een ieder die te goeder trouw een persoon helpt waarvan hij of zij gelooft op redelijke gronden dat die handelt in overeenstemming met een machtiging tot aftappen. Deze bepaling wordt geïntroduceerd om de persoon die legaal een aftapping uitvoert te beschermen.

Artikel 18: Betreding van panden en erven voor het uitvoeren van een bevel tot aftappen

125. Artikel 18 voorziet in het kader voor het uitvoeren van de toegangsclausule in het bevel tot aftappen, indien die er is. De aanvraag van een bevel tot aftappen waarin een bepaling is opgenomen die de bevoegde officier in staat stelt panden en erven te betreden zal worden gemaakt in overeenstemming met artikel 18 wat een bevoegde officier toestaat panden en erven te betreden op enig moment aangegeven in het bevel tot aftappen en enige handeling uit te voeren die gerelateerd is aan de doelstelling van het bevel tot aftappen.

Artikel 19: Plicht om bijstand te verlenen

126. Dit artikel voorziet in een dwingende maatregel voor het faciliteren van het aftappen van communicatie. Het verplicht een persoon, die telecommunicatiediensten verleent, een bevoegde officier toe te staan en te helpen, indien vereist en redelijk, om een bevel tot aftappen uit te oefenen. Voor het voorkomen van het misbruiken van de macht om bijstand te vragen, geeft lid (2) aan dat de plicht van een persoon om af te tappen zal worden gespecificeerd in het bevel tot aftappen door de rechter. Deze bepaling is essentieel voor het elimineren van mogelijk misbruik, vooral omdat artikel 20 een overtreding neerlegt in geval men nalaat bijstand te verlenen.

Artikel 20: Nalaten bijstand te verlenen

127. Krachtens artikel 20 begaat elke persoon van wie wordt geëist dat die bijstand verleent aan een bevoegde officier ingevolge een bevel tot aftappen en weigert dit te doen, een overtreding. De strafbaarstelling van de weigering om bijstand te verlenen is nodig omdat het bevel tot aftappen wordt verleend in uitzonderlijke omstandigheden voor het onderzoek naar ernstige misdrijven en het succes van het uitvoeren van het bevelschrift hangt vaak af van de bijstand van communicatie-aanbieders. Wanneer het verzoek voor bijstand wordt geweigerd , kan het onderzoek ondermijnt worden en de rechtsbedeling in het algemeen belemmeren.

Artikel 21: Geheimhouding van onderschepte communicatie

128. De zorgpunten betreffende privacy en de noodzaak voor geheimhouding van het aftappen rechtvaardigen de vereiste voor geheimhouding en voor de verplichting irrelevante data te vernietigen. Er is tevens een noodzaak de privacy van derden zo goed als mogelijk te beschermen waarvan de communicatie wordt onderschept zonder hun instemming. Om deze noodzaak voor geheimhouding aan te pakken, bevatten de wetten in veel landen, zoals Australië, Canada, Nieuw Zeeland en Zuid-Afrika, allemaal bepalingen die het ongeoorloofd gebruik of de openbaarmaking van onderschept materiaal verbieden.

129. In navolging van deze benadering, voorziet lid (1) van artikel 21 in strikte waarborgen op de mate waarin onderschept materiaal kan worden openbaar gemaakt, gekopieerd en bewaard, waarbij wordt vereist dat deze allen tot een minimum worden beperkt en waarbij de bevoegde officier wordt verplicht een aantal regelingen te treffen om de geheimhouding van het aftappen te verzekeren. Door te voorzien in degelijke waarborgen voor het proces van uitvoering van het bevel tot aftappen met betrekking tot geheimhouding van informatie, specificeert lid (2) specifieke informatie over het aftappen van communicatie en de uitvoering van het bevel tot aftappen dat confidentieel moet worden gehouden.

Artikel 22: Nalaten om informatie inzake aftappen geheim te houden

130. Artikel 22 voorziet in een verdere bescherming van de geheimhouding van onderschepte communicatie door het een overtreding te maken indien opzettelijk en zonder legaal excuus of rechtvaardiging iets dat hij of zij vereist werd confidentieel te houden onder de bepalingen van artikel 21 openbaar maakt.

