MANUAL DE INFORMÁTICA FORENSE

(Prueba Indiciaria Informático Forense)

Bases Metodológicas: Científica, Sistémica, Criminalística, Tecnológica-Pericial y Marco Legal

INCLUYE ACTUALIZACIÓN ON-LINE

María Elena Darahuge
Luis E. Arellano González

Prólogo del Dr. Ricardo Guibourg

ERREPAR

MARÍA ELENA DARAHUGE
LUIS E. ARELLANO GONZÁLEZ

MANUAL DE INFORMÁTICA FORENSE

(PRUEBA INDICIARIA INFORMÁTICO FORENSE)

Bases metodológicas: científica, sistémica, criminalística, tecnológica-pericial y marco legal

Darahuge, María Elena
Manual de informática forense : prueba indiciaria informático forense / María Elena Darahuge y Luis Enrique Arellano González. - 1a ed. - Ciudad Autónoma de Buenos Aires : Errepar, 2014.

E-Book.

ISBN 978-987-01-1681-3

1. Informática. I. Arellano González, Luis Enrique II. Título
CDD 001.5

Manual de informática forense

Fecha de catalogación: 19/06/2014

ERREPAR S.A.
Paraná 725 (1017) - Buenos Aires - República Argentina
Tel.: 4370-2002
Internet: www.errepar.com
E-mail: clientes@errepar.com

ISBN: 978-987-01-1681-3

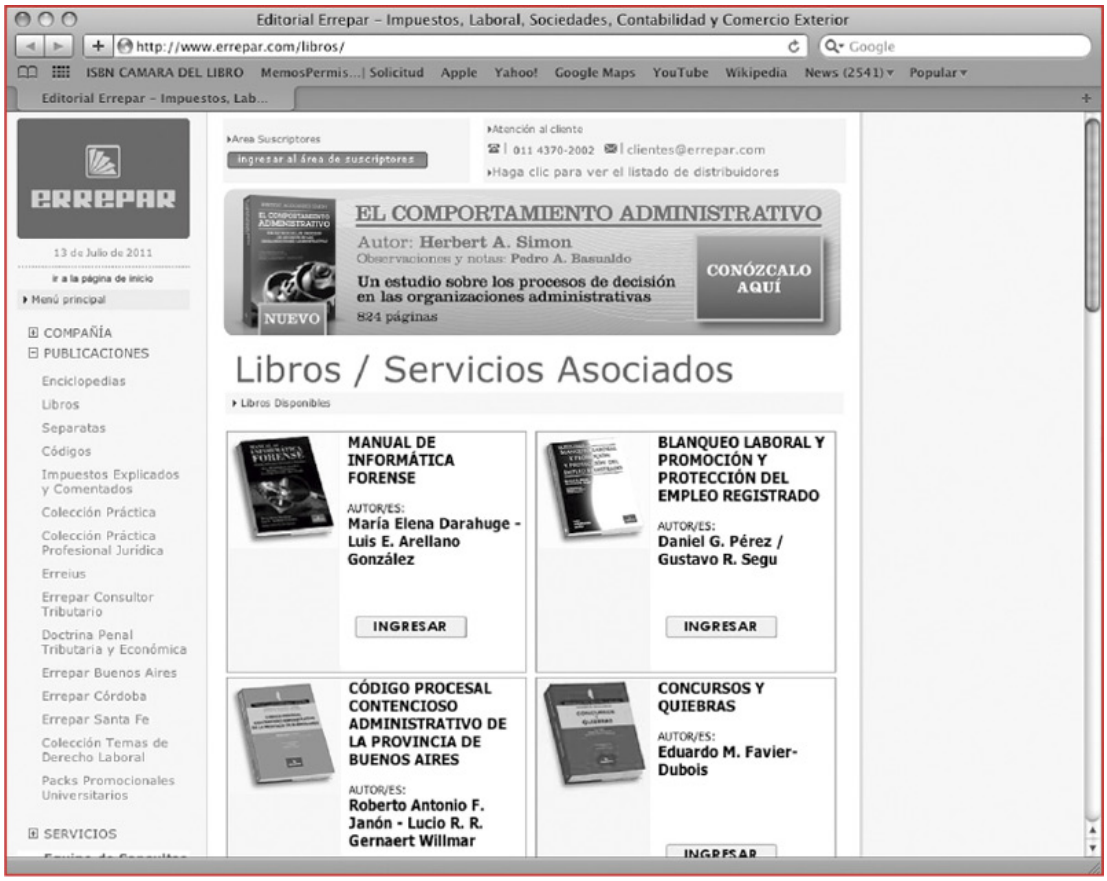
Nos interesan sus comentarios sobre la presente obra:
editorial@errepar.com

Digitalización: Proyecto451

ACTUALIZACIÓN ON-LINE

El contenido del presente libro se actualiza por Internet a través de nuestra página web.

