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

Elektronisch Bewijsmateriaal: Richtlijnen voor Model Beleid & Wetteksten

HIPCAR

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

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

Elektronisch Bewijsmateriaal:

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.

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 9^{e} 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

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 mondiaal ITU-EU-project voor de ACP-landen en omvat tevens de landen in Sub-Saharisch Afrika en in de Stille Oceaan.

Het doel van HIPCAR is CARICOM/ACP/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.

1.2. 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).

---

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.

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:

ICT-Beleidskader en Wetgevingskader voor Kwesties de Informatiemaatschappij rakende, omvattende zes deelgebieden: e-commerce (transacties en bewijs), persoonlijke levenssfeer & gegevensbescherming, onderschepping van berichten, cybercriminaliteit, en toegang tot openbare informatie (vrijheid van informatie).

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 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 openbare 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 de **interceptie van elektronische communicatie** verschaft een passend kader dat de illegale interceptie van communicatie verbiedt en heeft een minieme mogelijkheid geschapen zodat de rechtshandhaver in staat wordt gesteld om rechtmatig communicatie te onderscheppen, 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 herziening 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 openbare informatie (vrijheid van informatie) dan is gebleken in de andere kaders.

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 **interceptie van communicatie**. Alle vier kaders handelen over kwesties in verband met de behandeling van berichten verzonden via communicatienetwerken, 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 communicatienetwerk" - 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 de onderschepping 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 interceptie 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 openbare 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 Elektronisch Bewijs bij e-handel, 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 herzien 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 Data, Onderscheppen 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 HIPCAR Stuurgroep – voorgezeten door de Caribische Telecommunicatie Unie (CTU) – begeleidde en ondersteunde het team van consultants, waaronder Gilberto Martíns de Almeida en Pricilla Banner. De model wettekst over Elektronisch Bewijsmateriaal in e-handel werd in eerste instantie 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 concept document is daarna bekeken, besproken en aangenomen met een brede consensus door de participanten in twee consultatieworkshops voor de HIPCAR-Werkgroep inzake Kwesties de Informatiemaatschappij rakende gehouden te Saint Lucia van 8-12 maart 2010 en in Barbados van 23-26 augustus 2010 (zie Bijlagen). De Memorie van Toelichting bij de wettekst in dit document is opgesteld door Dhr. Martíns de Almeida waarin onder andere de zaken die naar voren zijn gebracht in de tweede workshop worden behandeld. Dit document bevat daarom data en informatie zoals bekend in augustus 2010.

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

---

[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.

1.6. Het belang van doeltreffend beleid en doeltreffende wetgeving inzake elektronisch bewijs bij e-handel

Elektronische handel - evenals ander hedendaags gebruik van ICT – is afhankelijk van de juridische toelaatbaarheid van elektronisch bewijsmateriaal als een fundamentele voorwaarde voor het wekken van vertrouwen dat nodig is voor de ontplooiing ervan. Dit feit is erkend door de internationale gemeenschap, zoals weergegeven in de model wetten inzake elektronisch bewijs van UNCITRAL en de Gemenebest, evenals door de relevante wetgeving in deze zin in een groot aantal staten.

In feite, hebben de toenemende gevaren voor de integriteit, beschikbaarheid, vertrouwelijkheid, authenticiteit en het auteurschap van elektronische documenten als gevolg van de acties van hackers, crackers, re-mailers, bedrijfsfraude en cybercriminaliteit in het algemeen veel bezorgdheid veroorzaakt over de risico's en beperkingen met betrekking tot de gerechtelijke toelaatbaarheid van elektronisch bewijsmateriaal.

Aan de andere kant, heeft de proliferatie van internationale normen en kaders voor informatiebeveiliging en IT-bestuur, uiterst veilige digitale handtekeningen, tijdstempel technieken en elektronische gerechtelijke procedures geleid tot een algemene indruk dat elektronisch bewijs nog veiliger en betrouwbaarder zou zijn dan conventioneel, niet-elektronisch bewijs, op voorwaarde dat een zekere mate van zorg wordt betracht.

Gelet op deze tegengestelde trends en mogelijkheden, moet een evenwicht worden gebracht door regelgeving die de relevante technische en procedurele aspecten met elkaar verzoent met het oog op het aanwenden van bewijs tegen een redelijke prijs, en die tevens aan goed aanvaarde beginselen voldoen, zoals het beginsel van gelijkwaardigheid tussen het digitale en niet-digitale bewijsmateriaal, het beginsel van voorzorg (wat de goedkeuring vereist van preventie of risicobeperkende maatregelen), en het beginsel van accreditatie (wat geaccrediteerde certificatie van processen vereist zodat er meer vertrouwen wordt gewekt).

Regelgeving inzake digitaal bewijsmateriaal is een taak die met diverse uitdagingen wordt geconfronteerd, zoals de evenredige bescherming van privacyrechten en van het beginsel dat men zichzelf niet kan bezwaren. Het bewaren van gegevens en data encryptie zijn voorbeelden van onderwerpen waar de productie van digitaal bewijs ligt op het snijpunt van de zorgpunten over veiligheid en privacy.

Het gebrek aan lokale regelgeving inzake digitaal bewijsmateriaal is een feit dat goed is opgemerkt door hackers en andere cybercriminelen, die zich richten op landen die minder waarschijnlijk gevallen op basis van elektronisch bewijs zullen vervolgen. Botnet regelingen zijn een voorbeeld van de gevaren voor burgers, overheden en bedrijven in landen die niet beschikken over specifieke wetgeving die voorziet in begeleiding en criteria op toelaatbaar digitaal bewijsmateriaal voor onderzoek en de productie, het verzamelen en bijhouden daarvan.

De impuls van staten om wetgeving inzake elektronisch bewijs te introduceren of om bestaande wetgeving inzake bewijsmateraal te wijzigen, zodat er rekening wordt gehouden met elektronisch bewijsmateriaal is ingegeven door het besef dat de traditionele ongeschreven wetsregels inzake bewijsmateriaal gebruikt voor het handhaven van burgerrechten en voor strafrechtelijke handhaving onvoldoende zijn om de technologische vooruitgang bij te benen, en die moeten daarom worden gemoderniseerd. De aard van elektronisch bewijsmateriaal zelf - met inbegrip van de nieuwheid en het feit dat het kan worden gezien als kwetsbaar en gemakkelijk te manipuleren – vormt een uitdaging voor landen bij het moderniseren van hun wetten. De kwetsbaarheid van elektronisch bewijsmateriaal betekent dat het kan worden gewijzigd, beschadigd of vernietigd door ondeskundig gebruik en ondeugdelijk onderzoek. Elektronisch bewijs is vaak ook transnationaal van aard wanneer de servers zich in meerdere landen bevinden, wat de moeilijkheid vergroot bij het gebruik van het bewijsmateriaal en het doen toelaten daarvan in een rechtbank.

Inleiding

In 2002 heeft het secretariaat van het Gemenebest een aanbeveling gedaan om haar model wetgeving aan te nemen of aan te passen op dit vlak in alle landen van de Gemenebest. Sindsdien heeft het snelle tempo van technologische vooruitgang en de toenemende complexiteit en verspreiding van cybercriminaliteit landen die geïnteresseerd zijn in het reguleren van elektronisch bewijs geconfronteerd met nieuwe uitdagingen. Cloud computing, cryptografie, tijdstempels, elektronische gerechtelijke procedures en nieuwe internationale normen zijn voorbeelden van nieuwe problemen waarmee rekening moet worden gehouden.

In het kader van dit scenario, moet regelgeving inzake elektronische bewijs worden verwoord in samenhang met regelgeving op het vlak van versneld bewaren van gegevens, bevel tot overlegging, huiszoekingsbevelen, dataopslag en andere, om te zorgen voor de vereiste doeltreffendheid.

Deel I:
Richtlijnen voor model beleid – Elektronisch bewijsmateriaal

Hieronder volgen de richtlijnen voor model beleid die een land kan overwegen met betrekking tot elektronisch bewijsmateriaal bij e-handel.

1. CARICOM/CARIFORUM-LANDEN ZULLEN ZICH EROP RICHTEN OM DE NODIGE GEZAMENLIJKE INTERPRETATIES VAST TE STELLEN VOOR SLEUTELBEGRIPPEN DIE WORDEN GEASSOCIEERD MET E-BEWIJSMATERIAAL[5]

- Er zal een passende definitie zijn van “computer”, “apparaat”, “computergegevens”, “computersysteem,” “inhoudelijke gegevens”, “verkeersgegevens”, “locatiegegevens”, “document”, “elektronische bescheiden”, “elektronisch document”, “elektronische handtekening”, “digitale handtekening” en “tijdstempel”.
- Er zal een voldoende ruime formulering van de definitie van deze termen zijn gekoppeld aan een lijst van illustratieve voorbeelden.
- Er zal een definitie zijn met betrekking tot welke terminologie wordt overgelaten aan rechterlijke interpretatie binnen het rechtsgebied van elke begunstigde staat, en hoe gevolg wordt gegeven aan dergelijke rechterlijke activiteit zodat de wettelijk voorgeschreven definities en rechterlijke definities op elkaar afgestemd blijven.

2. CARICOM/CARIFORUM-LANDEN ZULLEN HET VASTSTELLEN VAN HET NODIGE RAAMWERK NASTREVEN OM DE PUBLIEKE OF PARTICULIERE OORSPRONG EN DE ROL VAN DE PARTIJEN DIE VERANTWOORDELIJK ZIJN VOOR HET VERZAMELEN EN/OF MANAGEN VAN E-BEWIJSMATERIAAL[6] TE DEFINIEREN

- Er moeten wettelijke voorzieningen worden getroffen die de rol van "de overheid", officieren van justitie, en politie en, in voorkomend geval, de "accreditatie-instantie", "certificaat dienstverleners", "agenten", "24x7 toegang", bij het verzamelen en/of het beheer van e-bewijsmateriaal neerleggen.
- Er moet een bepaling zijn die neerlegt dat de overheid moet voldoen aan de regels voor het verzamelen en beheer van e-bewijsmateriaal vastgesteld in wetten of beleid inzake beveiliging van openbare informatie (bijvoorbeeld ten aanzien van de grenzen voor het gebruik van cryptografie, procedures bij de behandeling met apparaten, en andere protocollen in overeenstemming met de beste internationale praktijken voor digitaal forensisch onderzoek.).
- Er zullen bepalingen voor de erkenning van co- of zelfregulering in bepaalde sectoren van de markten of van activiteiten, met name waar digitale handtekeningen en het gebruik van andere technologieën geen redelijke kosten-batenanalyse bieden.
- Er zullen bepalingen zijn voor de vaststelling van de beginselen en de gebieden waar de toelaatbaarheid van e-bewijsmateriaal in de eerste plaats is gebaseerd op procedurele normen.

---

5 Er zal een publiekscampagne worden gevoerd met als doel het verhogen van het bewustzijn over e-bewijs, met inbegrip van een uitleg van de belangrijkste termen, op basis van het eigen inzicht van elke begunstigde staat.

