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 IV – DERECHO PENAL INTERNACIONAL

SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL

Propuesta de Resolución

Preámbulo

Los participantes en el Preparatorio Coloquio de la Sección IV, celebrado en Helsinki del 9 al 12 de junio de 2013, proponen las siguientes resoluciones al XIX Congreso Internacional de Derecho Penal, a celebrar en Río de Janeiro del 31 de agosto al 6 de septiembre de 2014:

Considerando que en el siglo XXI la vida de los ciudadanos se encuentra fuertemente influida y modulada por la tecnología de la comunicación e información (TIC), así como por las oportunidades y riesgos que acompañan a la Sociedad de la información y el ciberespacio, y que en consecuencia los crímenes cometidos en esas áreas afectan a importantes intereses personales y colectivos;

Constatando que los Estados comparten soberanía en el ciberespacio y tienen un interés común en su regulación y protección;

Reconociendo que los Estados han hecho esfuerzos considerables para reconocer la competencia y determinar el *locus delicti* de los delitos que pueden afectar a la integridad de los sistemas TIC y el ciberespacio, así como a los intereses personales y sociales relacionados con ellos;

Teniendo en cuenta las peculiaridades del ciberespacio, como la velocidad en que fluyen los datos, y el hecho de que puedan ser accesibles desde cualquier lugar del mundo;

Reconociendo además las dificultades de localización de la información y de la prueba en el ciberespacio;

Subrayando la importancia fundamental de la protección de los derechos humanos, en particular, el principio de legalidad, el derecho a la intimidad, el Derecho a un juicio justo, el principio de proporcionalidad en la investigación y persecución de las infracciones, y en general, todas las reglas y principios relativos al pocos debido;

Haciendo referencia a los instrumentos regionales e internacionales que se preocupan de guiar y coordinar los esfuerzos de armonización legislativa, como el Convenio de Budapest sobre cibercriminalidad, de 23 de noviembre de 2001, la Directiva Europea 2000/31/CE sobre comercio electrónico, la Decisión Marco europea 2005/222/JHA sobre ataques a los sistemas de información, la Directiva europea 2006/24/CE sobre retención de datos, el Acuerdo de los Estados Independientes de la Commonwealth sobre cooperación en la lucha contra los delitos relacionados con la información informática de 2001, la Convención árabe sobre lucha contra los delitos de tecnología de la información d 2010, el Acuerdo de la Organización de cooperación de Shanghái 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 para la ciberseguridad en África de 2012;

Con base en los debates y resoluciones de los anteriores Congresos Internacionales de Derecho Penal, en particular, las resoluciones de la Sección II del XV Congreso Internacional (1994) celebrado en Río de Janeiro, sobre delitos informáticos y otras infracciones contra la tecnología de la información, y las resoluciones de la Sección IV del XVIII Congreso Internacional (2009) celebrado en Estambul sobre la jurisdicción universal;

Recomiendan lo siguiente:

A. Consideraciones generales

1. Los Estados deberían desarrollar una respuesta coherente a los desafíos del ciberdelito, en particular, manteniendo su legislación y práctica en continua revisión con el fin de asegurar que su derecho penal, su derecho procesal penal y los regímenes de auxilio legal mutuo respondan a las necesidades del actualmente interconectado mundo globalizado.

2. Los Estados deberían considerar el acceso a los instrumentos internacionales existentes sobre cibercriminalidad o desarrollar otros mecanismos jurídicos internacionales con el fin de establecer el estado

de Derecho en el ciberespacio y evitar potenciales conflictos entre los Estados con ocasión de la aplicación de sus políticas y legislación en el ciberespacio.

B. Competencia sustantiva y locus delicti

3. El principio de territorial debe seguir siendo el primer principio de competencia jurisdiccional en el ciberespacio.

4. Los Estados deberían restringir el establecimiento de vías de competencia extraterritorial, con el fin de prevenir los conflictos de competencia más que confiar de manera primaria en su resolución cuando se produzcan.

5. Con la excepción de aquellos crímenes para los que se acepta la jurisdicción universal por parte del Derecho internacional, los Estados no deberían aplicar la jurisdicción universal de hecho o de derecho a los casos de contenido prohibido en el ciberespacio.

6. Las infracciones penales pueden tener más de un lugar. Los Estados pueden establecer un *locus delicti* si la conducta tiene lugar o causa sus efectos en el marco de sus fronteras.

7. Los Estados deberían restringir la aplicación de la teoría del resultado en situaciones en las que el efecto no ha sido "empujado" por el autor hacia el Estado, sino que ha sido "atraído" hacia él por un individuo de ese mismo Estado.