Artikel 23: Vernietiging van bescheiden

131. Deze bepaling regelt de verwijdering van bescheiden. Het is essentieel omdat niet alle data verzameld tijdens aftappen relevant is. Aangezien aftappen van communicatie normaal weken tot zelfs maanden duurt, is het heel goed mogelijk dat er persoonlijke informatie bij zit die niet relevant is voor het onderzoek. Veel van de informatie verzameld als gevolg van het aftappen heeft betrekking op derden die contacten onderhouden met de personen die het doelwit zijn van het aftappen. De mogelijkheid deze data te bewaren zal zeker in een inbreuk op de privacy resulteren

van zowel derden als het doelwit van het aftappen. Van het oogpunt van privacy bezien, moet de persoon van wie de rechten worden aangetast door een aftapping in kennis worden gesteld van de inbreuk. Dit omvat het probleem van het onderwerp, de tijd en de omstandigheden van dergelijke kennisgeving. Al deze problemen kunnen vermeden worden indien de privacy van de persoon die beïnvloed wordt door een aftapping gewaarborgd kon worden door de vernietiging van het onderschepte materiaal.

132. Om de privacy te beschermen, bevat artikel 23 een verplichting voor het direct vernietigen van enige bescheiden die niet te maken hebben met de doelstelling van het bevel tot aftappen. Daarnaast, vereist lid (2) de vernietiging van alle bescheiden wanneer blijkt dat er geen proces of geen verder proces zal plaatsvinden waarin die informatie mogelijk nodig zou kunnen zijn als bewijsmateriaal. Lid (2) is van toepassing met de uitzonderingen die zijn neergelegd in lid (3) waarin staat dat de vernietigingsplicht niet op alle bescheiden van toepassing zal zijn van enige informatie aangevoerd in een proces voor enige rechter.

133. Voor het controle houden op de vereiste om onderschepte communicatie geheim te houden en irrelevante informatie te vernietigen, verplicht lid (4) een bevoegde persoon om de informatie te verstrekken in overeenstemming met lid (2) aan een [rechter] in het eindrapport betreffende de uitvoering van het bevel tot aftappen. Deze bepaling is slechts relevant voor landen die besluiten de verplichting in relatie tot het eindrapport in hun aftapwetgeving op te nemen (zie de memorie van toelichting bij artikel 16: Eindrapport).

Artikel 24:

134. **Nalaten bescheiden te vernietigen** stelt het niet naleven van de vereisten om bescheiden te vernietigen strafbaar. Het doel van deze bepaling is het implementeren van een nog een goed waarborg voor het beschermen van de privacy van communicatie en om te verzekeren dat alle informatie die niet relevant is voor het doel van het aftappen wordt vernietigd.

HOOFDSTUK IV – AFTAPAPPARATUUR

135. Het is essentieel om aftapapparatuur te reguleren, aangezien het gebruik van elektronische apparaten voor het aftappen van communicatie een prima facie bedreiging vormt voor het recht op privé communicatie. De noodzaak om het gebruik van apparatuur dat aftappingen kan uitvoeren te verbieden werd binnen de gehele werkgroep overeengekomen. Echter, er is geen precies antwoord op welk mechanisme voor het verbieden en monitoren van het gebruik het meest effectief is. Twee mogelijke opties zijn besproken door de werkgroep. De eerste optie was het verbieden van het bezit, de verkoop en verwerving van enig apparaat dat er in eerste instantie op gericht is om communicatie af te tappen en een beperkt aantal uitzonderingen vast te stellen voor de rechtshandhavingsinstanties, overheid en aanbieders van telecommunicatiediensten. Echter, deze aanpak brengt het probleem te berde van apparaten die voor 'tweeërlei gebruik' zijn toe te passen, zonder het op te lossen. Verder, tijdens de discussie werd opgemerkt dat de reikwijdte van dergelijk verbod onzeker is.

136. De tweede benadering is om de apparatuur met aftapcapaciteiten op een lijst te plaatsen en om de reikwijdte van de beperking te specificeren. Deze benadering volgt het model van Zuid-Afrika en de OOSC model wet inzake het aftappen van communicatie. Toch is het belangrijkste argument tegen dit kader de praktische implementatie van deze bepaling en de haalbaarheid om een lijst te maken en onderhouden.

137. Hoewel de werkgroep het eens was om de handel in en het gebruik van aftapapparatuur te beperken, was er een intensief debat over de juiste benadering met betrekking tot de implementatie. De werkgroep besprak de twee hierboven genoemde opties, maar er werd geen consensus bereikt over deze kwestie. Dus de bepalingen van Hoofdstuk IV moeten worden beschouwd als aanbevelingen voor die landen die besluiten de benadering te volgen en een lijst op te stellen en te onderhouden van apparatuur met aftapcapaciteiten.