6 Er zal een overheidsbeleid zijn voor het versterken van de vaardigheden van de rechterlijke macht, zodat rechters en technische experts bekend zijn met het gebruik van de kernbegrippen, terminologie en procedurele standaarden van e-bewijsmateriaal.
Er zal een overheidsbeleid zijn dat institutionele samenwerking aanmoedigt voor het ontwikkelen van applicaties waarbij e-bewijsmateriaal wordt gebruikt als een manier om grotere elektronische ontsluiting van de overheid te bewerkstelligen.

- Er moeten bepalingen zijn voor de instelling en handhaving van technische normen ontwikkeld ter bevordering van het passend verzamelen en/of beheer van e-bewijsmateriaal.
- Waar van toepassing, wordt er een bepaling voorzien voor het vaststellen van het beginsel van wederkerigheid voor de erkenning van digitale certificaten afgegeven in een derde land, op grond van regionale gemeenschappelijke wetten en gezag, of niet.
- Waar van toepassing, wordt er een bepaling voorzien dat overheid, in bepaalde gevallen, zal worden uitgebreid tot particuliere instanties, mits die entiteiten zijn aangewezen om te fungeren als "e-Notarissen" – personen die derden digitale authentificatie van partijen verzorgen zonder vast te houden aan de technische en procedurele testen van een geregistreerd certificaat dienstverlener.
- Waar van toepassing, is er een definitie van wat kenmerkend is voor "notarieel bekrachtigen" en dus de mate waarin de functies van e-Notarissen rechten hebben en plichten die daar juridisch aan verbonden zijn.

3. CARICOM/CARIFORUM-LANDEN ZULLEN DE WETTELIJKE MANDATEN EN NORMEN VASTSTELLEN WAARAAN E-BEWIJSMATERIAAL ONDERWORPEN IS

- De wet/het wettelijk mandaat zal “systeem voor elektronische bescheiden” definiëren met als doel het interpreteren van dit beleid.
- De wet/het wettelijk mandaat moet faciliterend zijn van aard en de bepalingen dienen niet al te dicterend te zijn.
- De wet/het wettelijk mandaat moet vermelden dat elektronische documenten geen geldigheid op zichzelf kan worden ontzegd alleen omdat de documenten elektronisch van aard zijn.
- In voorkomend geval, zal de wet/het wettelijk mandaat de mate bepalen waarin de procedurele normen met betrekking tot de verzameling, het beheer en/of het gebruik van elektronische bescheiden de basis vormt voor toelaatbaarheid van elektronische documenten en de omstandigheden die indiening van technische e-bewijsmateriaal verlangen.
- De wet/het wettelijk mandaat vermeldt de juridische gronden van elektronisch bewijsmateriaal, en zal duidelijk de toelaatbaarheid uitbreiden naar administratieve en gerechtelijke activiteiten (met inbegrip van burgerlijke, handels-, straf-, arbeids-, administratieve en andere zaken).
- De wet/het wettelijk mandaat moet de aard en de gevolgen van het wettelijk vermoeden in verband met e-bewijsmateriaal vaststellen, om zo het gewicht te bepalen ten opzichte van andere soorten bewijsmateriaal (documentaire, en andere).
- De wet/het wettelijk mandaat stelt vast en voorziet in de publicatie van informatie over passende normen voor het bijwerken, opslaan en verwijderen van e-bewijsmateriaal.
- De wet/het wettelijk mandaat treft voorzieningen voor de duur van het bijhouden van gegevens die worden geproduceerd, verzameld, opgeslagen en/of beheerd als e-bewijsmateriaal, die gelijkwaardig zijn met de gebruikelijke praktijken voor het beheer van niet-elektronische gegevens.
- De wet/het wettelijk mandaat voorziet voor de publieke sector gebruikmakend van middelen om transparantie te bevorderen met betrekking tot de beschikbare middelen en instrumenten die de invoering van e-bewijsmateriaal kunnen vergemakkelijken.
- De wet/het wettelijk mandaat stelt vast dat het verzamelen en beheren van e-bewijsmateriaal zich zal laten leiden door de doelstellingen van veiligheid, doelmatigheid, doeltreffendheid.
- Er zal een overheidsbeleid zijn dat institutionele samenwerking aanmoedigt voor de ontwikkeling van applicaties die gebruik maken van e-bewijsmateriaal als een manier om verdere elektronische automatisering van de openbare dienstverlening mogelijk te maken.
- De wet/het wettelijk mandaat legt richtsnoeren neer voor het aanpakken van het beginsel van technologische neutraliteit, om flexibiliteit te bieden bij het ontwikkelen van e-bewijs instrumenten en mechanismen.

- Indien van toepassing, zal de wet bepalen in welke omstandigheden elektronische print-outs ("uitdraaien") van elektronische documenten worden geacht te voldoen aan de eisen van het best mogelijke bewijs.
- De wet stelt dat de ontvankelijkheid van e-bewijsmateriaal wordt geleid door de principes van functionele gelijkwaardigheid, voorzorg, en accreditatie.
- De wet stelt vast dat computer forensisch onderzoek wordt gebruikt bij gerechtelijke bewijsgaring en -uitwisseling met betrekking tot e-bewijsmateriaal.
- De wet reguleert de omstandigheden die het mogelijk maken dat het vermoeden van de integriteit van een elektronisch registratiesysteem wordt vastgesteld door middel van een beëdigde verklaring afgelegd naar beste weten en overtuiging van de deponent, en die het mogelijk maken dat de genoemde deponent onder kruisverhoor kan worden gesteld.
- De wet zal sancties vaststellen voor iedere persoon die in een beëdigde verklaring of aangeboden certificaat een verklaring aflegt waarvan die persoon weet dat deze vals is of niet gelooft dat deze waar is.
- De wet stelt criteria vast voor het harmoniseren van de sancties tegen een persoon die valse beweringen doet in een beëdigde verklaring of certificaat met betrekking tot de integriteit van een elektronisch registratiesysteem.
- De wet/het wettelijk mandaat voorziet in een bepaling voor vaststelling van passende procedures bij huiszoekingsbevelen, die zal zorgen voor de integriteit van de verzamelde gegevens.
- De wet/het wettelijk mandaat voorziet in de vaststelling van procedures voor de certificering en overlegging van verzamelde gegevens en ook van de digitale omgeving ten tijde van het verzamelen van de gegevens.
- De wet legt de erkenning vast van particuliere overeenkomsten inzake de toelaatbaarheid van elektronische bescheiden (en kan die bepaling uitbreiden tot strafrechtelijke vervolging indien er beperkingen zijn).
- De wet stelt dat partijen vrij zijn in te stemmen een bepaalde methode van elektronische handtekeningen te gebruiken, tenzij anders bepaald door de wet.
- De wet stelt dat een persoon die vertrouwt op een elektronische handtekening de juridische gevolgen zal dragen van zijn falen om redelijke maatregelen te nemen om de betrouwbaarheid van een elektronische handtekening te verifiëren.
- De wet stelt vast dat de certificaat dienstverlener documentatie beschikbaar houdt voor een bepaalde tijd inzake het bijhouden van de veiligheidsprocedures die worden gevolgd.
- De wet stelt vast dat de certificeringsinstantie bevoegd en verplicht is om tevens de tijd van de elektronische bescheiden te bevestigen ("tijdstempel").

4. CARICOM/CARIFORUM-LANDEN ZULLEN VOLDOENDE BESCHERMING BIEDEN VOOR E-BEWIJSMATERIAAL

- Er wordt een definitie gegeven van "imaging" met het oog op de bescherming van e-bewijsmateriaal.
- De wet/het wettelijk mandaat zal vaststellen dat personen worden beschermd tegen vooroordelen ten aanzien van de administratieve of gerechtelijke toelaatbaarheid van e-bewijs.
- De wet/het wettelijk mandaat voorziet in de erkenning van het gebruik van gecertificeerde elektronische tijdstempels.
- De wet/het wettelijk mandaat voorziet in de erkenning van procedurele normen ter zake van de betrouwbaarheid van het bewijs van gegevens bijgehouden in een specifiek elektronisch registratiesysteem.
- De wet/het wettelijk mandaat bepaalt tevens, eventueel via beschikkingen, de grenzen van legaal en illegaal gebruik van technologieën, zoals cryptografie, steganografie, en re-mailing, met betrekking tot e-bewijsmateriaal.
- De wet/het wettelijk mandaat voorziet in de erkenning van beelden als e-bewijsmateriaal, en geeft richtlijnen voor het dissociëren van elektronische afbeeldingen van "imaging".
- Het overheidsbeleid zal zich richten op het aanmoedigen van het gebruik van certificering van attributen, in digitale handtekening certificaten, ter verbetering van de capaciteit om de houder daarvan te identificeren en elektronisch bewijsmateriaal vast te stellen.
- De wet/het wettelijk mandaat zal het gebruik van veilige technieken (bijvoorbeeld veilige transmissie via IP) aanmoedigen wanneer teleconferencing wordt gebruikt, wordt toegepast voor publieke dienstverlening (bij voorbeeld bij bepaalde hoorzittingen in een gerechtelijke procedure).
- De wet/het wettelijk mandaat zal het juiste gebruik van camera's aanmoedigen en erkennen als een manier om e-bewijs vast te stellen.
- De wet/het wettelijk mandaat zal faciliteiten aanmoedigen en erkennen die kunnen worden toegewezen door telecommunicatie-apparaten voor de vaststelling van e-bewijs.

5. CARICOM/CARIFORUM-LANDEN ZULLEN HET KADER VASTSTELLEN VOOR E-BEWIJSMATERIAAL IN SAMENHANG MET OVERHEIDSBELEID INZAKE AANVERWANTE ONDERWERPEN

- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake nationale veiligheid.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake cybercriminaliteit.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die consistent is met het overheidsbeleid inzake de interceptie van communicatie.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake versneld bewaren.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake bevelen tot overlegging.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake huiszoekingsbevelen.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake real-time verzamelen.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake digitale handtekening.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake privacy en inzake gegevensbescherming.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake veiligheid van informatie.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake intellectuele eigendom.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake vrijheid van informatie.
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met verdragen over de wederzijdse erkenning van officiële overheidsdocumenten (in overeenstemming met het Verdrag van Den Haag).
- De wet/het wettelijk mandaat zal e-bewijsmateriaal reguleren op een wijze die in overeenstemming is met het overheidsbeleid inzake sociale digitale insluiting.

Deel II:
Model wettekst –
Elektronisch bewijsmateriaal

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

Indeling van de artikelen

Deel II

HOOFDSTUK I – INLEIDING

Citeertitel 1. Deze wet wordt aangehaald als de “Wet Elektronisch Bewijsmateriaal”, en wordt van kracht en treedt in werking [op xxx/ na publicatie in het Staatsblad].

Definities 2. (1) Geaccrediteerd certificaat: een certificaat afgegeven door een geaccrediteerde certificatie dienstverlener.

(2) Geadresseerde: met betrekking tot elektronische bescheiden, een persoon die door degene van wie die elektronische bescheiden afkomstig zijn als ontvanger daarvan wordt bedoeld, en omvat niet een persoon die optreedt als tussenpersoon met betrekking tot die elektronische bescheiden.

(3) Geavanceerde elektronische handtekening: een elektronische handtekening verstrekt door een geaccrediteerde certificatie dienstverlener.