Deberá ingresar a www.errepar.com/libros.



Seleccione la presente obra presionando el botón Ingresar, visualizará la siguiente pantalla:

La primera vez que intente consultar el material tendrá que registrarse como usuario, para lo cual se le pedirá que ingrese la clave de de acceso (22462691) y que complete una serie de datos personales.

Tenga presente que es muy importante que ingrese correctamente su dirección de correo electrónico, debido a que allí se le enviará su usuario y contraseña para acceder a los servicios asociados al libro.

Finalmente, presionando el icono correspondiente, tendrá acceso a las actualizaciones de esta obra.

LOS AUTORES

Prof. Ing. María Elena Darahuge
Licenciada e Ingeniera en Informática.
Profesora Universitaria en Ingeniería en Informática, UCSA.
Secretaria Académica del Curso de Experto en Informática Forense, FRA (UTN).
Profesora Asociada de la materia Sistemas Operativos, UAJFK.

Prof. Ing. Luis Enrique Arellano González
Abogado con orientación Penal, UBA.
Licenciado e Ingeniero en Informática.
Profesor Universitario en Ingeniería en Informática y en Criminalística, UCSA.
Licenciado en Criminalística.
Perito en Documentología, Balística y Papiloscopía, IUPFA.
Director del Curso de Experto en Informática Forense, FRA (UTN).
Profesor Asociado de la materia Sistemas Operativos, UAJFK.

Índice de contenido

CAPÍTULO 6. INFORMÁTICA FORENSE - LA PRUEBA DOCUMENTAL INFORMÁTICA

- Principios y relaciones periciales informático forenses
- La prueba documental informática
- Definición y relaciones
- Inteligencia estratégica
- La entrevista

CAPÍTULO 7. INSERCIÓN LEGAL DEL PERITO EN INFORMÁTICA FORENSE - LA INSPECCIÓN JUDICIAL

- Generalidades
- Legalidad de la requisitoria pericial
- Entorno legal del perito
- Formalidades de la aceptación del cargo
- Diligencias previas en el Juzgado
- Requisitos legales y formales de la inspección judicial
- Artículos pertinentes del Código de Procedimientos Penal de la Nación (CPPN)
- Responsabilidad legal del perito informático forense: posesión, protección, análisis, preservación y devolución de la prueba
- Legislación de fondo, el perito como testigo y el falso testimonio
- Legislación de forma
- Legislación complementaria, leyes y proyectos
- Jurisprudencia

CAPÍTULO 8. ACTIVIDADES PERICIALES COMPLEMENTARIAS

- La aceptación del cargo
- El informe pericial informático forense impreso y virtual
- El párrafo de presentación
- El objeto de la pericia y los puntos de pericia (tarea transdisciplinaria)
- Los elementos ofrecidos (equipos, programas, indicios y rastros)

Entradas de directorios
Nivel de clasificación y almacenamiento del nivel de aplicación
Análisis de particiones de los discos duros
Herramientas
En Windows XP
En Windows
Análisis de los datos de las unidades de CD-R y CD-RW - DVD y dispositivos con memoria flash
Visualización de diferentes tipos de archivos
Búsqueda de texto y palabras claves
Análisis del espacio no utilizado o no asignado
Áreas del sistema de archivo que contienen datos borrados o eliminados
Espacio no asignado
Eliminación o borrado de información en el disco rígido
Listar los directorios ocultos de la papelera
Estructura de INFO2.
Eliminación segura de los datos
Análisis de datos ocultos
Tipo: Enmascaramiento
Archivos protegidos con claves
Tipo: ocultamiento de información
Herramientas
Espacio no asignado, desperdiciado y libre
Tipo: Alteración del entorno
Herramientas
Código malicioso o *Malware*
Métodos de invasión o ataque
Modos de control de la invasión o ataque
Modo de distribución o impregnación
Objetivos del código hostil
Análisis del correo electrónico
Características del encabezado de los mensajes
Descripción del encabezado

