Gobierno de Reconciliación y Unidad Nacional
Unida Nicaragua Triunfa

APORTES DE NICARAGUA EN EL SEGUNDO PERIODO DE SESIONES DEL COMITÉ AD HOC ENCARGADO DE ELABORAR UNA CONVENCIÓN INTERNACIONAL AMPLIA CONTRA LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES CON FINES DELICTIVOS.

I. DISPOSICIONES SOBRE CRIMINALIZACIÓN

PRIMER GRUPO DE PREGUNTAS:

1. ¿Qué tipo de elementos [mentales/culpables] (por ejemplo, la intención [maliciosa/deshonesta]) deberían captarse al considerar los delitos de acceso e interceptación [ilegal/ilegal/no autorizada]? ¿Debería la convención considerar la posibilidad de establecer protecciones legales para los investigadores de ciberseguridad y otros profesionales que trabajan en ciberseguridad (incluyendo, entre otros, a los probadores de penetración)?

R: Debe considerarse el acceso directo o indirecto, parcial o total, la interceptación, el uso parcial o totalmente de un sistema informático o de comunicaciones, la utilización de Tecnologías de la Información y la Comunicación.

2. ¿Cree que alguna de las conductas propuestas debe dar lugar o tener la intención de dar lugar a un daño específico o grave, o a un daño material, para ser considerada como delito? ¿Cómo debería definirse el "daño"?

R: Lo que se persigue es la apropiación de los datos de ellos o cometer otro delito con éstos.

3. ¿Debería considerarse la infracción de las medidas de seguridad como condición para establecer algunas conductas como delito y, en caso afirmativo, en qué circunstancias?

R: Debe considerarse la tipificación de la infracción en la utilización de las tecnologías para la comisión de ilícitos, así como la causa de la apropiación. Generalmente la tipificación está supeditada a la intromisión, apropiación, interceptación de información y comunicaciones para cualquier fin.

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la interceptación intencional de información digital, realizada sin la debida autorización y/o en violación de las normas establecidas, incluida la que implique el uso de técnicas medios para interceptar datos de tráfico y datos procesados por medio de las TIC que no están destinados al uso público.

4. ¿Podríamos considerar las disposiciones propuestas sobre "Obstrucción de un ordenador, programa o datos", "Ataque al diseño de un sitio" y "perturbación de las redes de tecnologías de la información y las comunicaciones", ¿cómo formas de interferencia [ilegal] [no autorizada]?

R: Si. El que intencionalmente y por cualquier medio interfiera o altere el funcionamiento de un sistema informático o los datos contenidos en él, de forma temporal o permanente debe ser castigado por la ley.

5. ¿Cómo cree que la convención debería tratar la cuestión del "acceso no autorizado o la interferencia con una infraestructura de información crítica"?

R: Promover la adopción y fortalecimiento de medidas para prevenir y combatir eficazmente los delitos relacionados con las TIC y otros actos ilícitos;

Impedir acciones dirigidas a la confidencialidad, integridad y disponibilidad de las TIC, y prevenir el uso indebido de las TIC, tipificando como punibles los actos contemplados en esta Convención, y otorgando facultades suficientes para combatir eficazmente tales delitos y otros actos ilegales, facilitando su detección. , investigación y enjuiciamiento tanto a nivel nacional como internacional y mediante el desarrollo de acuerdos para la cooperación internacional;

Mejorar la eficiencia de la cooperación internacional y desarrollar dicha cooperación, incluso en el área de capacitación y provisión de asistencia técnica para prevenir y combatir los delitos relacionados con las TIC.

6. ¿Por qué algunos Estados miembros optan por utilizar el término "ilegal", y otros por "ilícito", y otros por "no autorizado", y cuál sería la diferencia en su opinión?

R: Los términos ilegales e ilícitos, son sinónimos, dependerá del evento en el que se esté utilizando y no autorizado es más un término utilizado en políticas o normativas.

7. ¿Por qué algunos Estados miembros eligen el término "sin derecho", otros eligen "sin la debida autorización", y otros "ilegal", y cuál sería la diferencia en su opinión?

R: Igual a la respuesta anterior, los términos van a depender del contexto en que se utilicen, el término común debería de ser "ILEGAL"

8. ¿Existe alguna diferencia entre "datos" o "información digital", y cuál sería el término adecuado a utilizar?

R: No existe ninguna diferencia, todo depende del contexto en que se esté utilizando el término (la información digital, está compuesta de datos).

9. ¿Existe alguna razón para que algunas propuestas no incluyan el deterioro de los datos en sus propuestas, y para que otras prefieran el término "bloqueo" al de "supresión"?

R: El término DETERIORO DE DATOS, no es común utilizarlo y nuestro hemisferio, generalmente utilizamos el DAÑO A LA INTEGRIDAD DE LOS DATOS.

10. ¿El acto de "copiar" forma parte de la interferencia de datos?

R: No, es parte del acceso ilegal.

11. En cuanto a los actos delictivos relacionados con la interferencia de [sistemas/redes], ¿cuáles son, en su opinión, los dispositivos (y su nomenclatura) a los que se aplica este artículo: sistema informático, red informática, red de telecomunicaciones, dispositivo electrónico o redes TIC?

R: Esto abarca TODOS LOS DISPOSITIVOS de las tecnologías de la información y las comunicaciones.

12. ¿Existe la necesidad de que la interceptación se realice de forma fraudulenta?