(4) Authenticatieproducten of -diensten: producten of diensten ontworpen voor het identificeren van de houder van een elektronische handtekening bij andere personen.

(5) Certificaat: een elektronische attestering die handtekening-verificatiedata verbindt aan een persoon en de identiteit van die persoon, of tijd-verificatiedata verbindt aan elektronische bescheiden of aan elektronische communicatie en de geassocieerde datum en tijd bevestigt.

(6) Computer: elk digitaal informatiesysteem dat is geïntegreerd door apparatuur en programma's bedoeld voor de creatie, opname, opslag, verwerking en/of verzending van data, waaronder enige computer, computertoestellen, of andere elektronische informatie- of communicatietoestellen, bedoeld voor het uitvoeren van dergelijke functies.

(7) Inhoudelijke gegevens: alle gegevens die in digitale, optische of andere vorm, met inbegrip van metadata, de essentie, materie, informatie, betekenis, doel, opzet, of inlichtingen, individueel of in een gecombineerde vorm, hetzij in onverwerkte of verwerkte vorm. Inhoudelijke gegevens omvatten alle gegevens die de betekenis of de inhoud van communicatie overbrengt, evenals de gegevens die worden verwerkt, opgeslagen of verzonden via computerprogramma's.

(8) Cryptografische dienst: elke dienst die wordt verleend aan een afzender of geadresseerde van een elektronische communicatie of aan elke persoon die elektronische communicatie opslaat, en die is ontworpen voor het vergemakkelijken van cryptografische technieken met als doel het garanderen -

(a) dat toegang kan worden verkregen tot de gegevens of elektronische communicatie of dat die slechts in een verstaanbare vorm kan worden gegoten door bepaalde personen;

(b) dat de authenticiteit of integriteit van de gegevens of de elektronische communicatie kan worden vastgesteld;

(c) van de integriteit van de data of de elektronische communicatie; of

(d) dat de bron van de data of de elektronische communicatie op juiste wijze kan worden vastgesteld.

(9) Data (of computergegevens, of elektronische gegevens): elke weergave van feiten, informatie of concepten in een vorm die geschikt is voor de verwerking in een informatiesysteem, waaronder een programma dat geschikt is te veroorzaken dat een informatiesysteem een functie vervult.

(10) Digitale handtekening: een elektronische handtekening op basis van asymmetrische cryptografie, waaronder aanverwante publieke en private sleutels.

(11) Elektronisch: omvat alles dat is gecreëerd, opgenomen, verstuurd of opgeslagen in een digitale of andere niet-materiële vorm door een elektronisch, magnetisch, optisch of enig ander middel dat de capaciteit heeft voor het creëren, opnemen, versturen of opslaan gelijk aan die middelen.

(12) Elektronische agent: een programma, computer, of ander elektronisch of geautomatiseerd middel, dat is geconfigureerd en aangesloten door een persoon, dat wordt gebruikt voor het geheel of gedeeltelijk initiëren of beantwoorden van elektronische bescheiden of een elektronische gebeurtenis, zonder dat het wordt beoordeeld door een individu.

(13) Elektronische authenticatie: elke procedure gebruikt met als doel het nagaan of een elektronische communicatie afkomstig is van de afzender en of het niet is gewijzigd tijdens de overdracht.

(14) Elektronische communicatie: elke overdracht van bescheiden door middel van tekens, signalen, schrift, beelden, geluiden, data of informatie van welke aard dan ook verzonden, geheel of gedeeltelijk door middel van een telefoon-, radio-, elektromagnetisch, foto-elektronisch of foto-optisch systeem dat handel tussen staten of buitenlandse handel beïnvloedt, maar omvat geen -

(a) telegrafische or verbale communicatie;

(b) communicatie gedaan via een uitsluitend met oproeptonen werkende semafoonontvanger;

(c) communicatie van een peilzender.

(15) Elektronische bescheiden: een reeks van gegevens die wordt gecreëerd, geproduceerd, opgenomen, opgeslagen, verwerkt, verstuurd, doorgegeven en/of ontvangen, op een fysiek medium in of door een computer of ander soortgelijk apparaat, en dat kan worden gelezen of waargenomen door een persoon door middel van een computersysteem of een ander soortgelijk apparaat, met inbegrip van een beeldscherm, print-out of andere output van die gegevens.

(16) Elektronische handtekening: een handtekening op basis van een elektronisch proces, met inbegrip van digitale handtekeningen, biometrische handtekeningen, en andere.

(17) Informatiesysteem (of computersysteem, of gegevensverwerkingssysteem): een apparaat of een groep van onderling verbonden of aanverwante apparaten, waaronder het internet, waarvan een of meer, op grond van een programma, de automatische verwerking van gegevens of enige andere functie uitvoert.

(18) Wet: common law (ongeschreven recht), wetgeving en afgeleide wetgeving.

(19) Juridische procedure betekent een burgerrechtelijke, strafrechtelijke of administratieve procedure in een rechtbank of voor een scheidsgerecht, raad of commissie.

(20) Locatiegegevens: alle gegevens verwerkt in een elektronisch communicatienetwerk waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven.

(21) Afzender, met betrekking tot elektronische bescheiden, betekent een persoon die –

(a) elektronische bescheiden verstuurt;

(b) een ander opdracht geeft elektronische bescheiden te versturen namens hem; of

(c) elektronische bescheiden laat versturen door zijn elektronische agent, maar omvat geen persoon die als tussenpersoon handelt met betrekking tot die elektronische bescheiden.

(22) Publiek lichaam omvat:

(a) ministerie of overheidsdepartement;

(b) geheel of gedeeltelijk in eigendom zijnde staatsbedrijven of -ondernemingen;

(c) instanties die wettelijk gezag uitoefenen, van wetgevende, uitvoerende of gerechtelijke aard;

(d) subnationale of lokale publieke autoriteiten, waaronder gemeenten.

(23) Bescheiden: informatie gecreëerd, verzameld, of ontvangen bij het initiëren, uitvoeren en voltooien van een activiteit en welke de inhoud, context en structuur omvat om bewijs te leveren dat die activiteit of transactie wordt ingeschreven, opgeslagen of anderszins gehandhaafd op een tastbaar medium of die is opgeslagen op een elektronisch of enig ander medium en toegankelijk is in zichtbare en hoorbare vorm.

(24) Veiligheidsprocedure: een procedure, ingesteld bij wet of overeenkomst of willens en wetens geaccepteerd door elke partij, die wordt gebruikt met als doel het verifiëren of een elektronische handtekening, communicatie of prestatie van een bepaalde persoon is of voor het ontdekken van veranderingen of fouten in de inhoud van een elektronische communicatie.

(25) Handtekening omvat enig symbool uitgevoerd of aangenomen, of enige methodologie of procedure gebruikt of aangenomen door een persoon met de intentie de bescheiden authentiek te verklaren, waaronder elektronische of digitale methoden.

(26) Handtekeningaanmaakgegevens: unieke gegevens, zoals codes of particuliere cryptografische sleutels, die worden gebruikt door de ondertekenaar om een elektronische handtekening te creëren.

(27) Abonneegegevens: alle informatie in de vorm van computergegevens of enige andere vorm die wordt aangehouden door een dienstverlener, met betrekking tot abonnees van zijn diensten, uitgezonderd verkeersgegevens of inhoudelijke gegevens, en door middel waarvan kan worden vastgesteld:

(a) de aard van de communicatiedienst die wordt gebruikt, de technische faciliteiten daartoe aangewend, en de periode van de dienstverlening;

(b) de identiteit van de abonnee, post- of geografisch adres, telefoon en ander toegangsnummer, facturerings- en betalingsinformatie, zoals beschikbaar is op basis van de dienstverleningsovereenkomst of -regeling; en/of

(c) alle informatie betreffende de locatie van de geïnstalleerde communicatie-apparatuur, zoals beschreven in de dienstverleningsovereenkomst of -regeling.

(28) Verkeersgegevens: computergegevens die:

(a) verband houden met communicatie door middel van een computersysteem; en

(b) zijn gegenereerd door een computersysteem dat deel is van de communicatieketen; en

(c) de oorsprong van de communicatie, bestemming, route, tijd datum, grootte, duur of soort van de onderliggende diensten toont.

HOOFDSTUK II – TOELAATBAARHEID

Wijziging van regels inzake authenticatie en beste bewijs

3. Deze wet wijzigt geen common law (ongeschreven recht) of wettelijke bepaling met betrekking tot de toelaatbaarheid van bescheiden, met uitzondering van die welke betrekking hebben op authenticatie en het beste bewijs.

Common law (Ongeschreven recht) en wettelijke bepalingen

4. Bij de toepassing van common law (ongeschreven recht) of wettelijke bepalingen met betrekking tot de toelaatbaarheid van bescheiden, kan de rechter rekening houden met de beginselen die de leidraad vormen voor toelaatbaarheid van elektronische bescheiden, zoals voorgeschreven door deze wet.

Algemene toelaatbaarheid van elektronisch bewijsma-teriaal

5. Niets in de bewijsvoeringsregels zal van toepassing zijn om toelaatbaarheid aan elektronische bescheiden te onthouden enkel op grond van het feit dat de bescheiden elektronisch zijn.

Toepassing van de regel van het beste bewijs

6. (1) In elke juridische procedure, met inachtneming van lid (2), waar de regel van het beste bewijs van toepassing is ten aanzien van elektronische bescheiden, wordt aan deze regel voldaan waar bewijs wordt geleverd van de integriteit van de computer in of waarmee de gegevens waren geregistreerd of opgeslagen.

(2) Bij het ontbreken van bewijs van het tegendeel, wordt de integriteit van de computer waarin elektronische bescheiden zijn geregistreerd of opgeslagen verondersteld in een gerechtelijke procedure:

(a) waarin bewijs wordt aangeleverd welke de bevinding staaft dat op alle relevante tijdstippen het computersysteem of soortgelijk apparaat goed functioneerde, of indien niet, dat in geen enkel opzicht waarin het niet goed functioneerde of buiten werking was, de integriteit van de bescheiden niet beïnvloed werd door dergelijke omstandigheden, en er geen andere goede redenen zijn om de integriteit van de bescheiden in twijfel te trekken;

(b) wanneer wordt vastgesteld dat de elektronische bescheiden werden geregistreerd of opgeslagen door een partij bij de procedure die een tegengesteld belang heeft aan de partij die het naar voren wil brengen; of

(c) wanneer wordt vastgesteld dat de elektronische bescheiden werden geregistreerd of opgeslagen in de gewone en normale gang van zaken door een persoon die geen partij is bij de procedure en die het niet registreerde of opsloeg onder het beheer van de partij die de bescheiden willen aanvoeren.

Integriteit van informatie, en specifieke toelaatbaarheidsregels

7. (1) Een verklaring vervat in elektronische bescheiden geproduceerd door een computer die een verklaring van horen zeggen uitmaken zullen niet worden toegelaten in een procedure als bewijsmateriaal van geen enkel feit dat daarin naar voren wordt gebracht, tenzij de integriteit van de computer is aangenomen krachtens lid 2.