138. De model wettekst suggereert de benadering van het opstellen van een lijst. Het doel van deze benadering is het verbieden van bepaalde handelingen en het vaststellen van een regelingsmechanisme op de illegale productie en het bezit van aftapapparatuur. Daarnaast is het de bedoeling het proces van het autoriseren van dergelijke apparatuur te reguleren. Het is er tevens op gericht alle belanghebbenden te beschermen door een consultatieproces te vereisen voordat het gebruik van bepaalde apparatuur wordt beperkt of verboden.

Artikel 25: Lijst van apparatuur met aftapcapaciteiten

139. Voor het veiligstellen van de benadering om een lijst te maken met apparatuur met aftapcapaciteiten definieert artikel 25 dat de Minister door middel van een kennisgeving in de staatscourant alle elektronische, elektromagnetische, akoestische, mechanische of andere apparatuur of toestellen, die voornamelijk worden gebruikt voor het aftappen van communicatie, in de omstandigheden die zijn aangegeven in de kennisgeving, kan laten opbrengen als beschermde apparatuur. Het proces voor het uitvaardigen van een dergelijke kennisgeving is vastgesteld in leden (2) – (7). Lid (4) voorziet in een waarborg voor alle belanghebbenden waarbij het ministerie wordt verplicht hen uit te nodigen schriftelijke commentaren in te dienen met betrekking tot het voorstel. Deze bepaling garandeert dat de procedure transparant is en de deelneming van alle belanghebbenden. Het is er ook op gericht de ontwikkeling van technologie te beschermen.

Artikel 26. Verbod op de productie, het bezit en het gebruik van beschermde apparatuur met aftapcapaciteiten

Artikel 27. Machtiging voor het gebruik van beschermde apparatuur met aftapcapaciteiten

140. Voor het definiëren van de beperking met betrekking to apparatuur die op de lijst staat, verbiedt artikel 26 de productie, het bezit en het gebruik van beschermde apparatuur met aftapcapaciteiten tenzij men daartoe is gemachtigd. De machtiging kan worden gegeven krachtens artikel 27 dat er in voorziet dat een ministerie de bevoegdheid heeft een vrijstelling te verlenen indien het in het openbaar belang is of indien het doel waarvoor de beschermde apparatuur wordt geproduceerd, samengesteld, in bezit genomen, verkocht, gekocht of geadverteerd redelijkerwijs noodzakelijk is of indien er speciale omstandigheden zijn die de vrijstelling rechtvaardigen. Artikel 27 voorziet ook in de vereisten voor de vorm en duur van het vrijstellingscertificaat.

Artikel 28. Overtreding

141. Voor het beperken van de productie en het bezit van apparatuur met aftapcapaciteiten worden bepaalde handelingen betreffende beschermde apparatuur strafbaar gesteld in artikel 28.

HOOFDSTUK V – OPENBAARMAKING VAN OPGESLAGEN COMMUNICATIEGEGEVENS

142. Hoofdstuk V werd ontwikkeld om de landen de mogelijkheid te geven opgeslagen communicatiegegevens te openbaar te maken die reeds verzonden waren en daarom per definitie niet worden beschouwd als onderwerp van een aftapping.

143. Dit hoofdstuk werd opgesteld op dusdanige wijze dat het de privacy van opgeslagen data beschermt. Het is opgenomen omdat in bepaalde gevallen het nodig kan zijn opgeslagen informatie te verkrijgen zoals locatiegegevens wanneer communicatie niet kan worden onderschept omdat zij reeds verzonden zijn. De werkgroep was het daarom erover eens, dat het niet opnemen van dit instrument in de model wettekst landen zou kunnen dwingen dit noodzakelijk instrument te introduceren in een tweede benadering. De OOSC model wet inzake aftappen van communicatie, evenals de wetgeving van Australië en het Verenigd Koninkrijk volgen dezelfde benadering en combineren de aftapwetgeving met wetgeving die is gerelateerd aan de openbaarmaking van opgeslagen communicatiegegevens.

144. Er was een intensieve discussie in de werkgroep over dit onderwerp. Hoewel er gezegd werd dat deze bepalingen nuttig zijn geweest voor de wetshandhaving in sommige rechtsgebieden, was men het erover eens dat dit lag buiten de reikwijdte van de model wettekst en alszodanig moet het duidelijk worden gemaakt dat dit deel optioneel was ter implementatie van de begunstigde landen.