Aspectos importantes a considerar en el análisis del encabezado del mensaje
Herramientas para el análisis del encabezado de correo electrónico
Visualización de encabezados en diferentes clientes de correo electrónico
Verificación de los archivos de impresión
Análisis de código malicioso
Sitios de programas antivirus con la descripción de los distintos tipos de virus:
Herramientas de Antivirus
Herramientas de control remoto
Herramientas exploradoras de red y de vulnerabilidades
Herramientas rastreadoras de la red o sniffers
Herramientas detector de DDoS (denegación distribuida de servicio)
Herramientas bombas lógicas y bombas de tiempo
Herramientas para el Registro de las acciones efectuadas por teclado y/o mouse
Herramientas para eliminación de huellas
Procedimiento
Análisis de celulares, PDA, GPS
VI - Cotejo, correlación de datos y conclusiones
Técnicas posibles a utilizar para el cotejo y correlación de los datos
Procedimiento para el cotejo y correlación de los datos
Procedimiento para la elaboración de las conclusiones
Elementos a cotejar y correlacionar
Fecha y hora
Tablas de enrutamiento
Tabla ARP
Tabla de procesos activos
Tipo de sistema operativo
Sistemas de Archivos

- Informática Forense
- Sistemas operativos – Protocolos y redes - Seguridad informática
- Investigación
- RFC – Request for Comment
- Normas

Internet

- Fraudes, delitos informáticos y crimen en el ciberespacio
- Seguridad informática
- RFC y estándares
- Auditoría
- Códigos de ética
- Jurídica
- Colegio de abogados
- Criminalística
- Grupos de discusión
- De interés general

PRÓLOGO

Hacia 1970, cuando empecé a interesarme en ella, la Informática era casi un tema de ficción científica. En las películas aparecían enormes máquinas llenas de luces intermitentes y carretes de cinta de movimiento espasmódico, a las que se atribuían poderes enormes, a ratos divinos, a menudo diabólicos. Vincular esas máquinas con el derecho era un verdadero desafío; no tanto técnico informático, sino técnico jurídico. En efecto, las computadoras siempre pudieron dar de sí mucho más que lo que los hombres de derecho fuimos capaces de pedirles. La persistente brecha entre estas dos variables obedeció a varios factores: uno, la aversión que la mayoría de los abogados sienten por las matemáticas y el temor de que un día las máquinas lleguen a reemplazarlos, utopía negativa que suelen comentar en términos de excelsitud del hombre, libre albedrío, irracionalidad de lo inanimado y otras referencias metafísicas. Otro factor consiste en el retraso epistemológico que afecta al conocimiento jurídico que –más allá de la evolución de sus contenidos– nunca tuvo su revolución copernicana y se encuentra hoy casi en el mismo punto donde lo dejó el emperador Justiniano en el siglo VI de nuestra era.

El desafío, pues, no giraba entonces en torno de la programación sino del modo de representar aquello que pudiera llamarse realidad jurídica. Era un tema apropiado para la filosofía del derecho y, al tratar de encararlo racionalmente, trabé relación y amistad con especialistas que se aproximaban también desde la elaboración de *software*, desde la recopilación de datos y desde la

administración de justicia, pero también desde lo que aparecía como una nueva rama del derecho: el derecho informático, que muchos confundían entonces con la informática jurídica. Yo trataba de distinguirlos: una cosa –decía– es ser el abogado de un psicoanalista y otra distinta ser el psicoanalista de un abogado.

Todo aquello ha quedado en la historia de una época que –con escasa autocrítica– se me antoja heroica. La informática jurídica avanzó mucho en sus aspectos documentales y de gestión, pero sigue retrasada (por los motivos ya apuntados) en el ámbito decisorio, que es el más fascinante. Sin embargo, gracias a la difusión de computadoras personales y portátiles, en los últimos veinte años la Informática pasó a formar parte imprescindible de la vida de cualquiera y las computadoras se convirtieron en eficaces máquinas de pensar auxiliares, acopladas a nuestros cerebros por medio de teclados, ratones y monitores.

