XIX Congreso Internacional de Derecho Penal. "*Sociedad de la Información y Derecho Penal*"
(Río de Janeiro, Brasil, 31 agosto - 6 septiembre 2014)
Asociación Internacional de Derecho Penal (AIDP-IAPL)

# SECCIÓN I – DERECHO PENAL PARTE GENERAL

# SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL

## Propuesta de Resolución

### Preámbulo

Los participantes en el Coloquio Preparatorio de la Sección I, celebrado en Verona del 28 al 30 de noviembre de 2012, proponen al XIX Congreso Internacional de Derecho Penal, que se celebrará en Río de Janeiro del 31 de agosto al 6 de septiembre de 2014, las siguientes resoluciones;

*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 importantes bienes jurídicos personales y colectivos ;

*Reconociendo* que los Estados han hecho considerables esfuerzos para definir y perseguir los delitos que puedan afectar a la integridad de los sistemas de las TIC y el ciberespacio, así como a los bienes jurídicos 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 de recopilación de información;

*Definidas* las redes de 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/o 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 Decisión marco 2005/222/JAI del Consejo de la UE relativa a los ataques contra los sistemas de información y la Directiva CE 2006/24/CE sobre conservación de datos;

*Recordando* la importancia de los principios básicos de la legislación y la práctica penal como el principio de legalidad, el principio de lesividad que limita la criminalización a aquella conducta que menoscaba o pone en peligro concreto bienes jurídicos personales o colectivos, el principio de culpabilidad y el principio de proporcionalidad entre la gravedad del delito y la gravedad de la reacción del Estado;

*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;

recomendamos lo siguiente:

### A. Consideraciones generales para la legislación penal

1. Las TIC y el ciberespacio han creado intereses específicos que deben ser respetados y protegidos, por ejemplo, la integridad y privacidad de los sistemas de TIC y 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, utilizan las redes TIC y el ciberespacio, lo que aumenta la peligrosidad de su conducta o le añaden una nueva calidad. Los legisladores, los tribunales y los sistemas de justicia penal han de aceptar el reto de adaptarse a esta situación.

2. Puesto que la integridad de las redes de TIC y del ciberespacio es vital para las sociedades modernas, incluidos los medios de comunicación, y dado que las conductas lesivas o peligrosas en estas áreas pueden menoscabar intereses importantes, los Estados deben diseñar políticas eficientes con respecto a la protección de las redes de TIC y los intereses afectados. Tales políticas deben ser proporcionadas y coherentes con la política criminal en general. Debe actualizarse continuamente con el fin de evitar nuevas formas de conductas lesivas o peligrosas.

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 manera desproporcionada a las medidas restrictivas de control en el ciberespacio puede interferir con los derechos fundamentales, especialmente con la libertad de expresión y la libertad de recabar información.

4. La política criminal debe ser coherente con el principio de lesividad. Los legisladores no deben penalizar una conducta que sólo infringe normas morales pero no lesiona ni pone en peligro concreto el interés de una persona o el interés colectivo necesitado de protección.

B. 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, salvo que pueda ser castigada la violación de obligaciones específicas de mantener seguros los datos que hayan sido impuestas a las personas responsables de los datos de otros. El descuido en la adopción de medidas de seguridad por los usuarios no debería eximir a los infractores de responsabilidad penal.

6. 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 de TIC y de los abusos de la libertad en el ciberespacio.

a) pueden ser alternativas viables 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.

b) 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) Si es necesario para los fines de disuasión, los legisladores pueden también considerar permitir el almacenamiento de datos que haga posible, bajo control judicial efectivo, la posterior identificación de los usuarios sospechosos de delitos graves.

C. Principio de legalidad

7. El principio de legalidad exige que los delitos en el ámbito de las TIC y el ciberespacio sean definidos por la ley. Esto 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. La legislación debería emplear términos que definan la conducta prohibida de la manera más precisa posible; cuando la tecnología cambie la ley puede tener que ser adaptada. Los tribunales no deben ampliar los términos de las prohibiciones penales más allá de su sentido usual.

D. Ampliación de las leyes penales

8. Muchas legislaciones han penalizado meros actos preparatorios de ataques a intereses relativos a las TIC y el ciberespacio, tales como la producción, distribución y posesión de malware. Tales ampliaciones de la ley penal son legítimas 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. 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 2009, Sección I (A)).

9. La criminalización de la posesión de software no debe dar lugar a limitaciones indebidas al uso legítimo del software.

10. La mera posesión y visualización de los datos puede ser punible únicamente cuando la posesión y la visualización sean intencionales y puedan causar daño, directa o indirectamente a las personas.

11. Los proveedores de servicios de red TIC no deberían estar obligados a censurar contenidos que procesan. Su responsabilidad penal en ese sentido debería limitarse a los casos en que han sido alertados, de una manera fiable y específica, de la existencia de contenidos prohibidos en su dominio, y no han tomado inmediatamente las medidas razonablemente necesarias para la restauración de la legalidad.

E. Cooperación internacional

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