145. Dus, de volgende bepalingen kunnen als optioneel worden beschouwd en vertegenwoordigen aanbevelingen voor landen die zouden kunnen besluiten deze benadering te volgen.

146. Hoofdstuk V van de model wettekst verbiedt de toegang tot opgeslagen communicatiegegevens en stelt een beperkte serie voorwaarden waaronder een bevel tot openbaarmaking kan worden uitgevaardigd. De aard van toegang tot opgeslagen data is verschillend van het aftappen van communicatie. Toegang tot opgeslagen data is geen dataverzameling tijdens de verzending en daarvoor is ook niet vereist dat aftapapparatuur wordt geïnstalleerd. Daarom zijn er mindere strenge regels toegepast in het geval waarbij toegang tot opgeslagen data vereist is. Echter, opgeslagen data zijn beschermd krachtens de wet evenals communicatie tijdens de verzending. Illegale toegang tot opgeslagen data is verboden onder artikel 29.

Artikel 29: Verbod op toegang tot opgeslagen communicatie

147. Op dezelfde wijze dat wederrechtelijk aftappen strafbaar is gesteld, stelt dit artikel de wederrechtelijke toegang tot opgeslagen communicatiegegevens strafbaar en verklaart de omstandigheden waaronder dergelijke toegang rechtmatig kan worden beschouwd. De werkgroep besloot de strafbaarstelling op te nemen ter verzekering van een degelijke bescherming van de privacy en de bescherming tegen een wederrechtelijke inbreuk.

Artikel 30: Openbaarmaking van opgeslagen communicatiegegevens

148. Artikel 30 stelt de aangewezen persoon in staat te vereisen van een aanbieder van telecommunicatiediensten opgeslagen data ter beschikking te stellen en/of opgeslagen data openbaar te maken door een bevel tot openbaarmaking te gebruiken. Als een waarborg om de geheimhouding van opgeslagen communicatiegegevens te beschermen, beperken leden (2) en (3) de voorwaarden waaronder bevel tot openbaarmakingen kunnen worden uitgevaardigd tot:

- nationale veiligheidsbelangen;
- het doel de voorkoming of opsporing van misdrijven of de voorkoming van publieke onrust;
- openbare veiligheidsbelangen;
- het doel het beschermen van openbare gezondheid;

- het doel in geval van nood, het voorkomen van de dood, een ongeval, of enige schade aan de fysieke en mentale gezondheid van een persoon, of voor het verlichten van een ongeval of schade aan de fysieke of mentale gezondheid van een persoon;

en het verbieden van het uitvaardigen van een bevel tot openbaarmaking tenzij de aangewezen persoon tevreden is dat het nodig is de data te verkrijgen en de data openbaar te maken aan een bevoegde officier.

149. Lid (4) voorziet in een reeks van vereisten met betrekking tot het bevel tot openbaarmaking. Het vereist dat de omstandigheden en de redenen voor het verlenen daarvan wordt gespecificeerd evenals de communicatiegegevens met betrekking waartoe het betrekking heeft en de manier waarop de openbaarmaking zal worden gedaan. Daarnaast, dient de bevoegde officier geïdentificeerd te worden. De reden voor het vaststellen van de vereisten met betrekking tot het bevel tot openbaarmaking is om de procedure transparant te maken en de openbaarmaking te beperken tot individuele zaken door alle bijzonderheden van de machtiging te specificeren.

150. Lid (5) stelt een reeks van beperkingen vast voor de machtiging die kan worden gedaan door het verbieden van elke vereiste die betrekking heeft dat communicatiegegevens worden verkregen aan het eind van een maand, beginnende op de datum waarop het bevelschrift is uitgevaardigd. Het verbiedt tevens de openbaarmaking van alle communicatiegegevens die niet in bezit zijn van de aanbieder van de telecommunicatiedienst, of die vereist wordt door hem of haar te worden verkregen, aan het eind van de periode.

151. Teneinde het bevel tot openbaarmaking geheim te houden, vereist lid (6), afhankelijk van een beperkt aantal uitzonderingen voorzien in lid (7), dat een aanbieder van telecommunicatiediensten die een bevelschrift ontvangt het bestaan en de werking van het bevelschrift evenals de daaraan gerelateerde informatie geheim houdt. Om het recht om juridisch advies te vragen door de aanbieder van telecommunicatiediensten te garanderen, voorziet lid (7) onder andere in de uitzondering die een aanbieder van telecommunicatiediensten in staat stelt informatie openbaar te maken aan een advocaat binnen het kader van een juridisch onderhoud.