Salvo

R: Salvo que sea una interceptación legal con orden judicial; cualquier otra interceptación sería fraudulenta, o ilícita e implicaría su penalización.

SEGUNDO GRUPO PREGUNTAS:

1. ¿Cree usted que el delito de fraude, cometido total o parcialmente en línea, es suficiente para abarcar otras conductas como el robo, la estafa, los delitos financieros y los delitos relacionados con los instrumentos de pago electrónico?

R: En relación con la primera pregunta, Nicaragua considera que el delito de Fraude no cubre necesariamente las otras conductas enunciadas, en ese sentido, el Fraude Informático está concebido como el que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación de los sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, para cubrir los otras conductas delictivas deben realizarse las otras tipificaciones en base a los hechos ocurridos.

2. En lo que respecta a la falsificación informática/TIC, ¿qué tipo de elementos [mentales/culpables] (por ejemplo, intención [dolosa/deshonesta]) deberían incluirse en la tipificación de dicho acto? ¿Debería la convención considerar el establecimiento de protecciones legales para los investigadores de ciberseguridad y otros profesionales que trabajan en ciberseguridad (incluyendo, entre otros, a los probadores de penetración)?

R: Nicaragua considera que quien indebidamente obtenga datos personales sensibles o información pública reservada contenida en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, incurre en un hecho de falsificación y las mismas deberían ser tipificadas en esta convención.

Visto que las conductas descritas anteriormente se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad soberana del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información pública clasificada como reservada de conformidad a la ley de la materia.

3. ¿Podríamos considerar las disposiciones propuestas sobre "creación y uso de información digital para engañar al usuario", como una forma de falsificación [informática] [TIC]?

R: Si, debe ser penalizado. En opinión de Nicaragua, la conducta que conlleva la creación y uso de información digital para engañar al usuario debe ser tipificado como delito para que sea penalizado.

4. ¿Cómo cree que la convención debería tratar los delitos relacionados con la identidad?

R: El que suplantare o se apoderare de la identidad informática de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, daña, extorsiona, defrauda, injuria o amenaza a otra persona para ocasionar perjuicio u obtener beneficios para sí mismo o para terceros.

5. ¿Cuál sería la justificación para incluir ofensas relativas a la violación a la propiedad intelectual en esta convención, estando cubierta en otros instrumentos?

R: Se refiere a la violación de los derechos de autor según se definan en la legislación de cada estado, cuando esta acción se comete intencionalmente, a escala comercial y por medio de un sistema informático, así como a la violación de otros derechos afines.

TERCER GRUPO DE PREGUNTAS:

1. ¿Cómo pueden definirse los delitos relacionados con el abuso sexual infantil en línea para proporcionar a los niños la mayor protección contra el daño? ¿Qué debe tenerse en cuenta en la elección de la terminología?

R: La utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía a través del uso de las Tecnologías de la Información y la Comunicación quien, por medio del uso de las Tecnologías de la Información y la Comunicación, induzca, facilite, promueva, utilice, abuse o explote con fines sexuales o eróticos a niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, haciéndola presenciar o participar en un comportamiento, espectáculo o acto sexual público o privado, se le debe penalizar.

Toda persona que haga propuestas implícitas o explícitas a personas menores de 16 años o personas con discapacidad necesitada de especial protección para sostener encuentros de carácter sexual o erótico, o para la producción de pornografía a través del uso de las Tecnologías de la Información y la Comunicación para sí o para terceros.

2. ¿Debería tipificarse como delito el acceso o la visualización de material de abuso sexual infantil; en caso afirmativo, debería establecerse una condición para la obligación de la tipificación de estos actos, como por ejemplo "en consonancia con los principios jurídicos/la legislación interna de un Estado Parte" o "sin perjuicio de la legislación interna de un Estado Parte"?

R: El acceso y la visualización del material pornográfico de acuerdo a nuestra legislación es una prueba y debe presentarse en juicio, porque en caso contrario el hecho quedaría como un presunto y se revictimizaría a la víctima.

Más bien en los patrullajes de las redes, este tipo de material debería de eliminarse y no importa de qué o tal estado seas, hay que sacarlo de las redes.

3. ¿Habría un acuerdo general sobre el límite de edad para que la definición de niño sea menor de 18 años, y a efectos de los artículos (que estaría en consonancia con la Convención sobre los Derechos del Niño)?

4. Cuál sería la justificación (falta de armonización, aparición de nuevas formas de abuso sexual en línea debido a los nuevos medios tecnológicos, insuficiencia de los instrumentos internacionales actuales...) para la inclusión de las disposiciones propuestas sobre: "extorsión sexual, difusión no consentida de imágenes íntimas y otros delitos relacionados con la pornografía"?

R: La falta de armonización, nuestra legislación establece que quien atormente, hostigue, humille, insulte, denigre u otro tipo de conducta que afecte la estabilidad psicológica o emocional, ponga en riesgo la vida o la integridad física, por medio del uso de las Tecnologías de la Información y la Comunicación, Cuando la víctima sea niña, niño, adolescente o persona con discapacidad necesitada de especial protección, se penaliza con una mayor cuantía la falta penal

Acoso sexual a través del uso de las Tecnologías de la Información y la Comunicación, Cuando una persona mayor de edad envíe mensajes, frases, fotografías, vídeos u otra acción inequívoca de naturaleza o contenido sexual a otra persona sin su consentimiento a través del uso de las Tecnologías de la Información y la Comunicación

5. ¿Cuál sería la justificación para la inclusión de las disposiciones propuestas sobre: "incitación o coacción al suicidio y participación de menores en la comisión de actos ilícitos"?

