# SECCIÓN IV – DERECHO PENAL INTERNACIONAL

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:

*Sobre la base* del proyecto de resolución elaborado en el Coloquio Preparatorio de la Sección IV, celebrado en Helsinki del 9 al 12 junio de 2013,

*Considerando* que en el siglo XXI la vida de los ciudadanos se encuentra fuertemente influida y modulada por las tecnologías 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 jurisdiccional 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 la 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 pruebas 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 y la protección de los datos, 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 proceso debido;

*Haciendo referencia* a los instrumentos internacionales y regionales 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 Directiva UE 2013/40 relativa a los ataques contra los sistemas de información, 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 de 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, las resoluciones de la Sección III sobre medidas procesales especiales y respeto de los derechos humanos y las resoluciones de la Sección IV sobre la jurisdicción universal del XVIII Congreso Internacional (2009) celebrado en Estambul;

*Definiendo* a efectos de la presente resolución las medidas coercitivas como aquellas medidas contrarias a la voluntad del sujeto o que infringen su derecho a la intimidad;

Han adoptado las siguientes resoluciones:

**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, dentro del respeto de los derechos fundamentales y humanos.

2. Los Estados deberían considerar la adhesión a los instrumentos internacionales existentes sobre cibercriminalidad. Los Estados y la comunidad internacional deberán trabajar para desarrollar otros mecanismos jurídicos internacionales, incluyendo estándares de cumplimiento normativo para las empresas multinacionales, 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 su legislación en el ciberespacio.

**B. Competencia jurisdiccional sustantiva y *locus delicti***

3. Si bien el principio de la territorialidad sigue siendo el principio fundamental de la competencia jurisdiccional también en el ciberespacio, produce efectos cuando se aplica a los delitos en el ciberespacio, ya que *de facto*

permite a los Estados localizar delitos en su territorio casi con una base universal y deja a los individuos en duda en cuanto a qué Estados pueden reclamar la jurisdicción. Los Estados deberían restringir el ejercicio de su competencia jurisdiccional a 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.

4. Para la determinación de los efectos, los Estados tomarán en consideración la existencia de un nexo particular con la infracción, tal como la intención del autor si puede deducirse del uso de su idioma, la disposición de servicios de pagos nacionales, un servicio ofrecido en una ciudad específica, etc.

5. 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.

6. 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.

7. Los Estados y la comunidad internacional podrían considerar el establecimiento de exigencias de cumplimiento normativo corporativo y la responsabilidad penal de las personas jurídicas en relación con los ciberdelitos.

**C. Investigaciones en el ciberespacio**

8. Ningún Estado tiene soberanía exclusiva sobre las redes TIC públicamente accesibles.

9. Excepto en los casos en los que se aplican medidas coercitivas o encubiertas, las agencias de persecución de delitos pueden acceder (y operar) a las redes TIC libres sin permiso de los proveedores y /o de los Estados, y con independencia de si el contenido contemplado se encuentra almacenado.

10. Con el fin de prevenir el ciberdelito y someter a control la investigación, los Estados y la comunidad internacional deberían considerar la imposición a los proveedores de servicios, de software y a los desarrolladores de aplicaciones y otros privados implicados en las TIC de una obligación de mejorar y establecer tecnología respetuosa con la protección de la privacidad de los datos.

11. Los Estados deberían considerar el establecimiento, con arreglo al derecho nacional, de la obligación de que los proveedores de servicios cooperen, previa autorización de una autoridad judicial independiente, con los organismos encargados de hacer cumplir la ley (por ejemplo, haciendo posible la trazabilidad de la transferencia de datos en el mundo cibernético, dando acceso a las contraseñas, descifrando el contenido o la instalación de dispositivos de búsqueda con fines de investigación). Esta obligación está sujeta al principio de proporcionalidad y el respeto de los derechos humanos fundamentales e internacionales.

