Planificación semanal de la asignatura de cibercrimen

Sesiones 1 y 2:

I. INTRODUCCIÓN. CONSIDERACIONES POLÍTICO CRIMINALES. DATOS SOBRE CIBERVICTIMIZACIÓN.

1. El Derecho Penal a remolque de las nuevas tecnologías: sociedad de riesgo. Incremento de los delitos de peligro abstracto. Desformalización. Expansión. Perfil pedagógico.

2. Influencia de Internet en el Derecho penal.

3. Lado oscuro del desarrollo: nuevas formas de criminalidad, utilización de las redes informáticas para facilitar la comisión de los delitos convencionales, macrovictimización, problemas de incriminación, problemas de competencia, anonimato: sensación de impunidad. Plataforma de la criminalidad organizada.

Sesión 3:

II. MARCO JURÍDICO INTERNACIONAL DE REFERENCIA.

Sesión 4:

III. BIENES JURÍDICOS AFECTADOS POR LA CIBERDELINCUENCIA.

Intimidad, honor, libertad, libertad e indemnidad sexual, patrimonio, propiedad intelectual, seguridad exterior e interior del Estado. Especial referencia a la protección penal de la intimidad y del patrimonio en relación con la delincuencia en el ciberespacio.

Sesión 5:

IV. TECNOLOGÍAS DE LA COMUNICACIÓN. LA PROTECCIÓN DE DATOS Y LOS RIESGOS ANTE LAS TECNOLOGÍAS DE LA COMUNICACIÓN.

1. Evolución de la intimidad: Teoría de las esferas. Privacy e impacto de nuevas tecnologías: derecho activo de control vinculado a la autodeterminación. Expansión redes telefonía. Sociedad postindustrial: moderno secreto profesional. El derecho al anonimato. El derecho al olvido.

2. Crisis de lo público. Invocación de autorregulaciones.

3. Tipificación del control clandestino auditivo y visual, control ilícito de señales de comunicación: interceptación de señales, de conversaciones, vulneración password.

4. Supuestos especiales: Videocámaras en espacios públicos. Escuchas clandestinas. Cámaras ocultas y grabaciones en las que el interlocutor participa. Difusión inconsentida de vídeos íntimos. Requisitos de las escuchas autorizadas judicialmente: análisis jurisprudencial.

5. Protección de datos: el habeas data informática.

Sesión 6:

V. LA CIBERDELINCUENCIA COMO PLATAFORMA PARA LA CRIMINALIDAD ORGANIZADA.

1. Crimen organizado y sociología criminal: concepto y características. Tipologías. Estructura organizativa. Corrupción, globalización, sofisticación. Relación Estado-crimen organizado.

2. Justificación de la respuesta penal específica ante el crimen organizado. Fundamento. Bien jurídico protegido. Incentivos de la colaboración con la justicia.

3. Técnica legislativa penal. Tipos penales. Problemas concursales.

4. Respuesta basada en que el delito ¿no resulte provechoso¿: el comiso, el blanqueo de capitales, organismos internacionales autónomos de control de las finanzas. Los paraísos fiscales y las jurisdicciones con secreto bancario.

Sesiones 7 a 10:

VI. TECNOLOGÍAS DE LA INFORMACIÓN. CONDUCTAS DELICTIVAS.

1. Delitos cuyo único medio de comisión es la Red: hacking, sabotaje informático (cracking). Especial referencia a la denegación de Servicios (Denial of Service).

2. Infracciones tradicionales que utilizan las redes telemáticas como instrumento: los fraudes en internet (phising), tratamiento del spoofing, el espionaje (Spyware), atentados a la propiedad intelectual e industrial (Linking, Inlining, Metatags, keywords), ataques a bienes personalísimos realizados a través de internet acompañados o no de TICs: ciberbullying, child grooming, Sexting.

3. Ataques por el contenido transmitido: pornografía infantil, ciberterrorismo.

Sesión 11:

VII. ATRIBUCIÓN DE RESPONSABILIDAD PENAL A LAS PERSONAS FÍSICAS Y JURÍDICAS POR PUBLICACIÓN DE CONTENIDOS DELICTIVOS (PROVEEDORES DE CONTENIDOS, PROVEEDORES DE SERVICIOS).

Sesión 12:

VIII. PERSEGUIBILIDAD. PROBLEMAS DE COMPETENCIA.