R: Con relación al fomento o coacción al SUICIDIO, se deben adoptar medidas legislativas y de otra índole que sean necesarias para tipificar como delito en el derecho interno de cada estado, la incitación al suicidio o la coacción al mismo, incluso de menores, mediante presiones psicológicas o de otro tipo sobre las redes de información y telecomunicaciones, incluida Internet.

Los Delitos relacionados con la participación de menores en la comisión de actos ilícitos que pongan en peligro su vida o su salud, se deben adoptar medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno el uso de las TIC para involucrar a menores en la comisión de actos ilegales que pongan en peligro su vida, salvo los actos previstos en el artículo 16 de la presente Convención.

Nuestra legislación penaliza a quien, haciendo uso de las Tecnologías de la Información y la Comunicación, incite, instigue, provoque o promueva la comisión de delitos, ensalce el crimen o enaltezca a su autor o partícipes o se lo adjudique,

6. ¿Cuál sería la justificación para la inclusión de las disposiciones propuestas sobre: "envío de mensajes ofensivos a través del servicio de comunicación; amenaza y chantaje; violación de la intimidad"?

Las amenazas a través de las Tecnologías de la Información y la Comunicación, las contemplamos como quien amenace a otro a través del uso de las Tecnologías de la Información y la Comunicación con:

a. Causar a él, a su familia o a otras personas con las que esté relacionado, un mal que constituya delito y que por su naturaleza parezca verosímil, se le impondrá pena de uno a tres años de prisión.

b. Hacer imputaciones contra el honor, o el prestigio, violar o divulgar secretos, con perjuicio para él, su familia, otras personas con la que esté relacionado, o entidad que representa o en que tenga interés, se le impondrá pena de dos a cuatro años de prisión.

Si la amenaza se hiciera en nombre de entidades o grupos reales o supuestos, se impondrá pena de tres a cinco años de prisión.

Si la amenaza de un mal que constituya delito fuese dirigida a atemorizar a los habitantes de una población, grupo étnico, cultural o religioso, colectivo social o a cualquier otro grupo de personas y tuvieran la capacidad necesaria para conseguirlo, se impondrá pena de cuatro a seis años de prisión.

CUARTO GRUPO DE PREGUNTAS:

1. ¿Cuál sería la justificación para la inclusión de las siguientes disposiciones propuestas?

a) "Delitos relacionados con la discriminación, el racismo o la xenofobia";

b) "Delitos relacionados con la distribución de estupefacientes y sustancias psicotrópicas, el tráfico de armas, la distribución ilegal de medicamentos y productos médicos falsificados; la fabricación de armas, la trata de personas, la asociación delictiva".

R: La justificación es el uso de las tecnologías de la información y las comunicaciones para incentivas y promover la comisión de este tipo de ilícitos:

Cada Estado parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito u otro acto ilegal en su derecho interno la humillación por medio de las TIC de una persona o grupo de personas por motivos de raza, etnia, idioma, origen o afiliación religiosa.

Delitos relacionados con la distribución de estupefacientes y sustancias psicotrópicas, se deberán adoptar medidas legislativas y de otra índole que sean necesarias para tipificar como delito en el derecho interno de cada estado, el tráfico ilícito intencional de estupefacientes y sustancias psicotrópicas, así como de los materiales necesarios para su fabricación, por medio de las TIC.

Delitos relacionados con el tráfico de armas; cada Estado adoptará medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno el tráfico ilícito intencional de armas, municiones, artefactos explosivos y sustancias explosivas por medio de las TIC.

Distribución ilegal de medicamentos y productos médicos falsificados, Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la distribución ilegal intencional de medicamentos y productos médicos falsificados por medio de las TIC.

Distribución ilegal de medicamentos y productos médicos falsificados; adoptar medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la distribución ilegal intencional de medicamentos y productos médicos falsificados por medio de las TIC.

2. ¿Cuál sería la justificación para la inclusión de una disposición sobre "delitos relacionados con el terrorismo y delitos relacionados con el extremismo"?

R: Ilícitos relacionados con el terrorismo; adoptar medidas legislativas y de otra índole que sean necesarias para tipificar como delito la utilización de las tecnologías de la información y las comunicaciones para la comisión de actividades terroristas, la incitación, el reclutamiento u otra participación en actividades terroristas, la promoción y la justificación del terrorismo, o para la recaudación o provisión de fondos para su financiación.

Con relación al extremismo, cada Estado parte adoptará medidas necesarias para tipificar como delito u otro acto ilegal en su derecho interno la distribución de material que implique actos ilegales por motivos políticos, ideológicos, sociales, raciales, étnicos, odio o enemistad religiosa, defensa y justificación de tales acciones, o para proporcionar acceso a dichos materiales, por medio de las TIC.

3. ¿Cuál sería la justificación para la inclusión de una disposición sobre la "incitación a la actividad subversiva o armada"?

R: Actividad subversiva o armada: cada Estado adoptará medidas legislativas y de otra índole que sean necesarias para tipificar como delito las llamadas emitidas por medio de las TIC para actividades subversivas o armadas dirigidas al derrocamiento violento del gobierno de otro Estado.

4. ¿Qué justificación tendría la inclusión de una disposición sobre "rehabilitación del nazismo, justificación del genocidio o crímenes contra la paz y la humanidad"?

