

ABOGACÍA

Derecho Informático y de las Nuevas Tecnologías

Profesores:

Titular: Roberto Abieri

Adjuntos: Gabriel Coronel
Lavecchia

Maria Porro Cimarosti

Carga Horaria: 64 hs.

Modalidad: Cuatrimestral

Comisión: TNA

2023

1. Fundamentación:

El gran desarrollo que ha tenido Internet a nivel global en los últimos años ha permitido que se extienda ampliamente el uso de las redes sociales, generando un cambio sustancial en el mundo de las comunicaciones y de las relaciones humanas. Las personas transitan dos caminos convergentes: la vida on line y la real. Las redes sociales participan en ambos aspectos de la vida del hombre y de la empresa. El concepto histórico de la intimidad y de reputación ha cambiado porque en la actualidad existen altos niveles de exposición y millones de personas opinando, en tiempo real.

Esta especialidad transversal a todas las demás, se la define como un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la Informática. Es el derecho especializado en el tema de las tecnologías de la información y la comunicación, sus usos, sus aplicaciones y sus implicaciones legales. Se estudiará al Derecho Informático como un punto de inflexión en las denominadas ciencias jurídicas, dado que todas las ramas del Derecho quedaron afectadas por la llamada Sociedad de la Información, transformando los procesos sociales, jurídicos y políticos.

2. Objetivos:

El objetivo del presente programa es que los alumnos puedan estudiar y debatir acerca de las variadas cuestiones que ofrece Internet desde un punto de vista práctico con la presencia de reconocidos profesionales especialistas y referentes en la materia.

Se busca que puedan comprender las situaciones tradicionales que plantea Internet, pero avanza sobre las actuales problemáticas que comprenden la responsabilidad civil de los sitios de internet, delitos que se pueden cometer a través de la web, los riesgos que existen para los menores en el uso de las Redes Sociales; la disminución, por parte de los empleados, de la expectativa de privacidad en el ámbito laboral, el papel que juega Facebook y Twitter y las consecuencias de exponer la vida.

3. Organización de los contenidos formativos:

Unidad 1: Informática y derecho

La Sociedad Tecnológica. El impacto de la informática, las redes y la interconexión virtual en la sociedad contemporánea. Su impacto en la realidad cotidiana y en el Derecho. Análisis y desafíos actuales. La llamada Web 2.0 y las Redes Sociales.

El impacto de la informática en el Derecho. Vinculación entre el Derecho positivo, la Informática y las Tecnologías de Información y Comunicación (TICs): la Informática al servicio del Derecho (Informática Jurídica) y la Informática como objeto de estudio del

Derecho (Derecho Informático). Los nuevos conceptos legales, sus alcances e interpretaciones y desafíos para el Derecho.

Unidad 2: La realidad virtual como nueva modalidad delictiva

Nociones y conceptos generales y específicos del Derecho Penal y Constitucional en materia de delitos. Principios y garantías constitucionales aplicables. La tipificación penal. Delitos relacionados con la informática en el Código Penal y Leyes Especiales. Situaciones de hecho aún no reguladas jurídicamente. Las figuras penales existentes. Nuevos conceptos y bienes jurídicos a proteger introducidos por la Ley 26.388. La importancia de la prueba como método de probanza de los hechos delictivos. Tipos de prueba. Su obtención conforme a la ley. La *Ciberdelincuencia*: Concepto, alcance, interpretación, formas de llevarla a cabo. Su distinción con los hechos punibles tradicionales. Necesidad de adecuación de los organismos del Estado para prevenir, investigar y perseguir las nuevas modalidades delictivas. Las *Cibercriminalidad*. Concepto, alcance. Normativa a nivel nacional e internacional. Objetivos. *Ciberterrorismo* y *Ciberguerra*. Concepto. Alcance. Adecuación de los Estados para combatirla. Su importancia y sus resultados obtenidos.

Unidad 3: Delitos informáticos

Uso seguro y responsable de Internet. La *prevención personal* como la herramienta más eficaz para combatir los delitos informáticos. La importancia de la prevención y conscientización individual, familiar y grupal.

Acceso ilegítimo informático. El acceso ilegítimo a un sistema, dato informático o base de datos personales. Acceso agravado. Captación ilegal de datos, imágenes y sonidos.

Daño informático. El daño informático y la distribución de programas destinados a causar daños. Daño informático agravado. Las infraestructuras críticas de información. Violación de comunicaciones electrónicas. Comunicación electrónica. Violación, interrupción y publicación indebida de comunicaciones electrónicas. Revelación de secretos.

Estafas informáticas. Estafa por medios informáticos y estafa a sistemas informáticos. Perjuicio patrimonial. Antecedentes. Modalidades de estafas informáticas. Phishing. Pornografía infantil. Ofrecimiento y distribución de imágenes de menores de edad. La tenencia con fines de distribución. El elemento subjetivo.

Conductas ilícitas informáticas aún no tipificadas. Robo de identidad digital, ciberhostigamiento (cyberbullying), seducción de menores con fines sexuales (grooming), sexting.

