Propuesta sobre definiciones, criminalización, medidas procesales y aplicación de la ley para la Negociación de la Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos - COLOMBIA

1. DISPOSICIONES GENERALES

Los Estados Parte deben, al prevenir y combatir el delito cibernético en todos sus aspectos, promover y garantizar el pleno respeto de los derechos de las mujeres y las niñas, y a su vez prestar especial atención a las cuestiones género, en particular a la violencia de género, incluyendo la violencia contra las mujeres y las niñas.

Los Estados Parte deben, al prevenir y combatir el delito cibernético en todas sus expresiones, promover y garantizar el respeto de los derechos humanos y libertades fundamentales. Todas las disposiciones de este Convenio/Instrumento se entenderán y aplicarán de manera concordante con las respectivas obligaciones internacionales en materia de derechos humanos.

2. Definiciones

Conforme al consenso establecido en la primera ronda de negociación respecto a la necesidad de acordar terminología y definiciones tecnológicamente neutras, aunado a lo expresado por el equipo del Consejo Europeo para el Convenio de Budapest[1], las definiciones contempladas tanto en el Convenio de Budapest como en su Segundo Protocolo resultan pertinentes, suficientes y adaptables a la evolución tecnológica, para ser propuestas ante el Comité Ad Hoc de la negociación.

Así, las definiciones a proponer son:

1) Sistema informático: *"…todo dispositivo aislado o conjunto de dispositivos interconectados…cuya función…sea el tratamiento automatizado de datos en ejecución de un programa*"[2].

2) Datos informáticos: *"…toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función"*[3].

3) Proveedor de servicios: *"…toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo*"[4].

4) Datos relativos al tráfico: *"…todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la*

[1] *"Briefing note for members of the T-CY*" del 25 de marzo de 2022.
[2] Artículo 1°, literal a, Convenio de Budapest sobre la Ciberdelincuencia.
[3] Artículo 1°, literal b, ibídem.
[4] Artículo 1°, literal c, ibídem.

cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente"[5].

5) Autoridad central: "*la autoridad o autoridades designadas en virtud de un tratado o acuerdo de asistencia mutua basado en la legislación uniforme o recíproca en vigor entre las Partes de que se trate, o en su defecto, la autoridad o autoridades designadas por una Parte[6]…encargadas de enviar las solicitudes de asistencia mutua o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución*"[7].

6) Autoridad competente: *"una autoridad judicial y administrativa o policial facultada por el Derecho interno, para ordenar, autorizar o llevar a cabo la ejecución de medidas…a efectos de la obtención o la presentación de pruebas en relación con investigaciones o procesos penales específicos*"[8].

7) Emergencia: "*situación en la que existe un riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas*"[9].

8) Datos personales[10]: *"la información relativa a una persona física identificada e identificable*"[11].

9) Parte transmitente: "*la Parte que transmite los datos en respuesta a una solicitud o en un equipo conjunto de investigación, o…la Parte en cuyo territorio se encuentre un proveedor de servicios transmitente o una entidad que preste servicios de registro de nombres de dominio*"[12]

10) Datos de los abonados: *"…cualquier información…que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes a los datos relativos al tráfico o al contenido, y que permitan determinar…el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio… la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado….los datos relativos a la facturación y al pago…cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación…*"[13].

3. <u>Criminalización</u>

Es pertinente proponer en el acápite de criminalización, lo siguiente:

En cuanto a los *cyber dependent crime*, cada Estado miembro debería adoptar las medidas legislativas y de otra índole necesarias para tipificar como delito, en su ordenamiento jurídico interno, las siguientes conductas:

a) Acceso ilícito: Acceder ilegítimamente a todo o parte de un sistema informático[14].

---

[5] Artículo 1°, literal d, ibídem.
[6] Artículo 3°, numeral 2, literal a, del Protocolo Adicional Segundo al Convenio Budapest sobre Ciberdelincuencia.
[7] Artículo 27, numeral 2, literal a, Convenio de Budapest sobre la Ciberdelincuencia.
[8] Artículo 3°, numeral 2, literal b, del Protocolo Adicional Segundo al Convenio Budapest sobre Ciberdelincuencia.
[9] Artículo 3°, numeral 2, literal c, ibídem.
[10] En el caso de la definición de datos personales, podríamos también proponer la definición de nuestra Ley 1581 de 2012 (con la respectiva adaptación de lenguaje a que haya lugar), la cual es del siguiente tenor: "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables".
[11] Artículo 3°, numeral 2, literal d, del Protocolo Adicional Segundo al Convenio Budapest sobre Ciberdelincuencia.
[12] Artículo 3°, numeral 2, literal e, del Protocolo Adicional Segundo al Convenio Budapest sobre Ciberdelincuencia.
[13] Artículo 18, Convenio de Budapest sobre la Ciberdelincuencia.
[14] Artículo 2, Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 269A de la Ley 1273 de 2009.