El hecho de que las computadoras formen parte de la vida cotidiana trajo consigo que, como los automóviles, los teléfonos y las armas de fuego, sirvieran también para cometer delitos o para contener indicios de actos ilícitos cometidos en cualquier rama de la actividad humana. Y, así como los médicos legistas escudriñan los cadáveres, los expertos en balística examinan las estrías de los proyectiles o anónimos funcionarios controlan las comunicaciones telefónicas de los sospechosos, aparecieron los peritos informáticos, capaces de buscar información en una computadora secuestrada, restaurar archivos borrados de un disco duro o verificar la autenticidad de un intercambio de correos electrónicos.

Esta nueva especialidad de la criminalística, que se ha vuelto indispensable para el procedimiento judicial, no es cosa sencilla. Requiere un profundo conocimiento de los elementos técnicos materiales e inmateriales, ingenio para extraer de ellos la información requerida venciendo

disfraces y disimulos, una cuidadosa revisión de las condiciones que permitan preservar el valor probatorio de esa información y un certero modo de vincular toda esta actividad con las necesidades legales del proceso que las requiera.

Todo esto está presente en el preciso y completo manual que han preparado mis amigos María Elena Darahuge y Luis Enrique Arellano González, expresado en nuestro idioma y con la claridad que es la cortesía del intelecto. Aunque muchas de las precisiones técnicas que contiene son ajenas a mi propia experiencia, considero un honor presentar el libro como un valioso instrumento para la investigación de los hechos a partir de los vestigios informáticos.

Ricardo A. Guibourg
Buenos Aires, marzo de 2011

“Dicere etiam solebat nullum esse librum tam malum
Ut non aliqua parte prodesset”. (1)
Plinio el Joven (Epístolas III)

PREFACIO

Cuando a principios del año 2004 comenzamos a reunir información para iniciar el dictado de un Curso de Informática Forense, con carácter informativo, para todo tipo de profesionales, en la Regional Avellaneda de la Universidad Tecnológica Nacional, advertimos una serie de eventos que finalizaría en la planificación y redacción de este manual. Las circunstancias que nos llevaron a ello pueden sintetizarse en:

- La mayoría de la bibliografía consultada era de origen estadounidense o europeo, casi en su totalidad en inglés, en menor cantidad en otros idiomas y escasamente en castellano.
- Las obras referidas consistían en descripciones generales de las técnicas relacionadas con la Informática Forense, obras anecdóticas con algún sentido práctico, o descripciones de operación de algunas herramientas específicas (con su correspondiente origen y marca registrada), que las convertían en manuales de dichas herramientas.
- No aparecían obras orientadas a generar un análisis conceptual, metodológico, formal y estricto de la Informática Forense como especialidad de las Ciencias Criminalísticas.

- Por otra parte aparecía una gran cantidad de herramientas sin clasificación ni orden aparente, entre los programas ofrecidos al respecto por la comunidad de *Software Libre* (entorno Linux).
- Se tornaba evidente la necesidad de efectuar una recopilación ordenada y sistemática de los distintos componentes detectables en la comunidad pericial, a efectos de aportar entidad metodológica, científica, criminalística, informática y legal a la nueva disciplina surgida de hecho y aún no formalizada de derecho.

En nuestro país, se han producido diversos intentos para normar la conducta delictiva informática, representada por las leyes 25.506, de Firma Digital y 26.388 de Delitos Informáticos. Sin embargo es muy poco lo que se ha avanzado desde aquel momento citado hasta la fecha, en lo que hace al Derecho Procesal. Algunas jurisdicciones han evolucionado más que otras integrando nuevas formas de notificación y consulta de expedientes, avanzando hacia el expediente digital (sueño de todo operador del derecho). Muy poco es lo que se puede encontrar en el Derecho Internacional, en particular en el Derecho Privado, a pesar de que muchos contratos entre exportadores e importadores de productos en especial regionales, se celebran por medio de intercambio de mensajes de correo electrónico, lo que se está haciendo extensivo al área comercial de las autopartes y otros emprendimientos similares. En cuanto al tratamiento específico de la Prueba Documental Informática, su confirmación por medio de la Prueba de Informes y su revisión por la Prueba Pericial Informático Forense, la disciplina se encuentra muy lejos de estar adecuadamente inserta en el Sistema Judicial y convenientemente normalizada mediante el uso de protocolos claros, fáciles de implementar y útiles en el apoyo a la decisión judicial (objetivo principal de toda prueba pericial).

