RECOMENDACIÓN DE LA CONFERENCIA DE MINISTROS DE JUSTICIA DE LOS PAÍSES IBEROAMERICANOS (COMJIB) RELATIVA A LA TIPIFICACIÓN Y SANCIÓN DE LA CIBERDELINCUENCIA

Los Ministros de Justicia y representantes de los Estados Iberoamericanos reunidos en Madrid el 28 de mayo del 2014;

VISTO el artículo 3º, apartado c), del Tratado constitutivo de la Conferencia de Ministros de Justicia de los Países Iberoamericanos del 7 de octubre de 1992;

RECORDANDO los valiosos intercambios técnicos y político criminales llevados a cabo en el marco del Seminario Iberoamericano sobre Cibercrimen desarrollado los días 6 y 7 de septiembre de 2011 en la ciudad de Buenos Aires; en la reunión del Grupo de trabajo sobre "Delincuencia Organizada Trasnacional y Cooperación Jurídica Internacional" del 8 y 9 de septiembre de 2011 en la misma ciudad; en los talleres convocados en Montevideo del día 17 al 19 de septiembre de 2012, y en Madrid del 4 al 6 de febrero de 2013; en la reunión de coordinadores llevada a cabo en Bogotá El 4 y 5 de Marzo de 2013, y en el taller desarrollado en Lima los días 24, 25 y 26 de junio de 2013;

TENIENDO PRESENTE que en la Comisión Delegada de la COMJIB celebrada en Río de Janeiro el día 23 de marzo de 2012 se aprobó una importante "Declaración sobre el ciberdelito" en la que se acordó: "respaldar los primeros pasos que se han dado en la línea de lucha contra la delincuencia organizada para iniciar el debate sobre la elaboración y firma de un documento internacional iberoamericano, capaz de dar respuesta a las necesidades arriba referidas, e impulsar la modificación de las legislaciones penales de manera armonizada". Razón por la cual se dictaron unas líneas generales "con la finalidad de concretar un borrador de Convenio Iberoamericano para regular el Ciberdelito";

ATENDIENDO a que en la Plenaria llevada a cabo en Viña del Mar se acordó, sobre el borrador aportado, elaborar un Convenio Iberoamericano sobre cooperación, prueba, jurisdicción y competencia en materia de ciberdelincuencia, así como una Recomendación que albergaría los principios relativos a los aspectos sustantivos que deberían encontrar acomodo en las legislaciones nacionales;

SIGNIFICANDO que en Viña del Mar se acordó, también, convocar un taller para terminar "de definir el contenido final" de los dos documentos acabados de referir, con el objetivo de elevar, para su firma, los dichos textos a la Cumbre Iberoamericana de Jefes de Estado y de Gobierno celebrada en Panamá en octubre del 2013, lo que no ha sido posible;

CONSIDERANDO, que buena parte de las legislaciones penales iberoamericanas tienen importantes carencias en los tipos penales referidos al ciberdelito, y que estas lagunas permiten tanto a la delincuencia individual como a la organizada lesionar o poner en

grave peligro a bienes jurídicos esenciales;

CONSCIENTES de que en otras regiones del mundo se han ido aprobando, o se está en trámite de hacerlo, Convenciones sobre ciberdelincuencia para una mejor protección de sus ciudadanos, lo que todavía no se ha efectuado en el ámbito iberoamericano;

MANTENIENDO el propósito de establecer criterios mínimos y comunes en la prevención y lucha contra el ciberdelito, y sin menoscabar los avances alcanzados en los respectivos ordenamientos jurídicos así como de las obligaciones internacionalmente asumidas por cada Estado;

CONVENCIDOS de que todos los esfuerzos para la prevención y lucha contra el cibercrimen son necesarios;

ENTENDIENDO que la presente Recomendación debe estar abierta a futuros desarrollos y ampliaciones a nuevos delitos y mecanismos de cooperación;

MANIFESTANDO la voluntad de que la presente Recomendación resulte compatible con otros análogos, así como con reconocidas buenas prácticas en el ámbito internacional;

ENTENDIENDO CONVENIENTE, incorporar o, en su caso, armonizar, en el marco de las políticas criminales que cada país adopte en la materia, las legislaciones penales sustantivas nacionales en la tipificación de las conductas que más adelante se identificarán, a los efectos de buscar mayor eficacia en la prevención, persecución y, eventualmente, sanción de los dichos comportamientos, así como para facilitar la cooperación judicial entre los distintos países y tratar de impedir la existencia de espacios de impunidad;

RECOMIENDAN, en relación a las siguientes conductas:

I. Acceso no autorizado a sistemas.

Tipificar como infracción penal el acceso no autorizado a un sistema informático siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo.

Considerar infracción penal el acceso a un sistema informático más allá de lo autorizado.