R: Rehabilitación del nazismo, justificación del genocidio o crímenes contra la paz y la humanidad, tipificar como delito en su derecho interno la difusión intencional por medio de las TIC de materiales que nieguen, aprueben o justifiquen actos que constituyan genocidio o crímenes contra la paz y la humanidad, tipificados por la

Sentencia del Tribunal Militar Internacional formado en virtud del Acuerdo de Londres del 8 de agosto de 1945.

5. ¿Debería la convención contener una disposición que penalice "el uso de las TIC para cometer actos tipificados como delitos en el derecho internacional"?

R: Uso de las TIC para cometer actos tipificados como delitos en el derecho internacional, cada estado debe adoptar medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno el uso de las TIC para cometer un acto que constituya un delito en virtud de cualquiera de los acuerdos internacionales enumerados en el anexo de la presente Convención.

Un estado al ratificar, aceptar, aprobar o adherirse, a los acuerdos enumerados en la presente Convención podrá ser parte de lo que aquí se acuerde y La declaración dejará de surtir efecto tan pronto como el estado así lo solicite.

Cuando un Estado parte deje de ser parte en un acuerdo enumerado en el Anexo de la presente Convención, podrá hacer una declaración con respecto a ese acuerdo (acuerdos), según lo dispuesto en el párrafo anterior.

QUINTO GRUPO DE PREGUNTAS:

1. ¿Apoyarían los Estados miembros la inclusión de disposiciones sobre la penalización de la obstrucción a la justicia y el blanqueo del producto de los delitos contemplados en la convención?

R: Consideramos necesario apoyar en esta convención el establecimiento de penas contra la obstrucción de la justicia y el blanqueo de capitales con la utilización de las tecnologías de la información y las comunicaciones, debiéndose hacer los correspondientes ajustes en las legislaciones correspondientes en cada uno de los estados.

Cada Estado parte, de conformidad con los principios fundamentales de su ordenamiento jurídico, elaborará y aplicará o seguirá una política eficaz y coordinada para combatir los delitos y otros actos ilegales relacionados con el uso de las TIC.

2. ¿Cómo cree que la convención debería tratar la participación en, la tentativa de, así como la complicidad en un delito?

R: Cada Estado deberá velar por que el establecimiento, la ejecución y la aplicación de las facultades y procedimientos previstos estén sujetos a las condiciones y salvaguardias previstas en su legislación interna, que garantizará la protección adecuada de los derechos humanos y las libertades, incluidos derechos derivados de las obligaciones que el Estado parte ha contraído en virtud del Pacto Internacional de Derechos Civiles y Políticos de 16 de diciembre de 1966 y otros instrumentos internacionales de derechos humanos aplicables.

3. ¿Debería ampliarse la responsabilidad penal más allá de las personas físicas a las personas jurídicas?

R: Desde el punto de vista penal, la capacidad de acción de responsabilidad y de pena, exige la presencia de una voluntad, entendida como facultad psíquica de la persona individual, que no existe en la persona jurídica, mero ente ficticio al que el derecho atribuye capacidad a otros efectos distintos penales; la culpabilidad y la pena, la persona jurídica no tiene capacidad de acción, de culpabilidad ni de pena. La sanción a la persona jurídica puede afectar a los socios inocentes, lo que

atentaría contra el principio de culpabilidad o de la personalidad de los hechos y las penas.

4. ¿Podría el convenio seguir la formulación de la responsabilidad de las personas jurídicas contenida en el artículo 10 de la UNTOC? ¿Sería necesario un delito separado que castigara la negligencia de las personas jurídicas en el mantenimiento de las medidas de seguridad requeridas?

5. ¿Cree usted que el convenio debería incluir una disposición sobre las circunstancias agravantes? En caso afirmativo, ¿debería tratarse de una disposición general sobre las circunstancias agravantes, o deberían incluirse en artículos específicos un elemento calificador de las circunstancias agravantes? ¿Y las circunstancias atenuantes?

R: Cada artículo especifico dada sus características particulares debería de contener sus circunstancias agravantes y atenuantes, sin menos cabo del diseño de unas disposiciones generales sobre circunstancia en las que pudiese o no ocurrir un hecho delictivo en el ámbito de las tecnologías de la información y las comunicaciones

6. En cuanto a "otros actos ilícitos", ¿podría el apartado 3 del art. 3 del art. 34 de la UNTOC ("Los Estados partes podrán adoptar medidas más estrictas o severas que las previstas en la presente Convención...") ser una solución para cubrir todos estos delitos?

APORTES DE NICARAGUA EN EL SEGUNDO PERIODO DE SESIONES DEL COMITÉ AD HOC ENCARGADO DE ELABORAR UNA CONVENCIÓN INTERNACIONAL AMPLIA CONTRA LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES CON FINES DELICTIVOS.

II. DISPOSICIONES GENERALES

1. ¿Cuál es la mejor manera de garantizar una convención adecuada teniendo en cuenta la diversa gama de medios tecnológicos utilizados para perpetrar la gama de delitos que se tipifican como delitos en virtud de esta convención?

R: La mejor manera es la cooperación entre los estados, el uso responsable de las tecnologías de la Información y las comunicaciones; así mismo consideramos que esta convención debe dejar establecido toda la gama de delitos posibles que ocurren en el ciberespacio, previendo la evolución constante de las tecnologías y modos de operar de la ciberdelincuencia.

2. ¿Cómo podemos asegurarnos de que la convención siga siendo adecuada para su propósito considerando los futuros desarrollos tecnológicos?

