ÍNDICE

6 ASPECTOS PROFESIONALES DEL INGENIERO INFORMÁTICO

- ***ASPECTOS PROFESIONALES DEL INGENIERO INFORMÁTICO***

En el presente tema vamos a estudiar los aspectos que cualquier Ingeniero en Informática debería conocer de cara a una incorporación al mercado profesional, y que definirán en muchos casos el éxito de los proyectos/trabajos que se le encomienden. Entre estos aspectos están las consideraciones éticas y legales que un Ingeniero Informático ha de seguir a la hora de desempeñar su actividad. Además se comentan los tipos de trabajos profesionales que un Ingeniero Informático puede desempeñar por el hecho de poseer la titulación correspondiente.

- ***ÉTICA INFORMÁTICA***
- ***DEFINICIÓN***

Primero, debiéramos considerar el concepto de ética. La ética es el campo de estudio que se preocupa de las cuestiones de valor, es decir, juicios acerca de que comportamiento humano es bueno o malo en cualquier situación dada. La ética es los estándares, valores, principios morales, etc. que cada uno usa en sus decisiones o actos; normalmente no hay una respuesta bien definida sobre lo que es bueno o malo.

Los juicios éticos no son muy diferentes en el área de la informática de los de cualquier otra área, porque la informática implica problemas de privacidad, autoría, robo y abuso, por poner algunos ejemplos.

En una sociedad en la que el ordenador cobra cada vez más un papel importante, y dado el importante crecimiento de Internet y el gran desarrollo en las áreas de las técnicas de la información y la informática, es necesario establecer una serie de normas que rijan el comportamiento profesional de los futuros doctores, licenciados o ingenieros informáticos.

La tecnología informática plantea nuevas situaciones y nuevos problemas y gran parte de estas nuevas situaciones y problemas son de una naturaleza ética; obviamente existen intentos de resolver estos problemas aplicando las actuales reglas y soluciones éticas de carácter general, por ello es importante echar la vista al pasado en busca de mejores valores éticos tradicionales. Las TIC (Tecnologías de la Información y de las Comunicaciones) cambiarán el mundo que conocemos actualmente, y desde el punto de vista ético, lo más importante y evidente es la necesidad de una nueva ética. Esta nueva ética será la *ética de la informática*.

- ***CARACTERÍSTICAS PRINCIPALES***

Ciertamente hay algunas consideraciones que hacen que la ética informática sea diferente al del resto de éticas profesionales:

- Existen injerencias externas, por parte de personas que no son profesionales informáticos, pero que asumen ese cargo son la debida preparación. Además, la informática está orientada al usuario, se intenta por todos los medios facilitarle el uso o la instalación del producto informático, por lo que debe ser una ciencia bastante tolerante a errores. Si un usuario utiliza un producto informático de forma indebida, no está claro quien es el responsable. Esto es un problema moral para el informático.
- Además existen posibles conflictos con otras ciencias o profesiones. Por ejemplo, en el caso de Internet y la necesidad de un medio libre de interferencias, puede ser necesaria la restricción de los contenidos de la Red, puesto que pueden existir contenidos en la Red que ataquen la moral de algún usuario, o puede que la publicación de ciertos programas atente contra el derecho a la propiedad individual.

El hecho de que la informática este tan presente en nuestras vidas, tanto social como profesionalmente, hace que sea tan importante establecer unas pautas de comportamiento, que no sólo proteja a los usuarios sino que también ayude a los informáticos en su trabajo.

- ***DEFINICIÓN PROFESIONAL DE UN INFORMÁTICO***

Debido a esta profunda relación con el usuario se debe marcar claramente los límites de los informáticos:

En España, en el ámbito jurídico, existe la responsabilidad civil profesional que contribuye a definir normas aplicables a su ejercicio, pero el control del ejercicio de la profesión no está controlado por organizaciones profesionales con personalidad jurídica como puede ser el Colegio de médicos o el Colegio de abogados. Por otra parte, dicho reconocimiento de la corporación profesional ha sido ampliamente demandado por los profesionales de la informática, pero ésta debe superar diversos problemas institucionales, políticos y económicos y hoy, en 1999, todavía, lamentablemente, no es una realidad. La pregunta que cabe hacerse para poder llegar a una ética y una deontología del informático, es si esa profesión está reconocida como tal en el ordenamiento legal de cada país. Hablaremos solamente de España, entendiendo que la mayoría de las consideraciones en el ámbito español son extrapolables en general a cualquier otro país occidental.