(2) Bij gebrek aan bewijs van het tegengestelde, wordt de integriteit van de computer waarin elektronische bescheiden zijn geregistreerd of opgeslagen aangenomen in een gerechtelijke procedure indien de transactiebescheiden:

(a) compleet en ongewijzigd zijn gebleven, met uitzondering van:

(i) de toevoeging van enige bekrachtiging; of

(ii) enige immateriële wijziging;

die het resultaat is van een normaal verloop van communicatie, opslag of weergave;

(b) elektronisch zijn gecertificeerd of elektronisch zijn getekend gebruikmakend van een methode verstrekt door geaccrediteerde certificatie-instanties;

(c) notarieel zijn bekrachtigd met betrekking tot de integriteit en inhoud daarvan;

(d) zijn geregistreerd in een niet-herschrijfbaar opslagmedium, of enig ander elektronisch middel waarin het niet mogelijk is elektronische bescheiden te wijzigen;

(e) zijn onderzocht en de integriteit daarvan is bevestigd geworden door een specialist aangewezen door de rechter; of

(f) met betrekking waartoe:

(i) bewijs wordt aangeleverd welke de bevinding staaft dat op alle relevante tijdstippen het computersysteem of soortgelijk apparaat goed functioneerde, of indien niet, dat in geen enkel opzicht waarin het niet goed functioneerde of buiten werking was, de integriteit van de bescheiden niet beïnvloed werd door dergelijke omstandigheden, en er geen andere goede redenen zijn om de integriteit van de bescheiden in twijfel te trekken;

(ii) wanneer wordt vastgesteld dat de elektronische bescheiden werden geregistreerd of opgeslagen door een partij bij de procedure die een tegengesteld belang heeft aan de partij die het naar voren wil brengen; of

(iii) wanneer wordt vastgesteld dat de elektronische bescheiden werden geregistreerd of opgeslagen in de gewone en normale gang van zaken door een persoon die geen partij is bij de procedure en die het niet registreerde of opsloeg onder het beheer van de partij die de bescheiden wil aanvoeren.

(3) Indien een verklaring vervat in elektronische bescheiden geproduceerd door een computer geen verklaring van horen zeggen is, zal dergelijke verklaring toelaatbaar zijn indien aan de voorwaarden aangegeven in lid (2) wordt voldaan met betrekking tot die elektronische bescheiden.

Print-outs

8. In elke juridische procedure waarin naar aanleiding van een elektronische vastlegging in de vorm van een print-out kennelijk of consequent gehandeld is geworden, welke is ingeroepen, of gebruikt als de vastlegging van de informatie vastgelegd of opgeslagen op de print-out, wordt de print-out voor de regel van het beste bewijs als bescheiden gebruikt.

Bewijslast inzake authenticiteit van elektronisch bewijsmateriaal

9. De persoon die voornemens is elektronische bescheiden aan te voeren in een juridische procedure heeft de bewijslast inzake het aantonen van de authenticiteit met behulp van bewijs dat de bevinding kan staven dat elektronische bescheiden zijn wat de persoon zegt dat die zijn. In geval er speciale wetgeving is die kwetsbaardere personen beschermt, waaronder consumenten en kinderen, en het vaststellen van de toekenning van de bewijslast gunstiger is voor dergelijke personen, dan zal die wetgeving voorrang hebben op dit artikel.

Standaarden

10. Voor de vaststelling onder enige andere wet of elektronische bescheiden toelaatbaar zijn, kan het bewijs worden gepresenteerd ten aanzien van elke standaard, procedure, gebruik of praktijk over hoe elektronische gegevens worden geregistreerd of verduurzaamd, gelet op de aard van het bedrijf of inspanning gebruikt, opgeslagen of bewaard, de elektronische bescheiden en de aard en het doel van de elektronische bescheiden. Overheidsinstanties belast met de ontwikkeling of goedkeuring van relevante technische normen of veiligheidsprocedures moeten richtlijnen uitvaardigen die voorzien in een oriëntatie op de toepasselijke criteria die moeten worden gevolgd voor naleving van dit artikel.

Beëdigde verklaringen

11. Wanneer het de bedoeling is om elektronische bescheiden aan te halen als bewijsmateriaal, is het toegestaan die bescheiden aan te halen in de vorm van een beëdigde verklaring.

Overeenstemming over toelaatbaarheid van bewijsmateriaal

12. (1) Tenzij anders bepaald in een wet, zijn elektronische bescheiden toelaatbaar, behoudens het oordeel van de rechter, indien de partijen bij het geding uitdrukkelijk zijn overeengekomen op enig moment dat de toelaatbaarheid ervan niet kan worden betwist.

(2) In weerwil van lid (1), maakt een overeenkomst tussen de partijen over de toelaatbaarheid van elektronische bescheiden, deze bescheiden nog niet toelaatbaar in een strafrechtelijke procedure in naam van eiser, indien ten tijde dat de overeenkomst werd bereikt, de verdachte of een van de verdachte personen die beschuldigd worden in de procedure niet juridisch werd bijgestaan of vertegenwoordigd.

Elektronische handtekening

13. (1) Een elektronische handtekening wordt geen rechtsgevolg onthouden slechts op basis van het feit dat het elektronisch is.

(2) Een elektronische handtekening kan getoetst worden op welke manier dan ook, met inbegrip van het aantonen dat er een procedure bestond waarbij het nodig is voor de persoon om met de transactie voort te gaan, dat er een symbool werd uitgevoerd of een veiligheidsprocedure ter verificatie dat de elektronische bescheiden van die persoon afkomstig zijn.

Eisen aan elektronische handtekeningen

14. (1) Wanneer de wet de handtekening van een persoon vereist, is aan deze eis voldaan door middel van een elektronische handtekening als de elektronische handtekening die wordt gebruikt net zo betrouwbaar en geschikt is als voor het doel waarvoor zij is gegenereerd of gecommuniceerd, in alle omstandigheden, met inbegrip van alle relevante overeenkomsten.

(2) Lid (1) is van toepassing ongeacht of de vereiste voor een handtekening in de vorm is van een verplichting of de wet voorziet in consequenties in geval van afwezigheid van een handtekening.

(3) Partijen kunnen overeenkomen een bepaalde methode voor elektronische handtekening te gebruiken, tenzij anders is bepaald bij wet.

(4) Wanneer een elektronische handtekening is vereist door de partijen bij een elektronische transactie en de partijen de type elektronische handtekening te gebruiken niet zijn overeengekomen, wordt aan de vereiste voldaan in relatie tot het gegevensbericht indien:

(a) de handtekeningaanmaakgegevens zijn verbonden aan de ondertekenaar en geen enkele andere persoon;

(b) de handtekeningaanmaakgegevens ten tijde van de ondertekening onder het beheer staan van de ondertekenaar en geen enkele andere persoon;

(c) enige wijziging aan de elektronische handtekening, gemaakt na de ondertekening zichtbaar is; en

(d) waar het doel van de wettelijke vereiste voor een handtekening is om een garantie te geven voor de deugdelijkheid van de informatie waarmee het verband houdt, enige wijziging aangebracht aan die informatie na de ondertekening zichtbaar is.

(5) Lid (4) beperkt de bevoegdheid van een persoon niet:

(a) om op enige andere wijze, met als doel het tegemoetkomen aan de vereiste waarnaar wordt verwezen in lid (1), de betrouwbaarheid van een elektronische handtekening vast te stellen; of

(b) bewijs aan te halen dat een elektronische handtekening niet betrouwbaar is.

(6) Een persoon die vertrouwt op een elektronische handtekening zal de juridische consequenties dragen van zijn verzuim om redelijke stappen te ondernemen ter verificatie van de betrouwbaarheid van een elektronische handtekening.

(7) De rechter zal rekening houden met enige wet die bepalingen neerlegt inzake de geloofwaardigheid van het auteurschap en de integriteit van digitaal getekende elektronische bescheiden.

Alternatieve technieken en procedures voor de productie van elektronisch bewijsma-teriaal

15. In aanvulling op de bewijsmiddelen in de voorgaande artikelen in deze wet, kan elektronisch bewijsmateriaal worden geproduceerd met betrekking tot bepaalde elektronische bescheiden door middel van alternatieve technieken en procedures, zoals attestatie door notarissen, of vrederechters of andere soortgelijke autoriteiten, de registratie op een niet-herschrijfbaar medium, en gerechtelijke computerkunde in justitiële bewijsgaring en -uitwisseling in de rechtsgang.

HOOFDSTUK III – ALGEMENE BEPALINGEN

Toelaatbaarheid van elektronische bescheiden uit andere landen

16. In het geval dat elektronisch bewijsmateriaal afkomstig is uit een ander rechtsgebied, wordt de toelaatbaarheid niet geschaad indien wordt bewezen of verondersteld dat de integriteit van de computer die in verband wordt gebracht met het relevante elektronische bewijsmateriaal in overeenstemming is met de standaarden vergelijkbaar met die welke zijn voorzien in artikelen 6 (2) (a), en 7 (2) van deze wet.

Erkenning van buitenlandse elektronische documenten en handtekeningen

17. (1) Bij de bepaling of informatie in elektronische vorm wel of niet, of in welke mate rechtskracht heeft, wordt geen aandacht besteed aan de locatie waar de informatie was gegenereerd of gebruikt, of de vestigingsplaats van de onderneming die het heeft gegenereerd, mits de elektronische bescheiden zich bevinden in het binnenlands rechtsgebied.

(2) Indien de elektronische bescheiden zich bevinden in een buitenlands rechtsgebied, zal lid (1) hierboven niet van toepassing zijn tenzij -

(a) de partij die bewijs aanhaalt van de inhoud van de elektronische bescheiden, niet minder dan 14 dagen voor de dag waarop het bewijsmateriaal wordt aangehaald, aan elke andere partij een kopie van de voorgestelde elektronische bescheiden heeft doen toekomen;

(b) de rechter beslist dat het toepasselijk is; of

(c) er een internationaal verdrag van kracht is dat de erkenning van elektronische bescheiden of van elektronische handtekeningen die zich bevinden in dat buitenlands rechtsgebied regelt.

Interpretatie in overeenstemming met algemeen aanvaarde beginselen

18. De bepalingen van deze wet zullen worden geïnterpreteerd en gehandhaafd in het licht van de internationaal geaccepteerde beginselen van technologische neutraliteit en functionele gelijkwaardigheid.

Regelgeving

19. De Minister kan regelgeving neerleggen met als doel de implementatie van deze wet en met betrekking tot het voorschrijven van alles dat is vereist of geautoriseerd door deze wet. De Minister kan hierbij de internationale beste toepassing in de praktijk en standaarden in overweging nemen.

Deel III:
Memorie van toelichting bij de model wettekst inzake elektronisch bewijsmateriaal

INLEIDING

1. Deze wettekst ontwikkelt een juridisch kader voor de toelaatbaarheid van elektronische bescheiden. De belangrijkste doelstellingen van deze wettekst (Wet) zijn het vaststellen van de algemene toelaatbaarheid van elektronisch bewijsmateriaal, het wijzigen van wetsregels met betrekking to authenticatie en beste bewijs, het vermelden van de criteria die grond geven voor het veronderstellen van de integriteit van computers en van elektronische bescheiden, het aankaarten van relevante bewijslast, het reguleren van toelaatbaarheid van elektronische handtekeningen, het bepalen van de interpretatie gebaseerd op internationaal aanvaarde beginselen, en het nadenken over de erkenning van elektronische bescheiden van oorsprong of gevestigd in andere landen.