R: Debe quedar establecido en esta convención, la reunión periódica de un grupo de expertos para ir actualizando y modernizando la misma, tomando en cuenta la constante evolución de las tecnologías de la información y las comunicaciones.

3. ¿Piensa que un capítulo sobre disposiciones generales, siguiendo la misma estructura que en UNCAC y UNTOC, podría ser posible para esta convención? (En su capítulo de disposiciones generales, las dos convenciones antes mencionadas contienen una disposición sobre "enunciado de propósito", "uso de términos", "ámbito de aplicación" y "protección de la soberanía"). De no ser así, ¿qué disposición debería agregarse o eliminarse y por qué?

R: Estamos completamente de acuerdo que en esta convención se disponga de un enunciado de Propósitos, uso de términos, ámbito de aplicación y protección de la soberanía de los estados.

4. ¿Debería la declaración de propósitos contener más de tres ideas principales (siendo estas, en términos generales, medidas para prevenir y combatir [el uso de las TIC con fines delictivos] [ciberdelincuencia], la cooperación internacional relacionada y la asistencia técnica relacionada)? ¿Qué otros elementos estarían interesados en incluir los Estados miembros en la declaración de objetivos? ¿Sobre cuál de estos elementos adicionales podrían los Estados miembros llegar a un consenso?

R: Consideramos que los estados podríamos llegar a un consenso en todos los objetivos planteados y estamos de acuerdo con la inclusión de las tres ideas principales en los propósitos.

5. ¿Es necesaria una referencia a la protección de los derechos humanos en la declaración de propósitos, si en el convenio se incluye un artículo exclusivamente sobre esta materia, como proponen algunos Estados miembros?

R:Consideramos que en la presente convención no es necesario profundizar en los derechos humanos, existe una convención particular al respecto donde todos los estados, somos respetuosos de la misma.

6. ¿Deben limitarse las cláusulas/artículos sobre prueba electrónica a los delitos previstos en la convención? ¿Debería el ámbito de aplicación del convenio tener en cuenta el ámbito de aplicación definido para las medidas procesales y/o para la cooperación internacional?

R: Consideramos que no deben limitarse las clausulas sobre las pruebas electrónicas, a los delitos que se han establecido en la presente convención debido a la evolución acelerada de las TIC's

7. ¿Debería incluirse en el ámbito de aplicación una cláusula sobre embargo preventivo, incautación, decomiso y devolución del producto de los delitos tipificados por el convenio, como proponen algunos Estados miembros?

R: Completamente de acuerdo

8. ¿Cubriría el lenguaje de los artículos 4 de la UNTOC y la UNCAC todas las preocupaciones de los Estados miembros con respecto a la protección de la

soberanía? ¿Las consideraciones de soberanía son diferentes en el contexto del uso de las TIC que en otros contextos tradicionales?

R: Las consideraciones de soberanía en el uso de la TIC´s no deberían ser diferente a lo ya establecido en convenciones anteriores de la ONU.

9. Entre la larga lista de términos propuestos para incluir como definiciones en el marco de la convención, ¿podría proponer una lista clave de términos que el Comité Ad Hoc debe considerar como una prioridad (en el entendimiento de que sería necesario hacer una lista final después de una revisión de las disposiciones finalmente acordadas, especialmente sobre tipos delictivos, medidas procesales y cooperación internacional)?

R: Si pudiésemos proponer una lista de definiciones

Términos Propuestos:

Acceso a sistemas de información: Es la entrada a dicho sistemas, incluyendo los accesos remotos.

Acceso a la información contenida en un dispositivo que permita el almacenamiento de datos: Es la lectura, copia, extracción, modificación o eliminación de la información contenida en dicho dispositivo.

Ataque informático significará la interferencia dirigida de software y/o hardware y software con sistemas de información o redes de información y telecomunicaciones para interrumpir y/o terminar su funcionamiento y/o amenazar la seguridad de la información procesada por dichas instalaciones;

Bienes; significará activos de todo tipo, ya sean corporales o incorporales, muebles o inmuebles, tangibles o intangibles, incluido el dinero en cuentas bancarias, activos financieros digitales, moneda digital, incluidas las criptomonedas, y documentos o instrumentos legales que acrediten el título de tales activos o cualquier parte de los mismos;

Botnet: dos o más dispositivos TIC en los que se ha instalado software malicioso y que se controlan de forma centralizada sin el conocimiento de los usuarios;

Copia de datos: Es la reproducción total o parcial de la información digital.

Ciberdelitos: Acciones u omisiones, típicas, antijurídicas, continuas o aisladas, de

carácter penal, cometidas en contra de personas naturales y/o jurídicas, utilizando como método, como medio o como fin, los datos, sistemas informáticos, Tecnologías de la Información y la Comunicación y que tienen por objeto lesionar bienes jurídicos personales, patrimoniales o informáticos de la víctima.

Daño sustancial se determinará de conformidad con la legislación interna del Estado Parte requerido.

Datos informáticos: Es cualquier representación de hechos, información o conceptos en un formato digital o analógico, que puedan ser generados, almacenados, procesados o transmitidos a través de las Tecnologías de la Información y la Comunicación.

Datos relativos al tráfico: Todos los datos relativos a una comunicación realizada a través de cualquier medio tecnológico, generados por este último, que indiquen el origen, el destino, la ruta, la hora, la fecha y el tipo de servicio o protocolo utilizado, tamaño y la duración de la comunicación.

Datos personales: Es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar.

Datos personales sensibles: Es toda información privada que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación.