12. Los Estados que llevan a cabo las investigaciones deben permitir a todas las personas involucradas la protección que les correspondería a ellos en un caso nacional similar, y al mismo tiempo permitirles la protección que les aporta el ordenamiento jurídico nacional del Estado en que se toman las medidas de investigación o donde las personas involucradas se encuentran ubicadas cuando se toman las medidas de investigación.

**D. Cooperación internacional en materia penal y ejecución**

13. Los Estados, cuando conceden asistencia legal mutua respecto de los ciberdelitos, deben estar seguros de que pueden adoptar todas las medidas de investigación que podrían ser legalmente adoptadas en un caso nacional similar.

14. Los Estados deberían ser capaces de suministrar rápida asistencia y ejecutar una orden provisional de preservación o congelamiento de la información y de la prueba durante un tiempo razonable y sin afectar indebidamente a los derechos de las partes.

15. Los Estados no pueden denegar la asistencia legal mutua con base en la falta de doble incriminación para los delitos cibernéticos, cuya criminalización es exigida por una obligación internacional que les incumbe.

16. La decisión (provisional) de una autoridad judicial independiente de cerrar un servidor o un sitio web, o una petición de un Estado para acabar con una *botnet*, podrá ser directamente ejecutada si así lo prevé un acuerdo internacional o la ley del Estado en el que el proveedor del servicio o en el que se encuentra ubicado el servidor del comando y control de la *botnet*. Siempre que sea posible, se debe dar preferencia a hacer inaccesible el sitio web solo en el territorio del Estado requirente, evitando así la limitación innecesaria de la libertad cibernética.

17 El uso posterior de la información recogida por los servicios de inteligencia en materia penal sólo está permitido cuando la información en cuestión podría haber sido obtenida a través de los mecanismos regulares de cooperación judicial o policial en materia penal.

**E. Derechos humanos reales en un mundo virtual**

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

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

en el que se están llevando a cabo las investigaciones extraterritoriales y en el que las personas implicadas se encuentren ubicadas si se están llevando a cabo investigaciones extraterritoriales,

20. Los Estados deberían grabar las investigaciones en el ciberespacio con vistas a asegurar la responsabilidad del Estado en caso de violaciones de derechos humanos. También deberían revelar tales datos a la defensa con la finalidad de asegurar un juicio justo y proporcionar recursos ante mecanismos de supervisión.

21. 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**

22. Las comunicaciones pueden ser enviadas de manera digitalizada por las autoridades directamente a los acusados, testigos, víctimas y peritos que se encuentren físicamente en otro Estado, siempre que dicho Estado acepte este método de comunicación. Las comunicaciones deben estar acompañadas de una traducción a un idioma comprensible por el destinatario y de una declaración señalando los derechos y obligaciones del destinatario en relación a la comunicación recibida, en particular en lo que se refiere a su derecho a la defensa letrada, al deber de comparecer, al desacato y al perjurio.

23. Las posibilidades de hacer uso de la tecnología digital, como las videoconferencias (*videolinks*), en la justicia penal internacional deben ampliarse a fin de disminuir la necesidad de medidas coercitivas como la extradición, así como para evitar la innecesaria transferencia temporal de una persona detenida o la presencia física de testigos y peritos ante las autoridades en el extranjero.

24. Debería animarse a los Estados a considerar la posibilidad y las condiciones de presentación de prueba mediante tecnología digital durante la fase de enjuiciamiento, incluso cuando el individuo no se encuentre físicamente presente en la vista.

25. La seguridad, integridad y confianza de la comunicación digital en uso por parte de las autoridades debe ser de mayor nivel.

26. Los Estados deben proporcionar instalaciones adecuadas para permitir las comunicaciones digitales directas entre cliente-abogado, sobre todo cuando el cliente está detenido.

27. La confidencialidad de las comunicaciones digitales utilizadas en la justicia penal internacional debe ser inviolable.