Artikel 31. Nalaten informatie over het bevel tot openbaarmaking geheim te houden

152. Om de geheimhouding van het bevel tot openbaarmaking te beschermen, stelt artikel 31 het falen om geheimhoudingsvereisten na te leven strafbaar.

HOOFDSTUK VI – KOSTEN VOOR AFTAPPEN

153. De toewijzing van de kosten is een essentieel discussiepunt in het kader van de uitvoering van aftappen. Het is vooral relevant met betrekking tot de implementatie van de plicht van aanbieders om bijstand te verlenen. Rechtshandhavingsinstanties moeten vaak vertrouwen op de ondersteuning van aanbieders van telecommunicatiediensten terwijl zij aftapping uitvoeren. Verder stelt de model wettekst de landen in staat een verplichting vast te stellen voor het aftappen van communicatie die opgevolgd dient te worden door de aanbieders. Daarom moet de kwestie van toewijzing van de kosten worden opgelost in ieder rechtsgebied dat aftappen van communicatie introduceert.

Artikel 32: Toewijzing van kosten

154. Dit artikel suggereert dat alle kosten die zijn gegenereerd door de ontwikkeling van technische capaciteiten om communicatie af te tappen op het niveau van de aanbieder (waaronder de investerings-, technische, onderhouds- en uitvoeringskosten) moeten gedragen worden door die aanbieder van telecommunicatiediensten. Echter, een land kan besluiten dat het een model van teruggave van directe kosten gemaakt door de aanbieder van telecommunicatiediensten hanteert met betrekking tot het personeel en de administratie die vereist is met als doel het verlenen van bijstand in de uitvoering van het bevel tot aftappen.

155. Er was een discussie in de werkgroep en de participanten van de consultatieworkshop over de voorgestelde benadering. De discussie concentreerde zich op de luimen van overheidsbeleid en de invloed die een dergelijke positie kan hebben op de kostenlast. Met betrekking hiertoe nam het debat in overweging dat de aanbieders reeds de kosten van andere diensten moeten dekken. Er werd opgemerkt dat deze positie gebaseerd moet zijn op de fiscale positie van de individuele staten en het zou een invloed kunnen hebben op de aantrekkingskracht van een ICT investering van een rechtsgebied. Als gevolg van het controversiële debat besloot de werkgroep de beslissing over de kosten over te laten aan de lidstaten.

156. Daarom zal elk land zijn eigen beslissing nemen met betrekking tot de benadering over hoe de kosten tussen aanbieders en de staat verdeeld worden.

HOOFDSTUK VII – WAARBORGEN

157. Hoofdstuk VII werd ontwikkeld in overeenstemming met de richtlijnen voor modelbeleid die vereisen dat het beroepsgeheim wordt beschermd en voor het implementeren van het mechanismen voor monitoring en toezicht met betrekking tot het aftappen van communicatie.

158. Echter, gezien de verschillen in nationale wetgeving, evenals de capaciteit van de verschillende landen om monitorings- en toezichthoudende instanties te creëren, besloot de werkgroep dat deel een aantal aanbevelingen inhoudt die de landen wel of niet kunnen opvolgen.

Artikel 33. Beroepsgeheim

159. De richtlijnen voor modelbeleid riepen tot bepalingen op voor het beschermen van het beroepsgeheim als een noodzakelijke waarborg. Deze aanbeveling verwijst naar bepaalde soorten professionele communicatie die onderworpen zijn aan de verplichting van beroepsgeheim onder nationale wetten of regelgeving neergelegd door de bevoegde nationale lichamen. De bepalingen die beroepsgeheim waarborgen zullen strikt beperkt worden tot die soorten van geprivilegieerde communicatie die worden beschermd onder de bestaande nationale wetten, zoals communicatie tussen een advocaat en een klant, medicus en een patiënt, communicatie beschermd onder wetten die het financieel en bankgeheim reguleren. De wet zelf kan geen privilege vaststellen voor communicatie in het algemeen aangezien dit volgens de leden van de werkgroep niet wordt gedekt door het mandaat.

160. De bescherming van het beroepsgeheim betekent niet dat communicatie van een bepaalde persoon helemaal geen onderwerp van aftappen kan zijn. Bij voorbeeld, indien een advocaat wordt verdacht van een misdrijf waarvoor aftappen is toegestaan, wordt de machtiging tot aftappen verleend. Echter, de data die worden verzameld bij dergelijke aftappen zullen niet worden gepresenteerd als bewijsmateriaal bij de rechter, en zal geprivilegieerd blijven indien zij beroepsgeheimen bevatten.