Decomiso significará la privación forzosa de bienes sin compensación de conformidad con una orden de un tribunal u otra autoridad competente;

Dispositivo: Es cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede ser utilizado para ejecutar cualquier función de la Tecnología de la Información y la Comunicación.

Dispositivos de almacenamiento de datos informáticos: Es cualquier medio a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo.

Embargo de bienes significará la prohibición temporal de la transferencia, conversión, disposición o movimiento de bienes, o la asunción temporal de la

custodia o control de bienes de conformidad con una orden de un tribunal u otra autoridad competente;

Entrega de datos y archivos informáticos: Se entiende la transferencia de informaciones, documentos o datos en formato electrónico que obren en poder de particulares, entidades públicas o privadas.

Evidencia electrónica significará cualquier información probatoria almacenada o transmitida en forma digital (en un medio electrónico).

Identidad informática: Información, datos o cualquier otra característica que individualice, identifique o distinga una persona de otra o a un usuario de otro usuario, dentro de un sistema informático.

Incautación y depósito de sistemas informáticos o dispositivos de almacenamiento de datos: Se entiende su ocupación física y su aseguramiento por las autoridades competentes.

Información; significará cualquier dato (mensajes, registros), independientemente de la forma en que se presente;

Información digital significa cualquier dato (registros), independientemente de su forma y características, contenido y procesado en dispositivos, sistemas y redes de información y telecomunicaciones;

Infraestructura de información crítica significará un conjunto de instalaciones de infraestructura de información crítica y redes de telecomunicaciones utilizadas para interconectar instalaciones de infraestructura de información crítica;

Instalaciones de infraestructuras críticas: los sistemas de información y las redes de información y comunicaciones de las autoridades públicas y los sistemas de información y los sistemas de control de procesos automatizados que operan en los sectores de defensa, sanidad, educación, transporte, comunicaciones, energía, banca y finanzas, nuclear y otras áreas importantes de la vida del Estado y la sociedad;

Interceptar: Acción de apropiarse o interrumpir datos informáticos contenidos o transmitidos por medio de las Tecnologías de la Información y la Comunicación antes de llegar a su destino.

Interferir: Obstaculizar, perturbar u obstruir por medio de las Tecnologías de la Información y la Comunicación los sistemas informáticos, públicos o privados.

Intervención de comunicaciones a través de las Tecnologías de la Información y la Comunicación: Se entiende la captación, escucha o grabación en tiempo real del contenido de dichas comunicaciones sin interrupción de las mismas, así como de los datos de tráfico.

Pornografía infantil: Comprende cualquier representación de la imagen o voz de un niño, niña o adolescente, realizando actividades sexuales o eróticas, implícitas o explícitas, reales o simuladas, así como la exposición de sus partes genitales, con fines sexuales, por cualquier medio sea directo, mecánico, digital, audio visual, o con soporte informático, electrónico o de otro tipo.

Persona con discapacidad necesitada de especial protección: Aquella persona con discapacidad que tenga o no judicialmente modificada su capacidad de obrar, requiera de asistencia o apoyo para el ejercicio de su capacidad jurídica y para la toma de decisiones respecto de su persona, de sus derechos o intereses a causa de sus limitaciones intelectuales o mentales de carácter transitoria o permanente.

Pornografía infantil tendrá el significado que se le da a ese término en el artículo 2 (c) del Protocolo Facultativo de 25 de mayo de 2000 de la Convención sobre los Derechos del Niño, relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía;

Producto se entenderá cualquier bien derivado u obtenido, directa o indirectamente, mediante la comisión de cualquier delito u otro acto ilegal contemplado en el presente Convenio, así como los ingresos u otros beneficios derivados de dicho producto, de bienes en los que dicho producto se haya transformado o convertido o de bienes con los que dicho producto se haya mezclado;

Proveedor de servicios: Es la persona natural o jurídica, pública o privada, que suministre a los usuarios servicios de comunicación, seguridad informática, procesamiento o almacenamiento de datos, a través de las Tecnologías de la Información y la Comunicación.

Programa informático: Es la herramienta o instrumento elaborado en lenguaje informático que ejecuta una secuencia de procesos en un sistema informático.

Redes de información y telecomunicaciones" significará un conjunto de equipos de ingeniería diseñados para controlar procesos tecnológicos por medio de tecnología informática y telecomunicaciones;

Requerimiento de preservación inmediata de datos que se hallan en poder de terceros: Se entiende la imposición a Personas Naturales o Jurídicas del deber de conservación íntegra de la información digital que obre en su poder o sobre la que tenga facultades de disposición.

Sellado, precinto y prohibición de uso de sistemas informáticos o dispositivos de almacenamiento de datos: Se entiende su bloqueo o la imposibilidad de su utilización conservando la integridad de su contenido.

Sistema informático: Todo dispositivo aislado, conectado o relacionado a otros dispositivos mediante enlaces de comunicación o la tecnología que en futuro la reemplace, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa informático.

Software malicioso se refiere al software cuyo propósito es la modificación, destrucción, copia y bloqueo no autorizados de información, o la neutralización del software utilizado para proteger la información digital;

Tarjeta inteligente: Cualquier dispositivo electrónico que permite la ejecución de cierta lógica programada para el almacenamiento de información y/o datos, que se utiliza como instrumento de identificación o de acceso a un sistema, para realizar gestiones electrónicas al titular autorizado.