2. Deze memorie van toelichting is bedoeld om de inhoud van deze wet toe te lichten, en moet worden gelezen in samenhang daarmee. Het belang van de belangrijkste bepalingen van deze wet wordt toegelicht en, in voorkomend geval, wordt de aandacht gevestigd op bepaalde besprekingen van de werkgroep, met de nadruk op verschillende opties van de regelgeving daarin besproken. 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.

3. Deze wet bestaat uit drie delen**:**

   - **Hoofdstuk I** geeft de definities;
   - **Hoofdstuk II** wijzigt wetsregels betreffende authenticatie en beste bewijs, stelt het beginsel van non-discriminatie van elektronische records vast, regelt de toepassing van de regel van het beste bewijs, omschrijft de criteria die grond geven voor het veronderstellen van de integriteit van computers en van elektronische bescheiden, schrijft de bewijslast toe, bepaalt de uitgifte van richtlijnen voor het voldoen aan technische normen en veiligheidsprocedures, erkent overeenstemming over toelaatbaarheid van elektronisch bewijsmateriaal in een gerechtelijke procedure, erkent elektronische handtekeningen als bewijsmateriaal, en behandelt alternatieve technieken en procedures voor de productie van elektronisch bewijsmateriaal;
   - **Hoofdstuk III** legt de algemene bepalingen neer betreffende toelaatbaarheid van elektronische bescheiden van andere landen, de erkenning van buitenlandse elektronische documenten en handtekeningen, interpretatie in overeenstemming met internationaal aanvaarde beginselen, en de mogelijke regelgeving in overeenstemming gebracht met de beste internationale praktijken en normen.

COMMENTAAR OP DE ARTIKELEN

HOOFDSTUK I – INLEIDING

4. Hoofdstuk I geeft inleidende bepalingen zoals de citeertitel en de bepaling over de inwerkingtreding in **artikel 1** en de definities in **artikel 2**.

5. Hoofdstuk I heeft een discussie op gang gebracht binnen de werkgroep met betrekking tot de wijze waarop wetten worden opgesteld in de verschillende rechtsgebieden. Er is besproken of een artikel moest worden toegevoegd waarin de doelstellingen van deze model wet, en er was een consensus dat deze kwestie zou worden overgelaten aan het oordeel van de begunstigde staten.

Artikel 2. Definities

6. De definitie van **Computer** gegeven in lid (6) laat ruimte over om ieder elektronisch apparaat dat functies kan uitvoeren die typisch zijn voor computers te omvatten.

7. Er was een discussie binnen de werkgroep over de vraag of er een expliciete verwijzing moet zijn naar telecommunicatie-apparatuur, zoals intelligente mobiele telefoons. Er werd overeengekomen dat het snelle tempo van de technologische vooruitgang, samen met het beginsel van technologische neutraliteit, het raadzaam maken een ruime formulering te gebruiken met als vermelding "elektronische informatie of communicatie-apparaten", als aanvulling op de verwijzingen naar "computer" en "computer-apparaten".

8. **Inhoudelijke gegevens** (samen met locatiegegevens en verkeersgegevens, die respectievelijk zijn gedefinieerd in de leden 20 en 28) zijn gegevens waarvan de creatie, communicatie, verwerking en opslag natuurlijke doelen zijn voor de productie van elektronisch bewijs, omdat ze de onderliggende communicatie en transacties tot een wezenseenheid maken.

9. De definitie van inhoudelijke gegevens is geformuleerd op zodanige wijze ("essentie, materie, informatie, betekenis, doel, opzet, of inlichtingen") om elke soort inhoud van elektronische bescheiden te omvatten.

10. Deze definitie verwijst zowel naar verwerkte en onverwerkte vormen inhoudelijke gegevens. Het doel hier was om niet alleen "ruwe" inhoudelijke gegevens die worden omgezet bij de verwerking van gegevens te omvatten, maar ook de verschillende gegevens die worden gegenereerd als output van een dergelijke verwerkingsactiviteit.

11. De definitie in kwestie verwijst ook naar 'metadata', dat is een tweede laag van gegevens, met "gegevens over gegevens " (zoals de taal die wordt gebruikt om de inhoud te schrijven, het tijdstip van de creatie, waar meer informatie over die inhoud gevonden kan worden, enzovoort). Aangezien het gebruik van metadata en metatags steeds populairder wordt (gegeven, met name, het gemeenschappelijke gebruik van internet zoekmachines aangedreven door een zulke metadata en metatags), kunnen metadata belangrijke elementen voor de productie van elektronisch bewijsmateriaal verstrekken betreffende inhoudelijke gegevens.

12. **Data** wordt gedefinieerd in lid (9) als elke weergave van feiten, informatie of concepten in een vorm die geschikt is voor de verwerking in een informatiesysteem.

13. Data werd gekozen als uitdrukking voor de definities in plaats van “informatie”, omdat dat een term is die in de wetgeving van sommige landen voorkomt in relatie tot algemeen bewijsmateriaal, niet speciaal elektronisch bewijsmateriaal. Aangezien de reikwijdte van deze wet slechts elektronische transacties omvat, is de intentie hier dat het slechts om feiten, informatie en concepten gaat die worden weergegeven in elektronische, binair digitale vorm.

14. De werkgroep besprak het voordeel van het opnemen van het begrip "status" in deze definitie, wat zou benadrukken dat de gegevens niet alleen logisch worden opgevat als opeenvolgingen van de getallen "0" en "1" (welke opeenvolgingen letters of cijfers vertegenwoordigen), maar ook de

tastbare verandering betekenen van elektromagnetische of optische status in een computer die het informatiesysteem 'leest' als corresponderend met de binaire cijfers. Hoewel de uitdrukking "status" leken (met inbegrip van rechters) kan helpen ook rekening te houden met het materiële aspect van gegevens en zo kan bijdragen data wettelijk te kwalificeren als "ding" (wat betekent, bij voorbeeld, dat het onderhevig is aan bezit of verduistering), kan het laatste deel van deze definitie, die aangeeft "... waaronder een programma geschikt voor het veroorzaken dat een informatiesysteem een functie vervult..." indirect het doel bereiken, tot op zekere hoogte, dat het ook de betekenis heeft van het tastbare karakter (zoals de uitvoering van een functie in een informatiesysteem wordt verwacht een tastbare verandering te veroorzaken). Daarom werd de voorkeur voor enige nadruk op het materiële aspect van de data overgelaten aan het oordeel van de begunstigde staten.

15. Ten slotte, maakt dergelijke definitie duidelijk dat gegevens een synoniem zijn van "computergegevens" en "elektronische gegevens", welke uitdrukkingen aanwezig zijn in aanverwante wetgeving op nationaal en internationaal niveau. Op deze wijze wordt de overeenstemming tussen de eerste en de laatste gegarandeerd, omwille van de consistentie, met name wat betreft de wetgeving van andere landen, waar de diversiteit van de gebruikte terminologie nog groter is, waardoor de noodzaak om bruggen te bouwen voor het vergemakkelijken van een algemene interpretatie en effectieve handhaving wordt verhoogd.

16. **Digitale handtekening** wordt gedefinieerd in lid (10) als een specifiek soort elektronische handtekening. In samenhang met de definitie van andere uitdrukkingen (zoals **geaccrediteerd certificaat, geavanceerde elektronische handtekening, authenticatie producten en diensten, certificaat, cryptografische dienstverlener, elektronische handtekening, handtekening** en **handtekeningaanmaakgegevens**) die de revue passeren in de andere leden van Artikel 2, verleent dit een coherente betekenis aan een kernsysteem voor het produceren van elektronisch bewijsmateriaal – het systeem van authenticatie, certificatie en accreditatie van digitale handtekeningen – waarmee de auteur, afkomst, tijd en andere elementen van elektronische bescheiden kunnen worden geïdentificeerd.

17. De definities aangenomen voor deze reeks uitdrukkingen houden er rekening mee dat de begunstigde staat wel of niet een bepaalde technologie of organisatie heeft geïmplementeerd om een systeem op te zetten van gecertificeerde elektronische handtekeningen, lokaal of gehuurd uit het buitenland. Om die reden, hebben deze definities zich geconcentreerd op fundamentele aspecten, waarbij voor verdere regulering meer specifieke opties worden opengelaten (zoals de verschillende structuren van taken en bevoegdheden, de verdeling van de regionale en/of nationale middelen, enzovoort).

18. Door het hanteren van een dergelijke aanpak, vergemakkelijkt de definitie van digitale handtekeningen de integratie met andere bepalingen van deze wet, zoals die betreffende de regel van het beste bewijs of met alternatieve middelen voor het produceren van elektronisch bewijsmateriaal, aangezien de aangenomen algemene formulering de flexibiliteit biedt om verschillende wijzen van gebruik van digitale handtekeningen te gebruiken voor het bewijzen van de integriteit en betrouwbaarheid van een computer of elektronische bescheiden te bewijzen, of om alternatieve vormen van elektronisch bewijsmateriaal te weerspiegelen of op te nemen.

19. De geautomatiseerde elektronische respons gebruikt als interface voor interactie van de mens met computers is kenmerkend voor de **elektronische agent** als omschreven in lid (12). Dergelijke definitie is een van de elementen die de concepten van afzender en geadresseerde van een elektronische communicatie integreren, en die kan bepalen of daadwerkelijke verzending of ontvangst heeft plaatsgevonden, en hoe en waar dat zal worden aangetoond.

20. Betrouwbaarheid van communicatie ondersteund door elektronische middelen is van fundamenteel belang voor het doel van de productie van relevant elektronisch bewijsmateriaal. Het concept van **elektronische authenticatie**, gedefinieerd in lid (13), helpt bij het bepalen van de procedures die kunnen worden gebruikt om te controleren of een bepaalde mededeling is gewijzigd tijdens de overdracht, en om na te gaan wie de opdrachtgever was.

21. De definitie van **elektronische communicatie**, vervat in lid (14), is belangrijk aangezien het zich richt op de overdracht van bescheiden, met inbegrip van de respectievelijke verzending en ontvangst, terwijl de definities van "computer " en van "informatiesysteem" zich slechts beperken tot het concentreren op de interne activiteiten uitgevoerd door de computer of door het informatiesysteem.

22. De werkgroep besprak of het een voordeel was of niet om verwijzingen op te nemen naar "enige draad- of mondelinge communicatie". Er werd enige bezorgdheid geuit met betrekking tot het feit dat dergelijke termen kunnen overlappen met reeds bestaande uitdrukkingen in de telecommunicatiewetgeving van bepaalde landen, met name met betrekking tot telefonie, semafoon, en peilzenders. De werkgroep besloot dat het wordt overgelaten aan het oordeel van de begunstigde staten of zij een dergelijke formulering handhaven of niet.

23. Lid (4) definieert **elektronische bescheiden** als een reeks van gegevens die kan worden gelezen of waargenomen door een persoon door middel van een informatiesysteem of een ander soortgelijk apparaat.