En España no existe reconocimiento legal de la profesión, como está establecida para los médicos, abogados, ingenieros, enfermeros o economistas, por citar algunas profesiones significativas. Existen algunas asociaciones profesionales de carácter general, pero cuyas atribuciones no llegan a ser las de los colegios profesionales, aunque no dejan de ser asociaciones profesionales de mayor o menor prestigio, pero centradas en la formación, investigación, etc., de sus miembros, si bien tratan de luchar por conseguir la colegiación como fin último. A destacar: **ALI** (Asociación de Licenciados en Informática) y **ATI** (Asociación de Técnicos en Informática) de marcado carácter profesional; **AEIA** (Asociación Española de Informática y Automática) de marcado carácter universitario y científico. El reconocimiento del *status* profesional es algo complicado por diversas razones, que vamos a analizar a continuación:

El primer problema importante es el planteado por la imprecisión y la extensión del campo o competencias profesionales; la informática, fundamentalmente, es una técnica que está introducida en todas partes y que recurre a niveles de conocimientos muy dispares, que van desde el usuario al diseñador o ingeniero de software/sistemas, pasando por el operador (cada vez mas confundido con el de un usuario de PC), programador, analista o especialista en *interfaz* hombre/máquina (a este panorama hay que añadir todos los puestos de trabajos relacionadas con la informática distribuida, las intranets e Internet). Esto implica que el campo de prácticas informáticas no es monopolio exclusivo de los informáticos, ya que en la profesión − si no se define adecuadamente − caben casi todas las personas que usan un PC con fines profesionales. De hecho, a la informática se puede acceder desde numerosas carreras y centro/escuelas profesionales/universitarios, que van desde FP−II y FP−III en Administración, Electrónica e Informática, hasta físicos, ingenieros industriales, ingenieros de telecomunicación, matemáticos junto con licenciados/ingenieros en informática o diplomados/ingenieros técnicos en informática. Y eso sin tener en cuenta el número de personas que, procediendo de estudios o carreras no vinculadas a la informática y/o las telecomunicaciones, se han formado en plan autodidacta o en centros y academias privadas o pertenecientes a las grandes casas comerciales, y que en función de su formación original han sido recicladas en las nuevas tecnologías de la información. Esta situación no se da en ninguna de las profesiones reconocidas que requieren un título para el ejercicio, libre o no, de la profesión; circunstancia ésta, que hace que la problemática de la profesión sea especialmente complicada y que por el momento no pueda decirse como va a resolverse e incluso si llegara a una solución análoga a la de otras profesiones más tradicionales e institucionalizadas. Añadamos que esta situación está más definida en el campo de las comunicaciones, lo que hace que un campo tan actual como es la actividad profesional de la telemática esté en estos momentos carentes de un marco colegial.

El segundo problema, íntimamente relacionado con el anterior, es de naturaleza política: en caso de existir una relación en cuanto a asociaciones profesionales, ¿quién puede pertenecer a la asociación que concede el *status*

de la profesión? En la mayoría de las asociaciones españolas y extranjeras, el criterio de admisión es la posesión de los conocimientos requeridos para ejercer la actividad. Estos conocimientos se acreditan generalmente por el título FPII, FPIII, Diplomatura/Ingeniería Técnica y Licenciado/Ingeniero en Informática, pero en España, tanto las empresas como la Administración, contratan en muchos casos a titulados de otras profesiones si acreditan experiencia práctica en el campo informático que demandan.