Podrá considerarse infracción penal agravada si los sistemas a los que se accede se refieren a estructuras o servicios esenciales para la comunidad.

II. Daños informáticos o atentados contra la integridad de los datos.

Tipificar como infracción penal cualquier acto consistente en introducir, borrar,

deteriorar, alterar, suprimir o hacer inaccesibles de forma grave datos informáticos, realizado a través de las tecnologías de la información y de la comunicación.

Podrá considerarse infracción penal agravada si los atentados afectan a datos informáticos referidos a estructuras o servicios esenciales para la comunidad o si causan un grave daño económico.

III. Daños o Atentados contra la integridad o disponibilidad de los sistemas informáticos.

Tipificar como infracción penal la conducta realizada a través de las tecnologías de la información y de la comunicación consistente en la inutilización, total o parcial, de un sistema informático cuando impidiese el acceso al mismo o imposibilitase el desarrollo de alguno de sus servicios.

Podrá considerarse infracción penal agravada si los sistemas se refieren a estructuras o servicios esenciales para la comunidad o si se causa un grave daño económico.

IV. Abuso de dispositivos

Tipificar como infracción penal la fabricación, importación, venta, facilitación, obtención para su utilización, de dispositivos, incluidos los programas informáticos, así como contraseñas o códigos de acceso, específicamente destinados a la comisión del delito de acceso no autorizado a sistemas o del delito de daños a datos informáticos y daños a sistemas de información.

V. Conductas vinculadas a la pornografía infantil.

Tipificar como infracción penal:

a) La producción de pornografía infantil.

b) La oferta o puesta a disposición de pornografía infantil.

c) La difusión o transmisión de pornografía infantil.

d) La adquisición para sí o para otro de pornografía infantil.

e) La posesión de pornografía infantil.

f) El acceso intencional a pornografía infantil por medio de las tecnologías de la información.

VI. Proposiciones a menores con fines sexuales por medios tecnológicos.

Tipificar como infracción penal la conducta realizada, a través de las tecnologías de la información y la comunicación, consistente en contactar con un menor que no haya

alcanzado la edad del consentimiento sexual para solicitar u obtener de él material pornográfico.

También será considerada infracción penal la conducta realizada a través de las tecnologías de la comunicación y la información consistente en contactar con un menor que no haya alcanzado la edad del consentimiento sexual para llevar a cabo actividades sexuales con él, cuando dicha proposición se haya concretado en actos materiales conducentes a dicho encuentro.

VII. Conductas relativas a la afectación de los derechos de propiedad intelectual

Tipificar como infracción penal la conducta realizada por medio de las Tecnologías de la Información y la Comunicación consistente en explotar ilícitamente o plagiar en todo o en parte, una obra literaria, artística o científica o la transformación, interpretación o ejecución artística de la misma, con ánimo de lucro y en perjuicio de tercero.

VIII. Difusión de mensajes con contenidos xenófobos, racistas o relativos a los crímenes contra la humanidad.

Tipificar como infracciones penales las siguientes conductas realizadas a través de las Tecnologías de la Información y Comunicación:

a) La incitación pública a la violencia o al odio mediante la difusión de escritos, imágenes u otros materiales, dirigidos contra un grupo de personas o un miembro de tal grupo, definido en relación con la raza, el color, la religión, el sexo, la orientación sexual, la identidad de género, la enfermedad o discapacidad, la ascendencia o el origen nacional o étnico.

b) La expresión o difusión de informaciones injuriosas referidas a grupos de personas, o miembros de las mismas, en relación con la raza, el color, la religión, el género, la orientación sexual, la enfermedad o discapacidad, la ascendencia o el origen nacional o étnico.

Podrá considerarse infracción penal agravada la apología pública, la negación o la trivialización flagrante de los crímenes de genocidio, crímenes de lesa humanidad y crímenes de guerra.

IX. Suplantación de identidad

Tipificar como infracción penal la conducta realizada por medio de las Tecnologías de la Información y la Comunicación y con ánimo defraudatorio consistente en suplantar

la identidad de una persona física o jurídica.

X. Estafa informática

Tipificar como infracción penal la conducta consistente en manipular el ingreso, procesamiento o resultado de los datos de un sistema de información, por medio de las Tecnologías de la Información y la Comunicación, y valiéndose de alguna operación informática, en perjuicio de tercero y con ánimo de lucro.

Podrá considerarse infracción penal agravada cualquiera de las siguientes conductas:

a) Cuando se cometa contra estructuras o servicios esenciales para la comunidad o si se causa un grave daño económico.

b) Cuando el autor, por sus funciones asignadas o por ser encargado de administrar o dar soporte al sistema o red informática o telemática, tenga posibilidad de tener acceso a los mismos.