Unidad 4: Privacidad y protección de datos personales

Intimidad y Privacidad. Diferencias entre intimidad, privacidad, reputación e imagen online. Los datos personales. La autodeterminación informativa.

La evolución de la protección del Derecho a la Privacidad de la mano de la evolución tecnológica. Los arts. 19, 18 y 43 de la Constitución Nacional y el art. 1071 bis del Código

Civil. El Habeas Data y la protección de los datos personales. La Ley 25.326 y el Decreto 1558/2001. Objetivo y alcances.

Datos Personales. Tipos de Datos: genéricos y sensibles. Definición (art. 2). Régimen especial. Prohibición de recolección de datos sensibles y excepciones (art. 7 y 8). Derechos y obligaciones de los Titulares. La Responsabilidades de los usuarios (art. 13, 14, 15, 16, 17). La acción de habeas data (art. 33 y ss.). Cesión de datos personales y transferencia internacional (art. 11 y 12).

Bases de datos Personales. Formas de recolección (art. 4). El consentimiento (art. 5). Concepto, alcance e importancia de la manifestación expresa de la voluntad del titular del dato. Excepciones al pedido de consentimiento. Información que deberá brindarse (art. 6). Consentimiento informado.

Obligaciones de los Titulares y Responsables de las bases de datos. Obligación de registro (art. 3). El Registro Nacional de Datos Personales de la Dirección Nacional de Protección de Datos Personales (DNPDP). Características. Distintos formularios. Requisitos técnicos de las bases de datos. Medidas y Documentos de Seguridad (art. 9). Disposición 11/2006 de la DNPDP. Auditorías.

Régimen Jurídico de las Entidades de Informes Crediticios. Empresas de informes de riesgo crediticio (Veraz, Fidelitas, Nosis). Modos de recolección de datos. La Central de Deudores del Sistema Financiero del BCRA. Tiempo de conservación de datos. Derecho al olvido. Posibles conflictos.

Bases de datos para publicidad y encuestas. Características y formas de operar. Correo electrónico masivo o no solicitado. Fallo sobre SPAM en Argentina. Uso indebido de datos personales. Sanciones civiles (daños y perjuicios), sanciones administrativas (Disposición 7/2005 DNPDP) y sanciones penales (art. 157 bis Código Penal).

Las Redes Sociales y la Privacidad en la web. Facebook. ¿Qué compartimos? Buenas prácticas para proteger nuestros datos. La importancia de las Políticas de Privacidad de los sitios web. El manejo de la reputación personal online.

Privacidad en el ámbito laboral. Derechos del empleador a controlar el trabajo frente al Derecho del empleado a proteger su privacidad. Límites. La problemática de uso del correo electrónico laboral, de los contenidos digitales de las computadoras, de las actividades en las redes sociales. El control laboral del correo electrónico.

Unidad 5: e-commerce

Nuevas formas de contratación. El uso del *Documento Electrónico*. El documento. El documento electrónico. El sistema del Código Civil. La incorporación del documento electrónico y digital en la legislación argentina. La *Firma Digital*. La firma. Firma electrónica y firma digital. Criptografía. Sistemas simétricos y asimétricos. *Certificados y/o comprobantes Digitales*. Infraestructura de Clave Pública (PKI) y organismos involucrados. *Certificadores Licenciados*. La Ley 25.506. Objetivos. Exclusiones. Requisitos de validez. Presunción de autoría e integridad. Sanciones.

Categorías de Comercio Electrónico. Concepto de Completo e incompleto. Categorías. Tienda electrónica (e-shop), centro comercial electrónico, aprovisionamiento electrónico

(e-procurement), subasta electrónica. Publicidad en la red. Ventajas del comercio electrónico.

Contratos electrónicos, su validez legal en Argentina y en el Derecho Internacional. Ley aplicable y Juez competente en materia de conflictos con sitios extranjeros. Casos. responsabilidad civil de sitios web y buscadores. Responsabilidad de los titulares de los sitios web y los buscadores. Incorporación de contenidos ilícitos e incorporación ilícita de contenidos. Obligaciones de los Proveedores de Servicio de Internet (ISP). Libertad de contenidos. Conservación de datos. Seguros de responsabilidad civil. Responsabilidad contractual y extracontractual, objetiva y subjetiva.

Unidad 6: Régimen jurídico de los sitios de internet

El Emprendedor web. El empresario y la empresa. Aspectos legales que se deben considerar en un emprendimiento o negocio en la web.

Sociedades Comerciales. Inspección General de Justicia (IGJ). Sociedades Comerciales (Ley 19.550). Concepto. La SA y la SRL. Características. El capital social. Administración. Diferencias con las Fundaciones, Asociaciones Civiles, Federaciones y Confederaciones. Marcas Comerciales. Concepto. Ley 22.362. Clases de marcas de productos y servicios. Registro. Beneficios y derechos del titular de una marca. Custodia. Marcas notorias. El Instituto Nacional de la Propiedad Industrial (INPI). Vistas y Oposiciones. Formularios. Plazos. Fallos.