8. En determinados efectos, los Estados tomarán en consideración la existencia de un nexo particular con la infracción, como la intención del autor.

9. Cuando un Estado localiza entre sus fronteras los efectos de una infracción, el principio de legalidad exige que el autor pueda haber tenido una expectativa razonable de que su conducta causaría efecto en aquel país.

10. Un Estado puede ejercer su competencia jurisdiccional sobre un individuo que se encuentra en su territorio y "atrae" contenido prohibido por su propio sistema legal, incluso si es lícito conforme al sistema jurídico del productor.

11. Los Estados podrían considerar el establecimiento de la responsabilidad penal de las personas jurídicas en relación con los ciberdelitos.

C. Investigaciones en el ciberespacio

12. Ningún Estado tiene soberanía exclusiva sobre las redes TI públicamente accesibles.

13. Las agencias de persecución de delitos, al Igual que los ciudadanos, tienen el derecho de navegar por las redes TI libres, sin permiso de los suministradores, y con independencia de si el contenido contemplado se encuentra almacenado o no.

14. Los Estados deberían considerar el establecer, en Derecho interno, la obligación de los suministradores de servicios de cooperar con las agencias de persecución de los delitos, haciendo que la transferencia de datos en el mundo cibernético sea trazable, dando acceso a las contraseñas, desencriptando contenido o instalando mecanismos de búsqueda con fines de investigación. Esta obligación se someterá al principio de proporcionalidad.

15. Todas las personas tienen derecho a la protección por parte de un sistema nacional si la expectativa de protección por dicho sistema puede considerarse legítima.

16. Los Estados, con sujeción al derecho interno, deberían poder usar libremente la prueba que encuentren en redes TI públicamente accesibles.

17. Sea cual sea la nacionalidad de la persona en cuestión Estado debería poder aplicar medidas coercitivas en otro Estado, salvo que lo permita el Estado del territorio.

D. Cooperación internacional en materia penal y ejecución

18. Los Estados deberían implementar las técnicas investigadoras necesarias que les capaciten para prestarse asistencia muta respecto de los ciberdelitos, con base en el principio de proporcionalidad.

19. Los Estados deberían ser, en particular, capaces de suministrar rápida asistencia y debería introducirse una orden provisional de preservación de los datos. La obligación de preservación de los datos debería ser sólo por un tiempo razonable.

20. En situaciones en las que hay un entendimiento común de los ciberdelitos, debería promoverse la eliminación del requisito de la doble incriminación como condición para la asistencia legal mutua.

21. La información obtenida mediante la asistencia legal mutua con fines de investigación debería poder ser usada como prueba, con sujeción al derecho interno.

22. La decisión (provisional) de un tribunal penal de cierre de un servidor, sitio web o elementos similares debería poder ser ejecutada de manera directa si así lo establece un acuerdo internacional o la ley del Estado en el que se localiza el suministrador del servicio.

E. Derechos humanos reales en un mundo virtual

23. Los Estados respetarán los estándares de derechos humanos internacionalmente reconocidos también en el contexto del mundo digital.

24. Si los Estados actúan extraterritorialmente al investigar en el ciberespacio, respetarán los estándares de derechos humanos aplicables en su jurisdicción (*agent control standard*).

25. Los Estados deberían grabar las investigaciones en el ciberespacio con vistas a asegurar la responsabilidad del Estado en caso de violaciones de derechos humanos.

26. Las responsabilidades de un determinado Estado por violaciones de derechos humanos deberían decidirse tras el conocimiento de la violación y no como condición para la admisibilidad de una queja ante el mecanismo de supervisión.

F. Sala judicial virtual

27. Las autoridades podrán enviar comunicaciones directamente a los acusados, testigos, víctimas y peritos que se encuentren físicamente en otro Estado, siempre que dicho Estado acepte este método de comunicación.

28. Siempre que lo consienta el individuo afectado, deberían ampliarse las posibilidades de uso de la tecnología digital, como los viodeolinks, con objeto de disminuir la necesidad de medidas tan intrusivas como la extradición.

29. Debería animarse a los Estados a considerar la posibilidad y condiciones de recogida de pruebas mediante tecnología digital, incluso aun cuando el individuo no se encuentre físicamente presente en la vista.

30. La seguridad y confianza de las líneas de comunicación en uso por parte de las autoridades debe ser de mayor nivel. Las comunicaciones deberían protegerse frente al pirateo.