b) Interceptación ilícita: Interceptar ilegítimamente datos informáticos, tanto en su origen, destino o en el interior de un sistema informático, o en las emisiones electromagnéticas provenientes de un sistema informático que los transporta[15].

c) Ataques a la integridad de los datos: Dañar, destruir, borrar, deteriorar, alterar o suprimir datos informáticos o un sistema de tratamiento de información o sus partes o componentes lógicos[16].

d) Ataques a la integridad del sistema: Obstaculizar ilegítimamente el funcionamiento o el acceso normal a un sistema informático, a los datos allí contenidos, o a una red de telecomunicaciones[17].

e) Abuso de los dispositivos: Producir, obtener, poseer, comerciar o difundir un dispositivo, incluido un programa informático, así como una contraseña, código de acceso, o datos informáticos similares, que permitan acceder a todo o en parte de un sistema informático, para la comisión de los delitos señalados en los literales a, b, c y d, del presente acápite[18].

f) Falsificación informática: Introducir, alterar, borrar o suprimir deliberada e ilegítimamente datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos[19].

En cuanto a los *cyber enabled crime*, cada Estado miembro debería adoptar las medidas legislativas y de otra índole necesarias para tipificar como delito, en su ordenamiento jurídico interno, las siguientes conductas:

a) Delitos relacionados con material de abuso sexual infantil: Producir, ofertar, difundir, transmitir, adquirir o poseer, a través de un sistema informático, material de abuso sexual infantil[20].

b) Fraude informático: Introducir, alterar, borrar, suprimir datos informáticos, o interferir en el funcionamiento de un sistema informático, con la intención dolosa o culposa de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona, en perjuicio del patrimonio de otra persona[21].

c) Violación de datos personales: Obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear, sin estar facultado para ello, con provecho propio o de un tercero, datos personales, contenidos en ficheros, archivos, bases de datos o medios semejantes[22].

---

[15] Artículo 3, Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 269C de la Ley 1273 de 2009.
[16] Artículo 4, Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 269D de la Ley 1273 de 2009.
[17] Artículo 5, Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 269B de la Ley 1273 de 2009.
[18] Artículo 6, Convenio de Budapest sobre la Ciberdelincuencia.
[19] Artículo 7, ibídem.
[20] Artículo 9, ibídem.
[21] Artículo 8, ibídem.
[22] Artículo 269F, Ley 1773 de 2009.

personas naturales y de sanciones pecuniarias en el caso de las personas jurídicas[23].

4. Medidas procesales y aplicación de la ley

Teniendo en cuenta las disposiciones consensuadas y de carácter vinculante para Colombia, sobre poderes y procedimientos, contempladas en la UNTOC, la UNCAC y el Convenio de Budapest sobre la Ciberdelincuencia, es pertinente proponer, en lo relativo a medidas procesales y aplicación de la Ley, lo siguiente:

Medidas	Disposición del instrumento internacional precedente
Poderes y procedimientos.	Artículo 14 del Convenio de Budapest.
Condiciones y salvaguardas.	Artículo 15 del Convenio de Budapest.
Conservación rápida de datos informáticos almacenados	Artículo 16 del Convenio de Budapest.
Conservación y revelación parcial rápidas de los datos relativos al tráfico.	Artículo 17 del Convenio de Budapest.
Orden de presentación.	Artículo 18 del Convenio de Budapest.
Registro y confiscación de datos informáticos almacenados.	Artículo 19 del Convenio de Budapest.
Obtención en tiempo real de datos relativos al tráfico.	Artículo 20 del Convenio de Budapest.
Interceptación de datos relativos al contenido.	Artículo 21 del Convenio de Budapest.
Jurisdicción.	Artículos 22 del Convenio de Budapest, 15 de la UNTOC y 42 de la UNCAC.
Embargo preventivo, incautación y decomiso	Artículo 31 de la UNCAC.

[23] Artículo 13 del Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 30 de UNCAC y el artículo 11 de UNTOC.