Nombres de Dominio. Nombres de dominio. El ICANN y el Sistema de Nombres de Dominio (DNS). Dominios de Nivel Superior Generales (gTLDs) y de cada país (ccTLDs). Registro de nombres en Argentina. La Dirección Nacional de Registro de Dominios de Internet (NIC-Ar). Reglas para el registro. Subdominios registrables (com.ar, org.ar, net.ar, gob.ar, edu.ar, tur.ar, mil.ar, int.ar). Conflictos con las marcas registradas. Análisis de casos. Solución de controversias.

Propiedad intelectual del sitio web. El Copyright. La ley 11.723. La Dirección Nacional del Derecho de Autor (DNDA). El depósito y registro de las obras (contenido, diseño, nombres). El derecho de uso y reproducción de obras protegidas. Registro del sitio web. Creative Commons. Safe Creative. Sanciones penales. ¡Los casos Cuevana, Taringa! y Megaupload.

Registro de software. Código fuente y código objeto. Ley 25.036. Beneficios del registro de software. La Cámara de Empresas de Tecnología de la Información de Argentina (CESSI). Software Propietario vs. Software Libre. Licencias. Inspecciones de Software Legal. Sanciones.

Adecuación y Registro de las Bases de Datos Personales. Los bancos de datos personales. La Ley 25.326. El Registro Nacional de Bases de Datos de la Dirección Nacional de Protección de Datos Personales (DNPDP). Obligatoriedad. Medidas y Documentos de Seguridad.

Leyendas legales para el sitio web y las comunicaciones. Términos y Condiciones del Sitio Web. Políticas de Privacidad. Cláusulas habituales. Leyendas obligatorias para formularios de registración, correos y comunicaciones electrónicas. Marketing y publicidad.

Contratos Informáticos. Diferencia con los contratos electrónicos. Particularidades. Concepto de sistema, entrega y test de aceptación. Obligaciones específicas. Etapa precontractual y documentación. Contratos informáticos esenciales: Confidencialidad (NDA), Carta de Intención (MOU), Due Diligence, Acuerdos con Inversores, Desarrollo de Sitios Web, Software (licencias, desarrollo de software a medida), Hardware, Publicidad en Internet, Acceso a Internet, Hosting, Escrow, Outsourcing de Sistemas de Información, Cloud Computing.

4. Bibliografía:

Bibliografía Obligatoria:

Palazzi, P. (2016). *Los delitos informáticos en el Código Penal. Análisis de la ley 26.388*.

Buenos Aires: Abeledo Perrot.

Fernandez Delpech, H. (2004). *Internet, su problemática jurídica*. Buenos Aires: Lexis Nexis.

Monastersky D. y Salimbeni, M. (2012). *Introducción al robo de identidad*. Buenos Aires: Identidad Robada.

Legislación:

Ley 25.326, Dec 1558/2001

Ley 26.388

5. Metodología de trabajo y enseñanza:

La asignatura se desarrolla bajo la modalidad teórico-práctica, a partir de la presentación expositiva por parte del docente para la presentación de los temas de las diferentes asignaturas. Se procurará la participación activa de los alumnos. Además, se utilizarán las siguientes formas de trabajo en el aula:

- Trabajos prácticos individuales y grupales
- Análisis de casos
- Proyecciones temáticas

6. Pautas de acreditación y evaluación:

Las condiciones para la acreditación y aprobación de la asignatura son las siguientes:

-Que el estudiante cuente con una asistencia mínima obligatoria del cincuenta por ciento (50%), tal como se establece en el Reglamento de Alumnos de la Universidad.

-Asimismo se requerirá que apruebe una evaluación parcial obligatoria, durante el desarrollo de la cursada. Para obtener la nota mínima de aprobación 4 (cuatro) se deberá contestar correctamente al menos el 60 % de las preguntas del examen. Del mismo modo se procederá con el examen recuperatorio.

-En caso de no ser aprobados, el estudiante podrá recuperar el parcial en dos instancias recuperatorias: antes de finalizar la cursada y en la primera fecha de final.

-Además deberá aprobar un Examen Final oral que consistirá en la exposición de alguna temática de la materia.

Las evaluaciones finales serán orales siempre que los alumnos cumplan con una asistencia igual o superior al setenta y cinco por ciento (75%). Cuando la asistencia a clase fuese inferior al setenta y cinco por ciento (75%) y superior al cincuenta por ciento (50%), indefectiblemente deberán aprobar una evaluación complementaria que podrá asumir diversos formatos (exámenes escritos, monografías, trabajos prácticos, etc.) como condición previa para rendir el oral.

5.- METODOLOGÍA DE TRABAJO Y ENSEÑANZA:

Se utilizarán estrategias didácticas, técnicas participativas que favorezcan el aprendizaje de los estudiantes.

Lo multidisciplinario de esta materia amerita para contar con profesores invitados.