SECCIÓN I – DERECHO PENAL PARTE GENERAL

Los participantes en el XIX Congreso Internacional de Derecho Penal, celebrado en Río de Janeiro del 31 de agosto al 6 de septiembre de 2014;

Considerando que en el siglo XXI la vida de las personas está fuertemente influenciada y determinada por las tecnologías de la información y la comunicación (TIC), así como por las oportunidades y riesgos que ofrecen la sociedad de la información y el ciberespacio y que, por lo tanto, los delitos en estos ámbitos afectan a importantes bienes jurídicos personales y colectivos;

Con base en el proyecto de resoluciones preparado por los intervinientes en el Coloquio Preparatorio celebrado en Verona del 28 al 30 de noviembre de 2012;

Reconociendo que los Estados y las organizaciones internacionales han hecho considerables esfuerzos para definir y perseguir los delitos que puedan afectar a la confidencialidad, integridad y disponibilidad de las redes TIC y el ciberespacio, así como a los intereses de las personas en estos ámbitos;

Teniendo en cuenta los riesgos asociados a una ampliación excesiva de la represión criminal en estos ámbitos, especialmente para la libertad de expresión y la recepción, recopilación, procesamiento y difusión de la información;

Definidas las redes TIC como aquellos sistemas que hacen posible la adquisición, procesamiento, almacenamiento y difusión de información sonora, visual, textual y numérica a través de redes informáticas y de telecomunicaciones y el ciberespacio como un espacio de comunicación llevada a cabo con la ayuda de tales redes TIC ;

Aludiendo a los valiosos instrumentos internacionales que tratan de guiar y coordinar los esfuerzos y armonizar la legislación, por ejemplo, el Convenio de Budapest sobre la ciberdelincuencia, de 23 de noviembre de 2001, la Directiva CE 2000/31/CE sobre comercio electrónico, la Directiva UE 40/2013 de 12 de agosto de 2013, la Convención árabe sobre lucha contra los delitos de la tecnología de la información de 2010, el Acuerdo sobre cooperación en el ámbito de la seguridad internacional de la información de 2010, y el proyecto de Convención de la Unión Africana sobre el establecimiento de un marco legal relativo a la ciberseguridad en África de 2012

Recordando la importancia de la protección de los derechos humanos así como el respeto de los principios básicos de la legislación y la práctica penal como el principio de *ultima ratio*, el principio de legalidad, el principio de lesividad que limita la criminalización a aquella conducta que menoscaba directamente o pone en peligro concreto bienes jurídicos personales o colectivos, el principio de culpabilidad y el principio de proporcionalidad;

Con base en los debates y resoluciones de anteriores Congresos Internacionales de Derecho Penal, en especial las resoluciones del XV Congreso Internacional de 1994 de Río de Janeiro, sección II, sobre los delitos informáticos y otros delitos contra la tecnología de la información;

Aprueban la resolución siguiente:

A. Consideraciones generales para la legislación penal

1. Las redes TIC y el ciberespacio han creado intereses específicos que deben ser respetados y protegidos, por ejemplo, la privacidad de las personas, la confidencialidad, integridad y disponibilidad de las redes TIC, y la integridad de las identidades personales en el ciberespacio. Los autores de algunos delitos tradicionales, como por ejemplo fraude, falsedad e infracciones de los derechos de autor, aumentan la peligrosidad de su conducta. Los legisladores, los tribunales y los sistemas de justicia penal han de aceptar el reto de adaptarse continuamente a esta situación.

2. Puesto que la confidencialidad, integridad y disponibilidad de las redes TIC y del ciberespacio son vitales para las personas y las sociedades modernas así como para los medios de comunicación, y dado que las conductas lesivas o peligrosas en estas áreas pueden menoscabar intereses importantes, los Estados y las organizaciones internacionales deben diseñar políticas eficientes con respecto a la protección de las redes TIC y los intereses afectados. Tales políticas deben respetar los derechos humanos y ser coherentes con los principios de la legislación penal, incluido el principio de proporcionalidad. Deben actualizarse continuamente con el fin de evitar nuevas formas de conductas lesivas o peligrosas. Se deberían incentivar y financiar en este ámbito investigaciones empíricas y técnicas para ayudar a los legisladores en estos ámbitos.

3. Por otro lado, se debe evitar un exceso de regulación y penalización del ciberespacio, ya que pone en peligro la libertad de comunicación que es el sello distintivo del ciberespacio. Los legisladores deben ser conscientes de que la regulación de la conducta, la creación de leyes penales y la imposición de medidas de control desproporcionadamente restrictivas en el ciberespacio puede interferir con los derechos fundamentales, especialmente con la libertad de expresión y la recepción, el procesamiento y la difusión de información.