Recordando que en un momento crítico de nuestra formación profesional hemos recurrido a obras simples, integradoras, pero sumamente esclarecedoras, como el *Manual de Criminalística* de Roberto Albarracín, que tan útil nos fuera en nuestra aproximación a la investigación del delito. Aproximación que luego debíamos orientar con obras específicas como *El ABC del Dactilóscopo* de Ricardo Rosset y Pedro Lago. Pensamos que era necesario conformar un texto de apoyo al perito informático forense que le permitiera actuar de manera profesional, unificando los perfiles mínimos pretendidos para esta actividad en apoyo de la investigación delictiva. Sus componentes principales debían incluir:

- **Un Marco Científico**, que le facilite realizar sus investigaciones y experiencias, apoyado estrictamente en el método científico. Asimismo debería aportarle las estructuras lógicas necesarias para justificar sus fundamentaciones de manera estricta e irrebatible, más allá de la fluidez argumentativa propia de cada profesional.
- **Un Marco Criminalístico**, a partir del cual pueda interrelacionarse con los restantes especialistas del área, interactuar con éstos, trabajar en forma mancomunada y en lo posible arribar a conclusiones coherentes desde todas las visiones específicas. De la misma forma en que la Medicina Legal es una especialidad de la Medicina imbuida de un amplio contenido Criminalístico y Legal (especialmente desde el Derecho Procesal), la Informática Forense es una disciplina Informática con las mismas características propias.
- **Un Marco Informático general**, a partir de las metodologías de Análisis de Sistemas, que le permitan utilizar aquellas herramientas de uso general que se adapten a las actividades periciales informáticas. En ese sentido, las etapas de relevamiento de información y desarrollo de un modelo coherente de análisis, se

evidencian como instrumentos adecuados para brindar soporte metodológico a la actividad del experto en Informática Forense.

- **Un Marco Informático específico**, en relación con las herramientas propias del tratamiento de la prueba indiciaria informático forense. Al respecto es dable destacar que éstas deben ser abordadas desde los dos ambientes más frecuentes en uso en nuestra sociedad, el de *software libre* y el de *software propietario*, más allá de sus características de pago o gratuito.
- **Un Marco Legal** abarcativo de las distintas actividades periciales a desarrollar. Esto implica la inserción legal del accionar pericial al concurrir al lugar del hecho (a requerimiento de un Tribunal, o de un cliente, con orden judicial que lo avale o sin ella), al realizar una inspección ocular, al documentar y secuestrar elementos probatorios, su responsabilidad respecto de la prueba indiciaria que se le ha confiado en custodia, los cumplimientos de los plazos legales, su condición de testigo experto, los artículos de los códigos de fondo y de forma que lo protegen o lo limitan y la interacción resultante de su presentación ante los distintos Fueros Judiciales.
- Los puntos anteriores, se verían reflejados en un informe pericial:
  – Científicamente fundamentado.
  – Criminalísticamente interrelacionado.
  – Modelado mediante técnicas propias del Análisis de Sistemas.
  – Investigado con las mejores herramientas disponibles.
  – Inserto en el marco legal correspondiente.
- No obstante y teniendo en cuenta la actual tendencia judicial hacia la metodología de juicio oral, no es suficiente con una fundamentación técnica adecuadamente implementada para defender un informe pericial. Hacen falta técnicas de argumentación,

redacción y oratoria contundentes, precisas e irrebatibles. De ahí la necesidad de recomendar la capacitación del profesional en el arte de la redacción y la oratoria que le permitan realizar una adecuada defensa oral y escrita de sus resultados periciales, ante posibles impugnaciones o pedidos de aclaración.

Estamos seguros de no haber podido realizar una obra adecuada a las pretensiones anteriores, pero también podemos asegurar que se trata de un punto de partida, disperso, con fallas, criticable y perfectible, pero punto de partida al fin.

---

1. “Se dice que no hay libro malo donde no se halle alguno bueno...”