Tecnologías de la Información y la Comunicación: Conjunto de medios de comunicación y las aplicaciones de información que permiten la captura, producción, reproducción, transmisión, almacenamiento, procesamiento, tratamiento, y presentación de información, en forma de imágenes, voz, textos, códigos o datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros, por medio de protocolos de comunicación, transmisión y recepción.

10. ¿Piensa que la AHC tiene que definir primero estos términos, o que las definiciones solo deben abordarse después de que se negocien los artículos sustantivos de la convención? ¿Cuál sería la mejor etapa en el proceso de negociación para discutir definiciones de manera enfocada?

R: Negociar los artículos sustantivos de la convención para después negociar las definiciones y términos que serán de uso común entre los estados

11. ¿Desean los Estados miembros considerar, en esta etapa, las diferencias entre "sistemas informáticos" y "dispositivos de TIC" y su impacto en el ámbito de aplicación del convenio?

R: Un Sistema Informático es un sistema que permite almacenar y procesar información en su conjunto.

Dispositivos de la TIC's son las tecnologías que utiliza la informática, la microelectrónica y las telecomunicaciones para crear nuevas formas de comunicación con el fin de facilitar la emisión, acceso y tratamiento de la información

Ambas terminologías son sinónimos utilizados en dependencia del contexto.

12. ¿Cómo debería la convención considerar la perspectiva de género en todas sus disposiciones?

R: Consideramos que no es necesario en esta convención abordar el tema de perspectiva de género, esto ya existe en otras convenciones de la ONU.

APORTES DE NICARAGUA EN EL SEGUNDO PERIODO DE SESIONES DEL COMITÉ AD HOC ENCARGADO DE ELABORAR UNA CONVENCIÓN INTERNACIONAL AMPLIA CONTRA LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES CON FINES DELICTIVOS.

III. DISPOSICIONES SOBRE LAS MEDIDAS PROCESALES Y LA APLICACIÓN DE LA LEY

PRIMER GRUPO

TEMAS: A. Jurisdicción; B. Alcance de las medidas procesales; C. Condiciones y garantías. D. Procedimientos Penales. (Véase A/AC.291/CRP11).

1. ¿En qué capítulo debe abordarse la "jurisdicción" (a este respecto, los Estados miembros han hecho propuestas en los tres capítulos: penalización, disposiciones generales y medidas procesales y aplicación de la ley)?

R: El tema de la Jurisdicción debe abordarse en el capítulo de las Disposiciones General, sin menos cabo de señalar ámbitos jurisdiccionales en el capítulo de aplicación de la ley.

2. ¿Debería la base para establecer la jurisdicción incluir que un Estado parte sea el objeto/objetivo de un crimen (lo cual estaba incluido en la UNCAC pero no en la UNTOC)?

R: Lo principal es el cumplimiento al derecho internacional, si un estado es objeto o no de un Cibercrimen directa o indirectamente, debe tomarse en cuenta la jurisdicción para la penalización del o los autores.

3. ¿Debería el artículo sobre jurisdicción cubrir también asuntos relacionados con la extradición, es decir, jurisdicción cuando la extradición no es posible (aut dedere aut judicare)?

R: Completamente de acuerdo, la jurisdicción debe regirse por el derecho internacional y la constitución y la legislación local de cada estado.

4. ¿Cuál es el alcance del capítulo sobre medidas procesales y ejecución de la ley? ¿Debería aplicarse solo a la lista de delitos establecidos por la convención (en su capítulo sobre tipificación)? ¿Podría aplicarse también a otros delitos? ¿Por qué sería necesaria tal ampliación a otros delitos?

R: Debería agregarse "otros delitos donde se utilicen las tecnologías de la información y las telecomunicaciones."

5. ¿A qué condiciones y garantías deben estar sujetas las medidas procesales?

R: Las condiciones y garantías deben estar sujetas al Derecho Internacional, Constitución y Marco Jurídico y Normativo de los Estados.

6. ¿Debería hacerse referencia a tratados de derechos humanos internacionales o regionales específicos en este capítulo, en particular en una disposición sobre condiciones y garantías? De ser así, ¿cuáles son los tratados de derechos humanos específicos a los que se debe hacer referencia (tratados regionales versus globales)? ¿Debería haber también una referencia a los principios legales universales (por ejemplo, necesidad, proporcionalidad), y cuáles podrían acordarse?

R: Somos del criterio que los derechos humanos están ampliamente relacionados en convenciones anteriores y no sería necesario mencionarlas en la presente convención, la cual es más técnica.

SEGUNDO GRUPO

E. Recopilación de información/contenido y metadatos transmitidos mediante tecnologías de la información y las comunicaciones; F. Preservación acelerada de datos informáticos almacenados; G. Preservación acelerada de información electrónica acumulada; H. Preservación acelerada y divulgación parcial de datos de tráfico; I. Orden de producción; J. Búsqueda e incautación de información almacenada o procesada electrónicamente o datos informáticos almacenados; K. Recopilación en tiempo real de datos de tráfico; L. Interceptación de datos de contenido; M. Conservación de datos. (Véase A/AC.291/CRP11).

1. ¿Qué facultades y procedimientos debería prever la convención a los efectos de detectar, desbaratar, investigar, enjuiciar y juzgar los delitos en cuestión?

R: Las facultades y procedimientos deben estar determinadas por lo que confiere el derecho internacional y lo que se contemple en la presente convención, la investigación y enjuiciamiento es facultad de cada estado de acuerdo con su marco legislativo.

2. ¿Existen condiciones y garantías específicas que deban aplicarse a determinadas medidas procesales?