La tercera pregunta es de orden económico: *¿Qué privilegios tendrán los miembros de la profesión informática?* Es también de difícil definición y aplicación. El título de informático profesional o informático se adecua a realidades de prácticas muy diversas. ¿Cómo se puede impedir a una persona, calificada o no, declararse consultor en informática? Por otra parte, muchas profesiones con diploma universitario o no, exigen el uso de herramientas informáticas, por ejemplo ingenieros de caminos, o arquitectos que realizan sus cálculos con programas de *software* propios o adquiridos en el mercado, o los contables y gerentes que proceden a la verificación informática de sus cálculos sobre la base de normas reconocidas en la profesión.

- ***ASPECTOS DE LA ÉTICA INFORMÁTICA***

Comercio:

1.1. Fraude.

1.2. Tácticas monopolísticas (Trust, Microsoft,...)

1.3. Spamming.

1.4. Impuestos.

1.5. Libre comercio.

Abuso informático:

2.1. Hackers.

2.2. Gusanos, caballos de Troya y virus.

2.3. Spamming.

Propiedad intelectual:

3.1. Leyes de Copyright y patente.

3.2. Copyright electrónico.

3.3. Piratería del software.

Privacidad:

4.1. Privacidad de las bases de datos.

4.2. Privacidad del correo electrónico.

4.3. Privacidad en la Red.

4.4. Encriptación.

4.4.1. Chip de recorte.

4.4.2. Regulaciones en la exportación.

4.5. Anónimo.

4.6. Spamming.

Riesgos:

5.1. Licencias.

5.2. Modelos de ordenadores.

5.3. Inteligencia artificial.

5.4. Software a prueba de fallos.

5.5. Seguridad en las redes.

5.6. Seguridad del software.

Consecuencias Jurídico−sociales:

6.1. Igualdad de acceso.

6.1.1. Igualdad de clase.

6.1.2. Igualdad de sexo.

6.1.3. Acceso para los discapacitados.

6.2. Consecuencias laborales.

6.3. Entresijos de la Era de los ordenadores.

Consecuencias de la expresión en la red.

7.1. Netiquette. (Modales o etiqueta en la red).

7.2. Libertad de expresión:

7.2.1. Pornografía.

7.2.2. Discriminación.

7.2.3. Filtros de Internet.

7.3. Anónimo.

7.4. Privacidad en el correo electrónico.

7.5. Cartas encadenadas.

Hay aspectos como la privacidad del correo electrónico (e−mail) que abarcan desde aspectos sociales, hasta aspectos comerciales, bien por la posibilidad de ser interceptados por terceras personas y constituir una violación de tu derecho a la intimidad, bien porque se pasan datos de la persona (como la dirección e−mail) a otras empresas, sin haberlo consultado con la persona afectada.

Spamming son aquellos ataques malintencionados e indiscriminados que se realizan, bien en la red por medio de cartas bombas, bien por la constante intromisión en la intimidad de cada persona, mediante programas que obtienen datos de la persona, bien por la destrucción de datos necesarios para esa persona.

Como se ve bien claramente, la ética informática abarca necesariamente al usuario, puesto que es él el que al hacer uso de su producto, debe respetar a las demás personas y/o usuarios, así como a los informáticos que han hecho posible que pueda disfrutar de su uso.

Por otra parte, es motivo de reflexión la creciente inquietud que surge entre los usuarios por el monopolio creado por las grandes compañías, que obligan a comprar sus productos para que el usuario tenga una mediana seguridad de compatibilidad con el resto de componentes informáticos de su equipo. A este respecto se están llevando a cabo procesos judiciales para evitar el abuso de las grandes compañías, que no solo obligan al usuario, sino que además impiden que otras compañías se abran paso en el sector informático, si no es bajo sus condiciones. Este aspecto es por lo demás parte del derecho informático, pero su vertiente moral estaría reflejada en la necesidad de hacer un producto informático que sea adaptable a los diferentes sistemas que pueda poseer el usuario, sin necesidad de imponer unas determinadas condiciones o productos de unas determinadas compañías.