4. Los legisladores no deben penalizar una conducta que sólo infringe normas morales o religiosas. La política criminal debe ser coherente con el principio de lesividad. Por ello, los legisladores no deben criminalizar una conducta que no lesiona ni pone en peligro concreto el interés de una persona o el interés colectivo, incluida la confidencialidad, integridad y disponibilidad y de las redes TIC.

B. Prevención de delitos y alternativas a la sanción penal

5. Se debería alentar a los usuarios de las redes TIC y a los proveedores de sistemas a proteger la seguridad de las redes, incluso mediante la autorregulación de los proveedores. El descuido en la adopción de medidas de seguridad no debería dar lugar a responsabilidad penal por parte de los usuarios. Sin embargo, los legisladores pueden considerar punible la violación de obligaciones específicas para asegurar la seguridad de los datos personales de otros.

6. Si es necesario para los fines de disuasión, los legisladores pueden también considerar permitir, respetando el principio de proporcionalidad, el almacenamiento de datos que haga posible, bajo control judicial efectivo, la identificación de los usuarios.

7. Puesto que las prohibiciones penales conllevan un fuerte reproche moral y pueden estigmatizar a los delincuentes, los Estados deben examinar cuidadosamente si las medidas no penales pueden ser igualmente eficaces en la prevención de los ataques a las redes TIC y de los abusos de la libertad en el ciberespacio. Las órdenes judiciales y la indemnización de daños y perjuicios a las víctimas de acuerdo con el derecho civil, así como instrumentos de justicia restaurativa pueden ser alternativas viables a la sanción penal. Las medidas administrativas, por ejemplo, el bloqueo del acceso o la eliminación de sitios web ofensivos, también pueden tener un efecto preventivo suficiente y pueden hacer innecesario el recurso al derecho penal. Sin embargo, las medidas administrativas no deben ser desproporcionadas o se corre el riesgo de que se conviertan en prácticas de censura aplicadas por las autoridades ejecutivas.

C. Definición de los delitos

8. De acuerdo con el principio de legalidad la ley debería emplear términos que definan la conducta prohibida en términos funcionales de la manera más precisa posible. Cuando la tecnología cambie la ley puede tener que ser adaptada. El principio de legalidad también se aplica a la definición de los deberes y obligaciones de las personas físicas y jurídicas en la medida en que su violación puede dar lugar a responsabilidad penal. Los tribunales no deben ampliar los términos de las prohibiciones penales más allá de su sentido usual.

D. Ampliación de las leyes penales

9. La sanción penal de los meros actos preparatorios de ataques a las redes TIC y el ciberespacio, tales como la producción, distribución y posesión de *malware*, es legítima solo en la medida en que los actos preparatorios como tales creen un riesgo de causar un daño o un peligro concreto para los intereses protegidos de los demás o la confidencialidad, integridad y disponibilidad de las redes TIC. Cuando se castiguen los actos preparatorios, la pena debería ser menor que la prevista para el delito consumado (ver a este respecto las resoluciones del XVIII Congreso Internacional de Derecho Penal de Estambul de 2009, Sección I (A)).

10. La posesión de *software* no debe criminalizarse solo para facilitar la prueba de la infracción. Tal criminalización no debe dar lugar a limitaciones indebidas del uso legítimo del *software*.

11. La mera posesión y visualización de los datos puede ser punible únicamente cuando la posesión y la visualización sean intencionales y lesionen directa o indirectamente o pongan en concreto peligro los intereses protegidos.

12.

a) Los proveedores de acceso a internet no deben ser responsables penalmente por la falta de control de los contenidos que procesan.

b) La responsabilidad criminal de los proveedores de alojamientos debe limitarse a los supuestos en los que:

- estén específicamente obligados por la ley a controlar ciertos contenidos antes de que sean accesibles para los usuarios, y sea razonablemente posible hacerlo, e intencionalmente no cumplan esta obligación, o
- hayan sido alertados, de una manera fiable y específica, del hecho de que están haciendo posible el acceso a contenidos ilegales, y conscientemente no hayan tomado de manera inmediata todas las medidas razonables para hacer que no se pueda acceder a tales contenidos.

E. Armonización internacional de las leyes

13. Se deberían armonizar a nivel mundial las políticas relacionadas con la protección de las redes TIC y el ciberespacio y los intereses de los usuarios con el fin de evitar graves discrepancias entre las regulaciones de la misma materia, mejorar la cooperación internacional y evitar conflictos de jurisdicción.