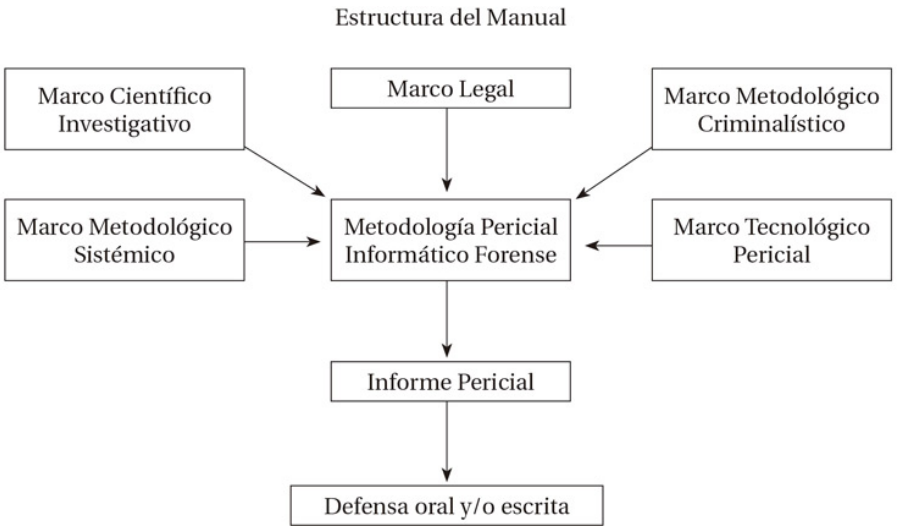
“Criminalística es la metodología integradora multidisciplinaria que provee la información tendiente al esclarecimiento del hecho, a partir de los indicios recolectados (prueba indiciaria).”

“Prueba indiciaria es la prueba integrada por el conjunto de elementos físicos y virtuales, que obran en un lugar determinado, necesarios y suficientes para efectuar una reconstrucción lógica, científica, tecnológica y técnica de los hechos investigados, por medio del correspondiente análisis pericial forense.”

“Informática Forense es el conjunto muldisciplinario de teorías, técnicas y métodos de análisis, que brindan soporte conceptual y procedimental, a la investigación de la prueba indiciaria informática.”

CAPÍTULO 1

ESTRUCTURA GENERAL



Este trabajo ha sido planificado y desarrollado con el objeto de aportar al perito informático forense una guía de referencias y consultas rápida, sencilla y fundamentada especialmente en la inter y transdisciplinariedad que este tipo de tareas implica.

Pese a lo novedoso de esta especialidad, es indudable que los fundamentos que la sustentan ya existían con anterioridad a su implementación práctica. La Metodología Pericial Informático Forense es alimentada, soportada y justificada por otras ciencias y técnicas precedentes, que aportan a la tarea pericial distintos entornos específicos entre los que debemos destacar:

1. **Marco Científico Investigativo:** El método científico se constituye en una herramienta fundamental de análisis para toda tarea tecnológica de investigación.

2. **Marco Metodológico Sistémico:** El Análisis de Sistemas nos aporta los elementos necesarios para realizar un análisis de la información estructurado y estricto, relacionado con las estructuras de datos analizadas y las arquitecturas involucradas.
3. **Marco Metodológico Criminalístico:** La prueba indiciaria como fundamento de la investigación criminal ha sido identificada como la reina de las pruebas y se ha utilizado de manera sistemática durante la totalidad del siglo pasado. Su eficiencia ha sido harto probada, sus defectos detectados y corregidos. Constituye la base indiscutible de la tarea pericial, incluyendo a la pericia informática forense entre sus disciplinas derivadas y determinando las relaciones interdisciplinarias derivadas de la interacción pericial en el lugar del hecho (real o virtual, propio o impropio) o la gestión y análisis de la prueba involucrada.
4. **Marco Tecnológico Pericial:** Si bien la pericia informática forense se encuentra integrada, respaldada y justificada en la investigación criminalística en general, debe su existencia individual a una metodología específica y diferente de las demás. Se apoya en herramientas, métodos y técnicas propios y actúa sobre una prueba indiciaria, que posee características particulares que la diferencian notoriamente de las restantes pruebas indiciarias, analizadas por otras disciplinas criminalísticas.
5. **Marco Legal:** La pericia informática forense, por su orientación específica a la investigación reconstructiva, de transgresiones que pueden o no constituir ilícitos de diferente naturaleza (penal, civil, comercial, contractual, particular), involucra una enorme gama de actores y relaciones de todo tipo. Es inevitable el análisis metodológico ordenado y estricto de la legislación relacionada con ésta en cada caso particular, no es posible describirlos a todos en una obra como la