24. Hoewel data wordt weergegeven in binaire vorm en wordt verondersteld te worden “gelezen” door een computer of “vertaald” door een computerprogramma, zijn “elektronische bescheiden” de weergave of uitvoer van een informatiesysteem die kunnen worden waargenomen door een mens.

25. Het onderscheid tussen deze twee aanvullende uitdrukkingen – “data”, en “elektronische bescheiden” – is noodzakelijk voor het wettigen van elektronisch bewijsmateriaal aangezien het bewijzen van sommige feiten, informatie of concepten kan afhangen van de perceptie door een persoon (of op de mogelijkheid door hem/ haar te worden waargenomen) en niet slechts op de mogelijkheid van technische bewijsgaring.

26. De definitie van “elektronische bescheiden” is ook van belang voor het vaststellen van de betekenis van “elektronisch informatieapparaat” (waarnaar werd verwezen in sommige van de bepalingen van deze wet binnen de formulering van “elektronische informatie of communicatieapparatuur”), aangezien duidelijk wordt bedoeld een apparaat gebruikt door mensen om toegang te krijgen tot elektronische bescheiden of om die waar te nemen.

27. Bovendien, is in de definitie van "elektronische bescheiden" de uitdrukking opgenomen "op een fysiek medium", wat naar verwachting de reikwijdte van de media in verband met elektronische bescheiden zal uitbreiden, waarbij het buiten de traditionele media zal gaan, zodat het bijvoorbeeld, biometrische media kan omvatten (zoals vingerafdrukken, of de iris), die steeds meer worden toegepast in de context van elektronisch bewijsmateriaal.

28. Op dezelfde wijze, maakt de verwijzing naar print-outs duidelijk dat elektronische bescheiden niet noodzakelijkerwijs worden weergegeven in een computersysteem, maar ook kunnen worden waargenomen als element daarbuiten.

29. Even belangrijk voor het begrijpen van de verschijnselen rond elektronisch bewijsmateriaal is de definitie van **informatie-systeem**, vervat in lid (17). Terwijl de definitie van "computer" aangeeft dat het een enkel elektronisch apparaat is, bestaat "informatiesysteem" uit groepen van onderling verbonden apparaten, kenmerkend voor elektronische netwerken.

30. De brede definitie kan netwerken omvatten op verschillende niveaus, waaronder het internet, dat technisch wordt beschouwd als een "netwerk van netwerken". Gezien de omvang van het internet als toneel voor de productie en vergaring van elektronisch bewijsmateriaal, is er een specifieke verwijzing naar. Het concept van groep van onderling verbonden apparaten is uitgebreid genoeg om alle apparatuur verbonden met het internet daaronder te begrijpen.

31. De werkgroep heeft tevens gediscussieerd over de vraag of deze wet het begrip "computersysteem" of de uitdrukking "informatiesysteem” moet gebruiken. Het feit dat "informatiesysteem" (en "informatieverwerkingssysteem") de uitdrukking is die gebruikt wordt in de wetgeving van de meeste landen heeft in zijn voordeel gewerkt. Hoewel er enkele technische

betekenisverschillen tussen "informatiesysteem" en "computersysteem" zijn, werden die als niet essentieel beschouwd voor de context van elektronisch bewijsmateriaal, en heeft de werkgroep dus gekozen om "informatiesysteem" te gebruiken, terwijl "computersysteem" en “gegevensverwerkingssysteem” werden toegevoegd als gelijkwaardige uitdrukkingen. Het niveau van technische nauwkeurigheid gewenst voor de aanpak van dergelijke concepten in deze wet werd overgelaten aan het oordeel van de begunstigde staten.

32. Juridische procedure betekent een burgerrechtelijke, strafrechtelijke of administratieve procedure in een rechtbank of voor een scheidsgerecht, raad of commissie.

33. De definitie van **juridische procedure**, vervat in lid (19), omvat niet alleen civiele procedures, maar ook strafrechtelijke en administratieve. Terwijl elektronisch bewijsmateriaal meestal goed wordt opgenomen in een civiele procedure, wordt het vaak aangevochten in een strafrechtelijke procedure, waar wordt aangevoerd dat de "virtuele" aard niet genoeg bewijs is voor een strafrechtelijke veroordeling. Op dezelfde wijze, wordt het "immateriële" aspect normaal in verband gebracht met elektronisch bewijsmateriaal buiten beschouwing gelaten in de administratieve sfeer, waarbij het wordt overgelaten aan de gerechtelijke procedure dergelijk bewijs te evalueren. Daarom is het belangrijk om duidelijk te maken dat op juiste wijze geproduceerd elektronisch bewijsmateriaal geldig zal zijn voor elke procedure, ongeacht of die civielrechtelijk of strafrechtelijk is, of juridisch of administratief.

34. De plaats waar apparatuur zich bevindt, is een belangrijk element voor de productie van elektronisch bewijsmateriaal aangezien het verschillende bevindingen en gevolgen kan impliceren, zoals toekenning van rechtsbevoegdheid en van geldende wetten, bepaling van het vereiste niveau van veiligheid en relevante aansprakelijkheid, vermelding van de afzender van documenten of communicatie, bewijs van de daadwerkelijke verzending of ontvangst daarvan, enzovoort. De definitie van locatiegegevens, in lid (20), erkent het belang van de geografische positie van apparatuur voor de overlegging van bewijsmateriaal in het kader van elektronische communicatienetwerken.

35. In deze definitie is gekozen voor "eindapparatuur" als parameter voor de bepaling van de geografische positie, aangezien deze term flexibel genoeg is om niet alleen computers te omvatten, maar ook ieder apparaat dat gebruikt kan worden in de context van een elektronische communicatiedienst.

36. Even belangrijk is dat deze definitie de reikwijdte van de bepaling van de geografische positie heeft beperkt tot "openbare" elektronische communicatiediensten, wat kan bijdragen tot het in balans brengen van veiligheidsredenen voor de noodzaak om geografische locatie te identificeren en privacy eisen, waar van toepassing.

37. Het concept van afzender, zoals neergelegd in lid (21), omvat niet alleen de persoon die daadwerkelijk de elektronische communicatie verstuurt, maar ook de persoon die een ander instructies geeft deze namens hem te versturen en de persoon die een elektronische agent gebruikt voor de versturing.

38. De alomvattendheid van een dergelijk concept wordt steeds belangrijker naarmate de omvang van de elektronische communicatie "verstuurd" door derden (zoals "elektronische call centers") of via elektronische agenten (zoals in de zogenaamde "web-wrap overeenkomsten ") groeit in een snel tempo.

39. De werkgroep heeft besloten om een opmerking in te lassen ter verduidelijking van het feit dat "elektronische agent" geen personen omvat. Dergelijke opmerking is in overeenstemming met de definitie van elektronische agent in lid (12).

40. **Publiek lichaam** wordt gedefinieerd in lid (22) met inbegrip van elk ministerie of overheidsdepartement, staatsbedrijven of -ondernemingen, instanties die wettelijk gezag uitoefenen, en subnationale of lokale publieke autoriteiten.

41. Een dergelijke alomvattende definitie is in overeenstemming met de definitie van **wet**, die wordt gegeven in lid (18) en omvat common law (ongeschreven recht), wetgeving en afgeleide wetgeving, evenals met de opmerking in punt 17 hierboven, waarin de mogelijkheid wordt genoemd van verdere regulering ter instelling van een systeem van authenticatie en/of certificering van digitale handtekeningen. Het probleem hier is dat elektronisch bewijsmateriaal een breed scala aan gevolgen voor overheidsinstellingen impliceert en voor iedere burger, zodat de verscheidenheid van wetgeving die het zal reguleren, evenals het aantal autoriteiten of staatsbedrijven of -ondernemingen die het zullen gebruiken, of die het kunnen reguleren vrij groot is, zodat de desbetreffende definitie alomvattend genoeg moet zijn.

42. Hoewel deze wet geen uitdrukkelijk aantal bepalingen bevat die gebruik maken van deze definitie (of indirect gebruik ervan maken, zoals in artikel 10, welke verwijst naar "de overheid"), stelt het vooraf de grote reikwijdte vast van openbare lichamen waarvan wordt verwacht dat zij verdere regelgeving zullen uitgeven of dat zij begunstigde zullen zijn van verdere regelgeving (zoals in de aangehaalde voorbeelden van de instelling van een systeem van authenticatie en/of certificering van digitale handtekeningen), wat zal zorgen voor passende gronden voor toekomstige afgeleide wetgeving.

43. De definitie van de **veiligheidsprocedure** vervat in lid (24) gaat verder dan de inhoud van de definities van "authenticatieproducten of -diensten" en "elektronische authenticatie", respectievelijk aan bod in leden (4) en (13), aangezien de integriteit van een computer berust bij de aanname van veiligheidsprocedures, onafhankelijk van eventuele tests op basis van elektronische authenticatie, alsook de technische normen met betrekking tot informatiebeveiliging zijn in principe van procedurele aard en vereisen niet noodzakelijkerwijs het gebruik van enige authenticatieproducten of -diensten. Daarom is de definitie van "veiligheidsprocedure" een belangrijk additioneel ingrediënt voor het wettigen van de productie van elektronisch bewijsmateriaal.

44. In de formulering van deze definitie zijn niet alleen veiligheidsprocedures opgenomen onderworpen aan technische normen, maar ook die bij wet zijn ingesteld, bij overeenkomst of door algemeen bekende praktijk, want het is belangrijk om de vrije wil van de belanghebbende partijen te erkennen om het gewenste niveau van veiligheidsprocedures te onderhandelen, evenals het bestaan van de beste praktijken op dit gebied op nationaal en/of internationaal niveau.

45. **Abonneegegevens** is een concept gedefinieerd in lid (27) met het doel abonneeregistratiegegevens en alle gegevens met betrekking tot documenten of communicatie betreffende die abonnee van een elektronische communicatiedienst te omvatten.

46. Registratiegegevens kunnen een belangrijk element zijn bij de productie van elektronisch bewijsmateriaal, met name waar het anonieme communicatie betreft, waardoor de noodzaak groter is om gegevens zoals naam, identiteitsdocumenten, en het adres van de abonnee te weten.

47. Op vergelijkbare wijze als wat er gebeurt met de definitie van **publieke lichamen**, is “abonneegegevens" een concept van belang voor verdere regulering van elektronische gegevens (en/of aanverwante zaken zoals de aansprakelijkheid van internet dienstverleners voor het houden van en leveren van abonneegegevens), en het belang dat van te voren neer te leggen in deze wet bestaat uit het garanderen van een uniforme betekenis voor later gebruik.

48. Lid (28) definieert verkeersgegevens met inbegrip van het omvatten van gegevens die van belang zijn bij het produceren van elektronisch bewijsmateriaal betreffende de stroom van elektronische communicatie. Details zoals herkomst, route, bestemming, datum, tijd, omvang en duur zijn erg belangrijk voor de bepaling van het auteurschap, plaats en tijd van bepaalde transacties, in het bijzonder aangezien elektronische communicatiestromen gesplitst worden in "pakketjes" die verschillende wegen kunnen afleggen voordat zij hun bestemming bereiken, zoals bij het internet.