161. Indien een land beslist de benadering te volgen die wordt voorgesteld door artikel 33 en dergelijke waarborgen te implementeren, dan wordt de lijst van beroepsgeheim dat is beschermd krachtens de wet worden opgesteld in overeenstemming met de nationale wetgeving.

Artikel 34: Monitoren van aftappen van communicatie

162. Artikel 34 beveelt de instelling van een Onafhankelijke Monitoringsautoriteit aan zoals vereist in de onderliggende richtlijnen voor modelbeleid. De mogelijkheid voor het onafhankelijk monitoren van aftappen is nodig voor het versterken van het systeem van checks-and-balances met betrekking tot zo'n inbreuk makend de maatregel als aftappen.

163. Als een optie, kan een land iedere autoriteit die niet actief betrokken is bij het onderzoeksproces en die de capaciteit heeft de nodige functies uit te voeren voor het toezien op het aftappen de functies toekennen van een Onafhankelijke Monitoringsautoriteit. Deze optie is in het bijzonder relevant voor kleine landen die een gebrek aan capaciteit ervaren.

164. Dit artikel geeft ook aanbevelingen met betrekking tot de functies van een Onafhankelijke Monitoringsautoriteit. Een land kan die verder beschrijven.

165. Men was overeengekomen tijdens de discussie in de werkgroep en tijdens de plenaire sessie van de consultatieworkshop dat een land wel of niet kan besluiten deze aanbeveling te implementeren afhankelijk van het nationaal systeem en de beschikbare capaciteit.

Artikel 35. Onafhankelijke commissaris inzake aftappen van communicatie

166. Dit artikel voorziet in een reeks aanbevelingen met betrekking tot de creatie van een onafhankelijk toezichthoudend lichaam (Onafhankelijke Commissaris inzake aftappen van Communicatie). Zoals hierboven uitgelegd, is dit artikel slechts een aanbeveling, die zal worden uitgevoerd door landen alleen indien zij het nodig achten. In plaats van de positie van commissaris te creëren, kan een land ook een commissie instellen voor het in evenwicht brengen van de macht op het toezicht van aftappen en om een situatie te voorkomen waarbij slechts een persoon die de leiding heeft de toegang tot informatie zou misbruiken.

HOOFDSTUK VIII – TOELAATBAARHEID VAN BEWIJSMATERIAAL

167. Het probleem werd besproken of de model wettekst de kwestie van toelaatbaarheid van onderschepte data als bewijsmateriaal zou moeten dekken indien dat niet wordt gedaan door andere wetgeving.

168. De werkgroep besliste een optie open te laten om de toelaatbaarheid van bewijsmateriaal op te nemen in de regelgeving. Echter, het werd overeengekomen dat elk rechtsgebied dergelijke bepalingen zal ontwikkelen in overeenstemming met de nationale wetgeving. Daarom is de enige aanbeveling die kan worden gemaakt, het verzekeren dat of (1) de nationale wetgeving deze zaak van toelaatbaarheid van bewijsmateriaal verkregen door aftappen dekt; of (2) bepalingen worden ontwikkeld in overeenstemming met de nationale benadering inzake toelaatbaarheid van bewijsmateriaal om deze kwestie te dekken in de wet die aftappen reguleert.

HOOFDSTUK IX – BIJLAGE

169. Deze lijst bevat een opsomming van ernstige misdrijven die behoudens artikel 8 het aftappen kunnen rechtvaardigen als maatregel voor het uitvoeren van een onderzoek.

170. De werkgroep nam een nieuwe bepaling op die een ministerie toestaat om overtredingen toe te voegen of te verwijderen van de lijst die in het overzicht is opgenomen. Een dergelijke instructie is onderworpen aan parlementaire goedkeuring.

171. De werkgroep was het ook eens met de bepaling inzake regelgeving die de minister in staat stelt regelgeving neer te leggen voor het implementeren van de doelstellingen van deze model wettekst. De regelgeving gemaakt krachtens dit artikel zal het onderwerp zijn van parlementaire goedkeuring.

