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)

SECCION II - DERECHO PENAL- PARTE ESPECIAL

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:

Tomando nota de que el rápido crecimiento global de las redes de tecnologías de la información y las comunicaciones (TIC) en el ciberespacio, que conducen a la conectividad global, está proporcionando amplias oportunidades para diversos delincuentes en la planificación y comisión del delito, mediante el aprovechamiento de vulnerabilidades online y mediante la amenaza a las infraestructuras críticas de la información y comunicaciones de los países;
Sobre la base de los proyectos de resolución aprobados en el Coloquio Preparatorio de la Sección II, celebrado en Moscú, del 24 al 27 de abril 2013;
Advirtiendo de que el advenimiento del mundo cibernético ha creado nuevos bienes jurídicos que están en juego y merecen reconocimiento y protección, y que, al mismo tiempo, los bienes jurídicos existentes se enfrentan a nuevos retos y nuevas vulnerabilidades, y surgen nuevos delitos cibernéticos;
Tomando nota de los informes nacionales que la convergencia y armonización, por un lado, pero también la falta de aplicación de las normas jurídicas internacionales vigentes, por otro, dan lugar a la necesidad de seguir trabajando en la convergencia y la armonización de los marcos jurídicos nacionales, conscientes del papel subsidiario y de ul*tima ratio* del derecho penal (véase la recomendación 4, Sección I);
Teniendo en cuenta la gran importancia y el impacto global del mundo de la cibernética en la vida cotidiana de las personas, en la sociedad en su conjunto, en el mercado internacional y el comercio, sobre las transacciones financieras, en las interacciones políticas e incluso en la guerra, lo que da lugar a nuevas y complejas cuestiones jurídicas, incluidas las relacionadas con la justicia penal;
Tomando nota de que en un mundo globalizado, interconectado e interdependiente, la información crítica y las infraestructuras de comunicación juegan un papel vital en las funciones gubernamentales y en los servicios, la seguridad nacional, la protección civil, la salud y la seguridad pública, y la banca y los servicios financieros;
Conscientes de que la promesa de comunicaciones más libres y más rápidas en todo el mundo por medios electrónicos también conlleva el riesgo de limitaciones de contenido y de forma, de un control generalizado y de violaciones de los derechos humanos y de la intimidad;
Reconociendo que en estos momentos la respuesta de la sociedad a los nuevos retos y amenazas que plantea la evolución y el cambio en la tecnología, la forma de vida y los valores conduce a más criminalización y al uso excesivo de la protección penal;
Conscientes de la importancia de estar alerta y de proteger y defender los valores y los principios jurídicos fundamentales, en especial los relacionados con los derechos humanos y la integridad, la dignidad y el valor de los seres humanos;
Teniendo en cuenta la importancia, la utilidad y el papel fundamental desempeñado por los medios de comunicación social en la vida privada y pública, la máxima de que debe garantizarse la libertad de comunicación y de expresión, equilibrada por el reconocimiento y el respeto de las responsabilidades mutuas;
Expresando su preocupación por el hecho de que los avances en las tecnologías de la información y de las comunicaciones han creado una grave necesidad de desarrollar y adoptar una política jurídica global para el mundo cibernético con el fin de asegurar su desarrollo ordenado y positivo, que debe utilizar normas jurídicas técnicamente neutrales para mantenerse al día con el ritmo de desarrollo técnico;
Preocupada por el posible exceso de confianza en las políticas represivas y la protección penal en lugar de apostar por enfoques innovadores y soluciones normativas y administrativas, y por la educación pública así como por las medidas de seguridad técnicas, organizativas y personales;
Comprometidos con la aportación de soluciones a los problemas y desafíos que presenta la tecnología de la información y de las comunicaciones, especialmente las nuevas formas y tipos de delitos, garantizando al mismo tiempo que la protección de los derechos humanos, las libertades fundamentales y los bienes jurídicos no sea menor online que offline;
Teniendo en cuenta el importante papel que la sociedad civil, las organizaciones no gubernamentales y los actores empresariales pueden desempeñar para hacer frente de una manera positiva y constructiva a los nuevos problemas y amenazas y sus repercusiones en el sistema legal;