HOOFDSTUK II – TOELAATBAARHEID

Artikel 3: Wijziging van regels inzake authenticatie en beste bewijs

49. Het belangrijkste doel van dit artikel is de integratie van deze wet neer te leggen met het common law (ongeschreven recht) en met wettelijke bepalingen die de toelaatbaarheid van bescheiden reguleren, waarbij wordt verduidelijkt dat slechts wettelijke bepalingen worden gewijzigd door deze wet, die zich bezighouden met authenticatie en met de regel van beste bewijs.

50. Onder vermelding van welke wetten zijn gewijzigd, geeft dit artikel automatisch aan dat de wetten niet gewijzigd door deze wet ook van toepassing zijn op de zaken die zij regelt. De zaken die deze wet behandelt zullen aldus worden gezien als een specifiek hoofdstuk binnen het toepassingsgebied van de meer algemene beginselen van toelaatbaarheid van bewijsmateriaal.

Artikel 4: Common law (ongeschreven recht) en wettelijke bepalingen

51. Het doel van dit artikel is om vast te stellen dat bij de toepassing van het common law of van wettelijke bepalingen die de toelaatbaarheid van bescheiden behandelen, de rechter rekening zal houden met de bepalingen van deze wet, waar het elektronische bescheiden betreft. Het is belangrijk dat de rechter het specifiek karakter erkent van de materie en van de bepalingen bedoeld in deze wet, zodat dit artikel de aandacht van de rechter vestigt op de noodzaak deze wet te handhaven.

Artikel 5: Algemene toelaatbaarheid van elektronisch bewijsmateriaal

52. Dit artikel legt het beginsel neer van non-discriminatie tegen elektronische bescheiden. Een bescheiden kan wel of niet betrouwbaar zijn als bewijsmateriaal, ongeacht of het elektronisch is of niet. Daarom is er geen reden voor discriminatie *a priori* tegen elektronische records. Men kan zelfs stellen dat bepaalde elektronische bescheiden (zoals in het geval van gecertificeerde digitale handtekeningen) betrouwbaarder kunnen zijn dan niet-elektronische bescheiden.

53. Het belang van dit artikel is dat daarin de toelaatbaarheid van elektronische bescheiden als algemene regel wordt neergelegd onderworpen aan de voorschriften vermeld in de daaropvolgende artikelen.

Artikel 6: Toepassing van de regel van het beste bewijs

54. Aangezien de regel van het beste bewijs een traditioneel rechtsprincipe is in het Common Law systeem, is het belangrijk dat wetgeving over elektronisch bewijsmateriaal in overeenstemming is met dergelijk beginsel.

55. Om de toepassing van dit beginsel te harmoniseren met de kenmerken van computers, is in dit artikel neergelegd dat aan de regel van het beste bewijs is voldaan wanneer de integriteit van een computer kan worden bewezen in of waarmee bepaalde data is geregistreerd of opgeslagen.

56. Aangezien de regel van het beste bewijs vereist dat de originelen van een gegeven document worden gepresenteerd maar het niet eenvoudig is te bepalen of sommige elektronische data een origineel is of een kopie, is het bewijs van de integriteit van een computer een aanpassing, *mutatis mutandis*, van de traditionele intentie van de regel van het beste bewijs.

57. Een dergelijke aanpassing heeft juridische, technische en economische redenen. Juridisch is de filosofie achter de regel van het beste bewijs om ervoor te zorgen dat het best mogelijke bewijs (normaal, de originelen van sommige documenten) wordt gepresenteerd. Van een technisch en economisch standpunt bezien, is het niet aannemelijk technologieën en procedures te implementeren (zoals de gecertificeerde digitale handtekening) die gelijkwaardig zijn aan een

origineel in alle elektronische bescheiden van een informatiesysteem. Daarom geeft de combinatie van juridische, technische en economische redenen aan dat de bewezen integriteit van een computer het best mogelijke bewijs is in normale omstandigheden.

58. De situaties, waarin het vermoeden van integriteit van een computer aannemelijk is, zijn vermeld in lid (2), en laten het eigenlijk toe (i) indien het bewijs wordt geleverd dat de bevinding ondersteunt dat de computer goed functioneerde, (ii) indien de elektronische bescheiden werden geregistreerd of opgeslagen door een partij die een tegenovergesteld belang heeft dan de partij die tracht het aan te voeren in een procedure, of (iii) wanneer de elektronische bescheiden werden geregistreerd of opgeslagen door een persoon die geen partij is bij de procedure of die de elektronische bescheiden niet heeft opgenomen of opgeslagen onder het beheer van een partij die het wenst aan te voeren. Kortom, een dergelijk vermoeden is van toepassing wanneer er bewijs is van de goede werking van een computer of wanneer er geen tegenstrijdige of verdachte belangen zijn van de partij die ernaar streeft de elektronische bescheiden aan te voeren in een procedure.

Artikel 7: Integriteit van informatie, en specifieke toelaatbaarheidsregels

59. Het vermoeden van de integriteit van computers overwogen in algemene termen in artikel 6 wordt ook behandeld in de bepalingen van artikel 7, waarin in het tweede lid een reeks van situaties wordt opgevoerd waarin de integriteit van elektronisch bescheiden leiden tot de aanname van de integriteit van de computer, in een juridische procedure, ongeacht of de elektronische bescheiden een verklaring van horen zeggen is of niet (zoals bedoeld in de leden (1) en (3), respectievelijk).

60. De opsomming begint met een verwijzing naar transactiebescheiden (dat wil zeggen, elektronische bescheiden), die compleet en ongewijzigd zijn gebleven afgezien van immateriële veranderingen ontstaan in het normale verloop van de communicatie, opslag of weergave. Dergelijke formulering is belangrijk gezien het feit dat computers en elektronische bescheiden nauwelijks kunnen worden "bevroren" en immuun gehouden van enige vorm van verandering, en dat beperkt de reikwijdte van wijzigingen die werkelijk de betrouwbaarheid van elektronisch bescheiden in gevaar kunnen brengen.

61. De beoogde tweede situatie verwijst naar elektronische bescheiden gewaarmerkt of elektronisch ondertekend, gebruikmakend van een methode verstrekt door geaccrediteerde certificatie-instanties. Het voordeel van het instellen van geaccrediteerde certificatie-instanties of -entiteiten kan hier duidelijk worden opgemerkt aangezien dergelijke accreditatie een formeel vermoeden op zichzelf garandeert en dus bijdraagt aan het vermoeden de materiële integriteit van het elektronisch dossier te concluderen.

62. De lijst gaat verder met vermelding van het alternatief van notariële bekrachtiging van de integriteit en inhoud, wat een andere optie is voor belanghebbende partijen en dit kan van belang zijn, aangezien notarissen vertrouwen kunnen toevoegen aan de integriteit en de inhoud waarvan zij getuigen.

63. De vierde hypothese bestaat uit het registreren op niet-herschrijfbare media, die per definitie geen enkele wijziging toelaten zodra elektronische bescheiden de eerste keer zijn opgeslagen. Dit kan een praktische en handige optie zijn voor de belanghebbende partijen die een gemakkelijk toegankelijk en goedkoper alternatief beschikbaar wensen te hebben.

64. De vijfde situatie is die van de technische bewijsgaring in de rechtsgang, waar de deskundige aangewezen door de rechter de integriteit van de elektronische record kan bevestigen.

65. De diversiteit van situaties die het vermoeden van integriteit van elektronische bescheiden staven en zich uitstrekken tot het vermoeden van integriteit van een computer is belangrijk, omdat elke belanghebbende toegang moet hebben tot een aantal praktische middelen voor de productie van elektronisch bewijsmateriaal.

Artikel 8: Print-outs

66. Hoewel een print-out op zichzelf niet elektronisch is, is het gegenereerd met behulp van elektronische middelen. Daarom, als de belanghebbende partijen consequent hebben aanvaard dat het een echte vertegenwoordiging vormt van de bijbehorende elektronische bescheiden, waarvan de betrouwbaarheid kan worden afgeleid uit het gedrag van de partijen staaft de bevinding dat dit aan de regel van het beste bewijs voldoet. Dit is wat artikel 8 vaststelt, en het is belangrijk omdat de meeste mensen de elektronische bescheiden inzake elektronisch bewijs afdrukken.

Artikel 9: Bewijslast inzake de authenticiteit van elektronisch bewijsmateriaal

67. Als algemene regel heeft de persoon die wenst elektronische bescheiden aan te voeren als bewijsmateriaal de bewijslast inzake de relevante authenticiteit daarvan in een juridische procedure.

68. Echter, kwetsbaardere personen zoals consumenten en kinderen kunnen voordeel hebben bij wettelijke bepalingen die de bewijslast omkeren. In dergelijk geval zullen die wettelijke bepalingen voorrang hebben boven de algemene regel die is neergelegd in artikel 9.

69. Dergelijke opmerking is belangrijk omdat kwetsbaardere personen vaak technisch en/of economisch niet in staat zijn bewijsmateriaal te produceren gebaseerd op elektronische bescheiden, maar niettemin moet hun toegang tot de rechter en de mogelijkheid om op een juiste verdediging te kunnen rekenen worden bevorderd en gegarandeerd.

Artikel 10: Standaarden

70. Gebruikelijke praktijken en gewoonten zijn een belangrijke indicatie over wat wordt verwacht als gedragspatroon voor registratie of opslag van elektronische bescheiden. Daarom kan bewijs worden gepresenteerd inzake bestaande normen, procedures, gebruik en praktijk die een dergelijk patroon aantonen en een richtlijn geven voor wat er wordt verwacht over toelaatbaarheid van elektronische bescheiden.

71. Artikel 10 staat stil bij de erkenning van een richtlijn en legt een verband met de aard van het bedrijf of de inspanning waarnaar het verwijst, evenals naar de aard en het doel van de elektronische bescheiden. Dit verband is belangrijk omdat de standaarden die gelden voor een bepaalde markt andere doelstellingen kan presenteren dan die van toepassing zijn op een andere markt (zoals het geval is waar het de veiligheid van de informatie betreft).

72. Dit artikel eindigt met het oproepen van overheidsinstanties die belast zijn met de afgifte van technische standaarden of met het instellen van veiligheidsprocedures om de juiste oriëntatie op de naleving van dit artikel te verstrekken. Dit is belangrijk omdat de bevoegde autoriteiten een algemene oriëntatie kunnen en moeten verstrekken, evenals een oriëntatie afgestemd op de individuele markten of omstandigheden, indien van toepassing.

Artikel 11: Beëdigde verklaringen

73. Artikel 11 legt neer dat elektronisch bewijsmateriaal kan worden gepresenteerd in de vorm van beëdigde verklaringen. Dit is weer een ander alternatief beschikbaar aan de belanghebbende partijen om elektronisch bewijsmateriaal te produceren.

74. De werkgroep heeft gedebatteerd over het nut andere bepalingen in dit artikel op te nemen, zoals een verklaring dat elke deponent de plicht heeft om een beëdigde verklaring af te leggen naar beste weten of geloof, en dat hij onderworpen is aan sancties opgelegd door de rechter in geval zijn verklaring onwaar blijkt te zijn, naast een bepaling over kruisverhoor inzake de beëdigde verklaringen.