172. Dit overzicht geeft een lijst van aanbevolen overtredingen:

- [Moord of doodslag of hoogverraad].
- [Ontvoering].
- [Money laundering] in strijd met de [Wet inzak [het tegengaan van] Opbrengsten van misdrijven en money Laundering].
- [Produceren, samenstellen, aanleveren of anderszins handelen in alle gevaarlijke drugs] in overtreding van de [Wet inzake Gevaarlijke Drugs].
- [Importeren of exporteren van gevaarlijke drugs] in overtreding van de [Wet inzake Gevaarlijke Drugs].
- [Import, export of doorvoer van alle wapens of munitie] in overtreding van de [Wapenwet].
- [Vervaardigen van, of handel drijven in wapens of munitie] in overtreding van de [Wapenwet].
- [Illegaal bezit van een verboden wapen of enig ander vuurwapen of ammunitie] in strijd met de [artikel van de Wapenwet].
- Een overtreding in strijd met [artikel van de wet inzake preventie van corruptie].
- [Brandstichting].
- [Internationale verdrag inzake vliegtuigkaping, terroristische daden, etc.].
- [Wet inzake het voorkomen van terrorisme].
- Poging of samenzweren tot het plegen, of het helpen of bijstaan, advies geven of het opdracht geven tot een overtreding die valt onder een van de voorgaande leden.

BIJLAGEN

Bijlage 1

Deelnemers in de Eerste Consultatieve Workshop voor de Werkgroep van het HIPCAR project, van de Werkgroep inzake ICT Wetgevingskader voor Kwesties de Informatiemaatschappij rakende Gros Ilet, Sainte-Lucie, 8-12 Maart 2010

Officieel Benoemde Deelnemers en Waarnemers

Land	Organisatie	Familienaam	Voornaam
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation & Competition Authority	DORSETT	Donavon
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of Trade, Industry and Commerce	COPPIN	Chesterfield
Barbados	Cable & Wireless (Barbados) Ltd.	MEDFORD	Glenda E.
Barbados	Ministry of Trade, Industry and Commerce	NICHOLLS	Anthony
Belize	Public Utilities Commission	SMITH	Kingsley
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Grenada	National Telecommunications Regulatory Commission	ROBERTS	Vincent
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Guyana	Office of the Prime Minister	RAMOTAR	Alexei
Guyana	National Frequency Management Unit	SINGH	Valmikki
Jamaica	University of the West Indies	DUNN	Hopeton S.
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Saint Kitts and Nevis	Ministry of Information and Technology	BOWRIN	Pierre G.
Saint Kitts and Nevis	Ministry of the Attorney General, Justice and Legal Affairs	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FELICIEN	Barrymore
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	FLOOD	Michael R.
Saint Lucia	Ministry of Communications, Works, Transport and Public Utilities	JEAN	Allison A.
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	ALEXANDER	K. Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel

Bijlage 1

Land	Organisatie	Familienaam	Voornaam
Suriname	Telecommunicatie Autoriteit Suriname/Telecommunication Authority Suriname	LETER	Meredith
Suriname	Ministry of Justice and Police, Department of Legislation	SITALDIN	Randhir
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PHILIP	Corinne
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon

Regional/Deelnemers vanuit Regionale en/of Internationale Organisaties

Organisatie	Familienaam	Voornaam
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	GEORGE	Gerry
Caribbean ICT Virtual Community (CIVIC)	WILLIAMS	Deirdre
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Delegation of the European Commission to Barbados and the Eastern Caribbean (EC)	HJALMEFJORD	Bo
Eastern Caribbean Telecommunications Authority (ECTEL)	CHARLES	Embert
Eastern Caribbean Telecommunications Authority (ECTEL)	GILCHRIST	John
Eastern Caribbean Telecommunications Authority (ECTEL)	HECTOR	Cheryl
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Office of Trade Negotiations (formerly CRNM) Caribbean Community Secretariat (CARICOM)	BROWNE	Derek E.
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

Experts voor het HIPCAR Project

Familienaam	Voornaam
MARTÍNS DE ALMEIDA	Gilberto
GERCKE	Marco
MORGAN[17]	J Paul
PRESCOD	Kwesi

[17] Workshop Chairperson

Bijlage 2

Deelnemers in de Tweede Consultatieve Workshop (fase B) voor de Werkgroep van het HIPCAR project, van de Werkgroep inzake ICT Wetgevingskader voor Kwesties de Informatiemaatschappij rakende Crane, Saint Philippe, Barbade, 23-26 Augustus 2010