Convencidos de la importancia de colaborar y cooperar con los sectores privado y público, recordándoles su papel y sus responsabilidades para asegurar el ciberespacio y la prevención de los delitos cibernéticos en beneficio general de la sociedad;
Haciendo hincapié en la necesidad de un entendimiento común de la ciberdelincuencia y de la ciberseguridad y de esfuerzos de colaboración por parte de la comunidad jurídica internacional que puedan apoyar y garantizar un mundo cibernético seguro conformando marcos aplicables a través de las fronteras e interoperables con regímenes jurídicos internacionales y nacionales y con los sistemas del lugar;
Tomando nota con agradecimiento de la labor de las organizaciones internacionales y regionales, y en particular la labor del Consejo de Europa en la elaboración de la Convención sobre la ciberdelincuencia (2001); las normas legales de la Unión Europea; las contribuciones de la Organización de los Estados Americanos, de la Liga Árabe, de la Comunidad Económica de Estados de África Occidental, de la Comunidad de Estados Independientes, del Banco Mundial, de la OCDE, de las Naciones Unidas y de otras organizaciones dirigida a iniciar una interacción fructífera entre el sector gubernamental y el sector privado sobre las medidas de seguridad y contra el delito en el ciberespacio;
Teniendo presente el objetivo principal de la AIDP de defender el Estado de derecho y apoyar el desarrollo de la ley para hacer frente a las tendencias y fenómenos actuales y responder de manera eficiente y positiva a la constante necesidad de elevar el nivel de protección de la persona y la comunidad;
Destacando el trabajo previo de la AIDP en esta área crucial como las conclusiones del Congreso de la AIDP de Jóvenes Penalistas (Noto, de junio de 2001, tema 3), el Coloquio Preparatorio sobre el Tráfico Internacional de Mujeres y Niños (Río de Janeiro, abril de 2002) y la mesa redonda sobre la trata internacional de mujeres y niños, celebrada con motivo del XVII Congreso AIDP (Beijing, septiembre de 2004);
Han adoptado las siguientes resoluciones:
1. Al abordar la amenaza y la realidad de la delincuencia informática y la necesidad de la seguridad cibernética, los sistemas jurídicos y la justicia penal deben equilibrar los intereses individuales, colectivos, del sector privado y del público. Debe evitarse un exceso de confianza en la protección penal y apostar a favor de una robusta prevención, defensa activa, educación y sensibilización del público, y de las penas sustitutivas.
2. Los bienes jurídicos que deben protegerse incluyen la confidencialidad, integridad y disponibilidad de los datos y de los sistemas TIC, la autenticidad de la información, la vida y la integridad física, la integridad de los niños, la privacidad, la protección frente al daño y la pérdida de la propiedad (incluida la propiedad virtual), los derechos de autor y el honor, la libertad de expresión y otros derechos humanos fundamentales.
3. La protección de los consumidores, el consentimiento informado, la limitación de los fines, el derecho a la cancelación, corrección y notificación, deben ser los valores primordiales para orientar la formulación de leyes y reglamentos sobre la recopilación de datos, la venta y la compra en Internet, las transacciones e inversiones financieras, y el marketing y las campañas promocionales.
4. Los encargados del procesamiento de datos personales comerciales, como los proveedores de Internet y de telecomunicaciones, las plataformas de medios sociales, y los desarrolladores de aplicaciones, deberían estar obligados a adoptar la privacidad para diseñar políticas y, por defecto, si es necesario mediante medidas obligatorias. La violación de las mismas debe ser respondida con sanciones bien penales o no criminales.
5. Un esfuerzo concertado es esencial para prevenir y combatir: el acceso ilegal a sistemas TIC; la interceptación ilegal de transmisiones no públicas de datos electrónicos; la interferencia de datos y sistemas sin derecho alguno; el abuso de dispositivos, software, contraseñas y códigos; la falsificación y el fraude informáticos; y el acceso no autorizado por parte de organismos gubernamentales. Esto incluye la adopción de un nivel mínimo de protección penal contra los actos intencionales y perjudiciales que supongan una violación de la confidencialidad, integridad y accesibilidad de los datos y de los sistemas TIC.
6. Se deben adoptar medidas legales apropiadas para establecer circunstancias agravantes o delitos específicos sancionables con penas más graves por interferir en el funcionamiento de las infraestructuras de información y comunicaciones críticas.
7. La producción y la distribución, difusión, importación, exportación, oferta, venta, compra, posesión y el acceso a sabiendas a la pornografía infantil y cualquier complicidad y participación en cualquiera de estos actos debe ser firme y coherentemente prevenida y criminalizada con sanciones apropiadas, especialmente cuando involucra a niños reales, a menos que sea para su propio uso privado habiendo alcanzado la mayoría de edad sexual.
8. El robo de identidad, incluido el llevado a cabo a través de *phishing*, en su conjunto o en sus componentes, debe ser tipificado, si no se dispone lo contrario por otras disposiciones penales. Si los Estados optan por criminalizar la mera posesión de información relacionada con la identidad o hacerse pasar por personas no existentes, deben limitarse a los actos cometidos con intención criminal de causar daño. Tales disposiciones no deben restringir ni criminalizar la libertad de pensamiento y de expresión, en particular las actividades literarias y artísticas.

9. Dada la creciente preocupación por la frecuencia y gravedad del acoso cibernético, el ciberacoso escolar, y la captación cibernética de menores, se deberá prestar especial atención para responder eficazmente al problema, haciendo hincapié en los enfoques positivos, la prevención, la educación y la sensibilización pública, y las penas sustitutivas, en lugar de aplicar solo la protección penal.
10 La protección de los derechos de propiedad intelectual debe centrarse en aquellas violaciones intencionales con fines comerciales significativos o que produzcan daños graves.
11. La gestión temeraria o por negligencia grave de infraestructuras críticas de las TIC y de grandes cantidades de datos sensibles, tales como los datos de la tarjeta de crédito, debe corregirse a través de sanciones no penales o criminales. Del mismo modo, la no adopción de medidas de seguridad razonables y / o la revelación de la información necesaria sobre las violaciones de seguridad en su debido momento por los proveedores de servicio de Internet puede ser motivo de una acción civil o penal.