75. Gezien het feit dat de elektronische bescheiden van vluchtige aard zijn, kan de afhankelijkheid van beëdigde verklaringen een punt van zorg zijn, en daarom kan dat in evenwicht worden gebracht door enige nadruk te leggen op de aansprakelijkheid van de deponent. Echter, de regelgeving met betrekking hiertoe kan overlappen met bestaande procedurele normen. Vandaar, dat de werkgroep heeft besloten dat de goedkeuring van de betreffende aanpak wordt overgelaten aan het oordeel van de begunstigde staat.

Artikel 12: Overeenstemming over toelaatbaarheid van bewijsmateriaal

76. Als algemene regel, tenzij geen enkele andere wet anderszins bepaald, kunnen de partijen bij een juridische procedure de toelaatbaarheid van gegeven elektronische bescheiden overeenkomen, afhankelijk van het oordeel van de rechter.

77. Deze bepaling zal niet van toepassing zijn op strafrechtelijke procedures waar de verdachte niet juridisch werd bijgestaan of vertegenwoordigd op het moment dat dergelijke overeenstemming werd bereikt.

78. Artikel 12 is belangrijk aangezien het een particuliere overeenkomst bevoordeeld, waardoor controverses kunnen worden vermeden, die anders kosten van een onnodige procesgang en vertragingen kunnen bepalen.

Artikel 13: Elektronische handtekening

79. Vergelijkbaar met wat is voorzien in artikel 5 met betrekking tot elektronische bescheiden, wordt in artikel 13 bepaald in lid (1) dat elektronische handtekeningen niet mogen worden gediscrimineerd uitsluitend omdat zij elektronisch zijn.

80. Lid (2) legt de mogelijkheid neer dat elektronische handtekeningen kunnen worden getoetst op welke wijze dan ook. Gezien het snelle tempo van technologische ontwikkelingen op het gebied van elektronische handtekeningen en het belang van de naleving van het beginsel van technologische neutraliteit, lijkt het onwaarschijnlijk dat de bestaande verschillende manieren van toetsen van elektronische handtekeningen goed worden afgebakend.

81. Een illustratief voorbeeld van hoe verschillend de wijzen van het staven van elektronische handtekeningen kunnen zijn, wordt gegeven in hetzelfde lid, door te verwijzen naar het bewijs van het bestaan van een procedure waarbij een persoon een symbool moet uitvoeren ter verificatie dat de elektronische bescheiden van die persoon afkomstig zijn (wat heel gebruikelijk is op websites van het wereldwijde web als voorwaarde om internetgebruikers toegang te geven tot specifieke delen van dergelijke websites).

Artikel 14: Eisen aan elektronische handtekeningen

82. Lid (1) van artikel 14 bepaalt dat elektronische handtekeningen voldoen aan wettelijke vereisten aan een handtekening van een persoon indien zij net zo betrouwbaar en geschikt zijn. Deze bepaling is belangrijk omdat elektronische handtekeningen effectief betrouwbaar en geschikt zijn en in sommige gevallen zelfs meer dan niet-elektronische handtekeningen.

83. Lid (3) bepaalt dat de partijen vrij zijn een bepaalde wijze van elektronische handtekening overeen te komen, tenzij anderszins bepaald door de wet. Deze bepaling is belangrijk aangezien het in overeenstemming is met de algemene beginselen van vrijheid om bewijsmateriaal vast te stellen, terwijl het in een commentaar voorziet dat toepasselijk kan zijn, bij voorbeeld, waar het gebruik van elektronische handtekeningen gebaseerd op cryptografie in strijd kan zijn met de individuele privacy- of nationale veiligheidswetten.

84. Partijen bij een overeenkomst geven misschien niet aan welk type elektronische handtekening zal worden gebruikt door hen. Dit is een situatie die heel gebruikelijk is in de praktijk, dus lid (4) besteedt er aandacht aan en voorziet in een reeks criteria voor het voldoen aan contractuele vereisten inzake het elektronisch tekenen van gegevensberichten. De criteria waarnaar wordt verwezen zijn onder meer het verband tussen de ondertekenaar en de handtekeningaanmaakgegevens (die onder het beheer staan van de ondertekenaar), en de mogelijkheid voor het opsporen van enige wijziging van de elektronische handtekening op het moment van ondertekening of erna.

Artikel 15: Alternatieve technieken en procedures voor de productie van elektronisch bewijsmateriaal

85. Artikel 15 verwijst naar alternatieve technieken en procedures voor de productie van elektronisch bewijsmateriaal met betrekking tot bepaalde elektronische bescheiden, waarbij wordt geciteerd (i) attestatie door notarissen, of vrederechters of andere soortgelijke autoriteiten, (ii) de registratie op een niet-herschrijfbaar medium, en (iii) gerechtelijke computerkunde in justitiële bewijsgaring en -uitwisseling in de rechtsgang.

86. De erkenning van gerechtelijke computerkunde, dat een kennisgebied is dat is gespecialiseerd in elektronisch bewijsmateriaal, is bijzonder belangrijk, in het bijzonder omdat het wordt geassocieerd met justitiële bewijsgaring en -uitwisseling, waardoor het zelfs betrouwbaarder wordt aangezien van de expert aangesteld door de rechter wordt verwacht dat die neutraal is en een gekwalificeerde professional.

Deel III

HOOFDSTUK III – ALGEMENE BEPALINGEN

Artikel 16: Toelaatbaarheid van elektronische bescheiden van andere landen

87. Artikel 16 legt de toelaatbaarheid neer van elektronische bescheiden die afkomstig zijn uit een ander rechtsgebied, mits de integriteit van de computer die in verband wordt gebracht met het relevante elektronische bewijsmateriaal in overeenstemming is met de standaarden vergelijkbaar met die welke van toepassing zijn op het bewijs van integriteit van elektronische bescheiden afkomstig uit het binnenlands rechtsgebied (d.w.z. bewijs dat de computer juist functioneerde en dat de integriteit van de elektronische bescheiden behouden was).

88. Deze bepaling is van belang voor de veilige stroom van elektronische communicatie met andere landen, welke essentieel is voor de belangen van de begunstigde landen voor het uitbreiden van elektronische communicatie en bedrijven met andere landen.

89. Gegeven het feit dat elk land zijn eigen regels heeft voor elektronisch bewijsmateriaal, kan het vastleggen van een minimale vereiste, door slechts bewijs te eisen over de integriteit van de computers of van de elektronische bescheiden, de taak vergemakkelijken om een algemene deler vast te stellen.

Artikel 17: Erkenning van buitenlandse elektronische documenten en handtekeningen

90. Alhoewel artikel 16 handelt over elektronische bescheiden die afkomstig zijn uit andere landen, handelt lid (2) van artikel 17 over elektronische informatie die zich bevindt in andere landen.

91. Dit lid geeft een reeks van situaties waarin gelijke behandeling kan worden gegeven aan de informatie die zich bevindt in een buitenlands rechtsgebied, zoals te vergelijken met informatie die zich in het binnenlands rechtsgebied bevindt. Hieronder zijn het bepalen van de rechter in die zin en het bestaan van een internationaal verdrag dat zorgt voor de relevante erkenning.

92. Deze bepaling is belangrijk want het kan de veilige stroom van elektronische communicatie en transacties versterken tussen de begunstigde staat en andere landen. Aangezien elektronische bescheiden die zich bevinden in het buitenland technisch moeilijker te benaderen zijn voor het doel van het verifiëren van de integriteit daarvan, garandeert deze bepaling procedures en een situatie die dergelijke technische beperkingen kan overbruggen.

Artikel 18: Interpretatie in overeenstemming met internationaal geaccepteerde beginselen

93. Artikel 18 bepaalt dat deze wet wordt geïnterpreteerd en gehandhaafd in het licht van de beginselen van technologische neutraliteit en functionele gelijkwaardigheid, wat internationaal geaccepteerde beginselen zijn.

94. Die beginselen zijn aangenomen door zo goed als alle landen die elektronisch bewijsmateriaal en aanverwante aspecten hebben gereguleerd. Het beginsel van technologische neutraliteit bevordert sociale digitale insluiting aangezien het de mogelijkheid tot ontwikkeling vergroot of het gebruik van gelijkaardige technologieën, wat de betere toegang bevordert en lagere prijzen. Het principe van functionele gelijkwaardigheid erkent dat er geen beperkingen worden opgelegd aan de on-line omgeving die niet aanwezig zijn in de off-line omgeving, wat de migratie van communicatie en transacties van de laatste naar de eerste bevordert.

95. Deze bepaling is belangrijk aangezien het vaststelt dat deze beginselen van toepassing zijn op elke bepaling van deze wet, wat de interpretatie en handhaving daarvan zal sturen in de richting van de sociale en economische doelen die worden beoogd door deze beginselen.

Artikel 19: Regelgeving

96. Artikel 19 geeft bevoegdheid aan de Minister voor het neerleggen van regelgeving voor het uitvoeren van de doelen van deze wet en voor het voorschrijven van alles wat vereist of toegestaan is te worden voorgeschreven, en voegt daaraan toe dat de Minister daarbij de internationale beste toepassing in de praktijk en standaarden kan overwegen.

97. Het doel van dit artikel is de erkenning van en het aandacht schenken aan het voordeel van het uitvaardigen van verdere regulering met als doel de juiste implementatie van deze wet.

98. De werkgroep heeft met betrekking hiertoe een aantal zaken besproken die zullen worden aangepakt in internationale verdragen of nationale regelgeving.

99. Zaken zoals een accreditatiesysteem voor electronische handtekeningen (waaronder authenticatie, certificatie en accreditatie van digitale handtekeningen, attributen, en tijd), integratie met procedurele wetten (bij voorbeeld, om te verzekeren dat de uitvoering van procedures van huiszoekingsbevelen, bevelen tot overlegging, directe vergaring, video-conferenties van gerechtelijk verhoor, elektronische gerechtelijke procedures, versneld bewaren van data, en interceptie van communicatie deze wet opvolgen), en integratie met aanverwante inhoudelijke wetten (over databehoud, aansprakelijkheid van internet dienstverleners, en met betrekking tot cybercriminaliteit, onder andere) daarvan is geconstateerd dat die de aandacht verdienen van de nationale regelgever.

100. Uitdagende trends zoals cloud-computing, steganografie, LiveCD, en andere die zorgpunten kunnen opleveren voor de productie en erkenning van elektronisch bewijsmateriaal werden genoemd als onderwerpen die speciale studies vereisen. Het belang van het uitvoeren van dergelijke studies, en het uitvaardigen van daaraan gerelateerde regelgeving, is dat anders de handhaving van deze wet kan worden afgezwakt of de wet veroudert.

101. Ontwikkeling van regionale wetgeving, en de harmonisatie met internationale verdragen, wordt geacht van belang te zijn voor de begunstigde staat om de formele samenwerking met andere landen en periodieke controle en afstemming met de alsdan geldende internationale beste toepassing in de praktijk te garanderen. Het belang van deze ontwikkeling en harmonisatie is dat de handhaving van deze wet anders wordt beperkt in omvang of gereduceerd tot "informele" samenwerking.

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[7]	J Paul
PRESCOD	Kwesi

[7] 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[8]	J Paul
PRESCOD	Kwesi

[8] 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