Officieel Benoemde Deelnemers en Waarnemers

Land	Organisatie	Familienaam	Voornaam
Antigua and Barbuda	Ministry of Information, Broadcasting, Telecommunications, Science & Technology	SAMUEL	Clement
Bahamas	Utilities Regulation and Competition Authority	DORSETT	Donavon
Barbados	Ministry of Economic Affairs, Empowerment, Innovation, Trade	NICHOLLS	Anthony
Barbados	Ministry of Finance, Investment, Telecommunications and Energy	BOURNE	Reginald
Barbados	Ministry of the Civil Service	STRAUGHN	Haseley
Barbados	University of the West Indies	GITTENS	Curtis
Belize	Public Utilities Commission	PEYREFITTE	Michael
Dominica	Government of Dominica	ADRIEN-ROBERTS	Wynante
Dominica	Ministry of Information, Telecommunications and Constituency Empowerment	CADETTE	Sylvester
Dominica	Ministry of Tourism and Legal Affairs	RICHARDS-XAVIER	Pearl
Grenada	National Telecommunications Regulatory Commission	FERGUSON	Ruggles
Guyana	Office of the President	RAGHUBIR	Gita
Guyana	Public Utilities Commission	PERSAUD	Vidiahar
Jamaica	Attorney General's Chambers	SOLTAU-ROBINSON	Stacey-Ann
Jamaica	Digicel Group	GORTON	Andrew
Jamaica	LIME	SUTHERLAND CAMPBELL	Melesia
Jamaica	Ministry of National Security	BEAUMONT	Mitsy
Jamaica	Office of the Prime Minister	MURRAY	Wahkeen
Saint Kitts and Nevis	Attorney General's Chambers	POWELL WILLIAMS	Tashna
Saint Kitts and Nevis	Department of Technology, National ICT Centre	HERBERT	Christopher
Saint Kitts and Nevis	Ministry of Youth Empowerment, Sports, Information Technology, Telecommunications and Post	WHARTON	Wesley
Saint Lucia	Attorney General's Chambers	VIDAL-JULES	Gillian

Bijlage 2

Land	Organisatie	Familienaam	Voornaam
Saint Lucia	Ministry of Communications, Works, Transport & Public Utilities	FELICIEN	Barrymore
Saint Vincent and the Grenadines	Ministry of Telecommunication, Science, Technology and Industry	ALEXANDER	Kelroy Andre
Saint Vincent and the Grenadines	Ministry of Telecommunications, Science, Technology and Industry	FRASER	Suenel
Suriname	Ministry of Trade and Industry	SAN A JONG	Imro
Suriname	Ministry of Transport, Communication and Tourism	STARKE	Cynthia
Suriname	Telecommunicatie Autoriteit Suriname/Telecommunication Authority Suriname	PELSWIJK	Wilgo
Suriname	Telecommunicatiebedrijf Suriname/Telesur	JEFFREY	Joan
Trinidad and Tobago	Ministry of National Security	GOMEZ	Marissa
Trinidad and Tobago	Ministry of Public Administration, ICT Secretariat	SWIFT	Kevon
Trinidad and Tobago	Ministry of Public Administration, Legal Services Division	MAHARAJ	Vashti
Trinidad and Tobago	Ministry of the Attorney General, Attorney General's Chambers	EVERSLEY	Ida
Trinidad and Tobago	Telecommunications Authority of Trinidad and Tobago	PERSAUD	Karina
Trinidad and Tobago	Telecommunications Services of Trinidad and Tobago Limited	BUNSEE	Frank

Regional/Deelnemers vanuit Regionale en/of Internationale Organisaties

Organisatie	Familienaam	Voornaam
Caribbean Centre for Development Administration (CARICAD)	GRIFFITH	Andre
Caribbean Community Secretariat (CARICOM)	JOSEPH	Simone
Caribbean ICT Virtual Community (CIVIC)	HOPE	Hallam
Caribbean ICT Virtual Community (CIVIC)	ONU	Telojo
Caribbean Telecommunications Union (CTU)	WILSON	Selby
Eastern Caribbean Telecommunications Authority (ECTEL)	WRIGHT	Ro Ann
International Telecommunication Union (ITU)	CROSS	Philip
International Telecommunication Union (ITU)	LUDWIG	Kerstin
Organization of Eastern Caribbean States Secretariat (OECS)	FRANCIS	Karlene

Experts voor het HIPCAR Project

Nom	Prénom
ALMEIDA	Gilberto Martíns de
GERCKE	Marco
MORGAN[18]	J Paul
PRESCOD	Kwesi

[18] Workshop Chairperson

International Telecommunication Union
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Geneva, 2013