R: Las condiciones y garantías procesales deben estar determinadas por el derecho internacional y la legislación de cada estado.

3. ¿Deberían aplicarse ciertas medidas procesales a ciertos tipos de datos?

R: Sí, códigos maliciosos utilizados para violentar esquemas de seguridad de las tecnologías de la información y las comunicaciones.

4. ¿Qué plazos se deben aplicar a la conservación de los datos pendientes de solicitud de las autoridades competentes para su divulgación?

R: Los ISP, deben almacenar no menos de seis meses los datos, por su posible uso ante hechos vinculados a Ciberdelitos o incidentes que afecten las tecnologías de la información y las comunicaciones.

5. ¿Desean los Estados miembros debatir las diferencias de nomenclatura entre la información electrónica y los datos informáticos? acumulado versus almacenado (datos o información) en esta etapa de las negociaciones?

R: Son sinónimos y van a estar en dependencia del contexto y temática que se aborde

6. Los Estados miembros tal vez deseen considerar si la definición de información del suscriptor, bajo una disposición sobre "orden de producción" sería (1) requerida; y (2) mejor mantenida dentro de esta disposición, o bajo las disposiciones generales de la convención sobre el uso de términos.

R: Consideramos que mejor debe estar en las disposiciones generales, uso de términos.

7. ¿Debe indicarse la sospecha de delitos relacionados con las TIC o la comisión de delitos penales como motivo para el registro y la incautación, o para la interceptación de datos de contenido?

R: Si, para ambos casos.

8. ¿Los Estados miembros ven la necesidad de permitir declaraciones o reservas con respecto a las disposiciones sobre medidas procesales, para permitir una ratificación más amplia de esta convención?

R: Consideramos que no debería ser necesario porque las condiciones de las medidas procesales van estar determinadas por el derecho internacional y el marco jurídico de las estados.

Gobierno de Reconciliación y Unidad Nacional
Unida Nicaragua Triunfa

TERCER GRUPO

O. Freezing, seizure and confiscation; P. Disposal of confiscated proceeds of crime or property; S. Protection of witnesses; T. Assistance and protection of victims. (See A/AC.291/CRP11).

1. ¿Qué nivel de detalle debe haber en las disposiciones sobre congelamiento, incautación y decomiso, así como la disposición de los productos del delito o bienes decomisados?

R: Consideramos que en esta convención no se debe entrar en muchos detalles de las disposiciones, ya que las mismas deben ser regidas por el marco legal de cada estado.

2. ¿Debería contener la convención una disposición sobre la protección de los testigos? En caso afirmativo, ¿qué factores de protección son importantes para incluir en dicha disposición y qué nivel de detalle, en términos de definiciones y descripción de los procedimientos relacionados, se debe esperar? ¿Le gustaría al comité seguir la formulación de la UNTOC (artículo 24)?

R: La protección a testigos debe estar regulada por el derecho internacional y la legislación de cada estado, consideramos no se puede profundizar en esta convención en ese tema en específico.

3. ¿Debería contener la convención una disposición sobre la asistencia y protección de las víctimas? En caso afirmativo, ¿qué factores de protección son importantes para incluir en dicha disposición y qué nivel de detalle, en términos de definiciones y descripción de los procedimientos relacionados, se debe esperar?

R: Igual que la anterior.

4. ¿Qué papel deben tener las víctimas y los denunciantes? ¿Le gustaría al comité seguir la formulación de la UNTOC (artículo 25)?

R: El papel de las víctimas y denunciantes, debe estar regido por el derecho internacional y el marco legal y normativo de cada estado.

Gobierno de Reconciliación y Unidad Nacional
Unida Nicaragua Triunfa

CUARTO GRUPO

N. Admisión de evidencia digital; Q. Técnicas especiales de investigación; R. Establecimiento de antecedentes penales; U. Medidas para mejorar la cooperación con las autoridades encargadas de hacer cumplir la ley. (Véase A/AC.291/CRP11).

1. ¿Debe la convención establecer estándares para la recopilación y admisibilidad de evidencia digital en general? ¿Cuáles serían las ventajas y desventajas de este enfoque?

R: Consideramos que se podría establecer en esta convención los estándares, sus ventajas serían la uniformidad de procedimientos para la recopilación y admisibilidad de la evidencia digital, la desventaja que estos procedimientos podrían no ajustarse al marco legal y normativo de algunos estados.

2. ¿Debería contener la convención una disposición sobre técnicas especiales de investigación? En caso afirmativo, ¿cuáles deben mencionarse y qué nivel de detalle, en términos de definiciones y descripción de los procedimientos relacionados, debe esperarse? ¿Le gustaría al comité seguir la formulación de la UNTOC (artículo 20)?

R: Consideramos que la convención no debería contemplar este aspecto; la investigación va a estar determinada por los diferentes protocolos de actuación de cada uno de los estados ante los Ciberdelitos o hechos que afecten las tecnologías de la información y las telecomunicaciones.

3. ¿Debe la convención contener una disposición sobre el establecimiento de antecedentes penales siguiendo la formulación de la UNTOC (artículo 22)?

R: No necesariamente, existen organismos como la INTERPOL que se encargan de este tema.

4. ¿Debería contener la convención una disposición sobre medidas para mejorar la cooperación con las autoridades encargadas de hacer cumplir la ley siguiendo la formulación de la UNTOC (artículo 26)?

R: La convención podría proponer un acápite sobre la cooperación entre los estados y las autoridades e instituciones de aplicación de la ley.