- ***CÓDIGOS ÉTICOS***

El primer código ético que viene a la cabeza de cualquier persona es el juramento hipocrático de los médicos; esta es la primera referencia que se encuentra uno al indagar sobre códigos morales. En general se puede definir un código moral simplemente con la norma de realizar su trabajo tal que lo haga lo mejor posible y con ánimo de mejorar. Cualquier profesional desea mejorar en su profesión, y no solo por ofrecer un mejor servicio a sus usuarios sino por el afán de aprender y mejorar, es decir, por orgullo profesional.

- ***CÓDIGO ÉTICO DE LA ACM***

El código ético de la ACM (Association of Computer Machinery) es uno de los puntos de referencia para cualquier profesional informático, que podemos observar en el Anexo IX.

- ***CÓDIGO DEONTOLÓGICO DE LA ALI***

La Asociación de Doctores, Licenciados e Ingenieros en Informática (ALI) es la asociación española más importante (junto con la ATI) en lo que se refiere al mundo profesional de los Informáticos y posee un código deontológico propio, que reproducimos a continuación:−−>[Author:RVH]

La Asociación de Doctores, Licenciados e Ingenieros en Informática (ALI) proclama este código de ética profesional como norma de conducta de los miembros de la Asociación, en particular, y de los titulados Superiores en Informática, en general, en el desempeño de su labor profesional, comprometiéndose, así mismo, a la persecución y denuncia de aquellas prácticas o actividades profesionales que vulneren el espíritu del presente Código Deontológico o que afecten al prestigio y reconocimiento de nuestra profesión.

El titulado superior en informática, desde el desempeño de su actividad profesional...

- *. Trabajará siempre de forma honesta y leal, y nunca participará de forma consciente en actividades ilegales o impropias de su labor profesional. Respetará el cumplimiento de todas las normas y leyes, actuales y futuras, que afecten al ejercicio de nuestra profesión y las actividades que de ellas se deriven.*
- *. Efectuará su trabajo de forma objetiva e independiente, evitando ejercer actividades que puedan afectar su independencia de forma supuesta o real, especialmente cuando de su trabajo dependan decisiones de otros.*
- *. Mantendrá la confidencialidad de la información a la que tenga acceso por razón de su cargo o desempeño profesional, y no podrá utilizarla en beneficio propio o de terceras personas.*
- *. Respetará en todo momento la propiedad intelectual de terceros, garantizando la integridad de los productos y servicios bajo su responsabilidad.*
- *. Procurará obtener y documentar de forma suficiente los estudios o trabajos en los que base sus conclusiones y recomendaciones.*
- *. Garantizará que los sistemas de información a su cargo cumplan las normas, procedimientos y controles que aseguren su correcto funcionamiento.*
- *. Combatirá la creación, introducción o presencia de elementos que puedan poner en peligro de forma premeditada la seguridad de los sistemas de información.*
- *. Ajustará sus ingresos derivados de su actividad profesional de forma razonable y proporcional al trabajo desempeñado, y no se aprovechará del desconocimiento tecnológico de los destinatarios del mismo para conseguir un beneficio deshonesto o ilegal, propio o de terceros.*
- *. Mantendrá su nivel de competencia profesional con la participación en las actividades de desarrollo adecuadas que dedicará siempre para obtener la máxima calidad de su trabajo.*
- *. Trabajará desde su ejercicio para que el avance científico y profesional redunde en el progreso hacia una sociedad más justa y digna.*
- ***NORMAS DEONTOLÓGICAS DE LA ATI***

La Asociación de Técnicos de Informática es el otro gran exponente español en lo que a la profesión Informática se refiere. Posee unas normas deontológicas que ha de cumplir todo Técnico en Informática en el mundo profesional. Lo reproducimos a continuación:−−>[Author:RVH]

El miembro que acepte la designación se compromete a respetar las normas deontológicas profesionales, y en especial, se compromete a:

- *. Cumplir el ordenamiento legal que afecte al desarrollo de su misión.*
- *. Desempeñar puntual y fielmente el cometido solicitado.*
- *. Emitir juicios en conciencia y de forma objetiva.*
- *. Basarse siempre en consideraciones técnicas verificables, diferenciando siempre lo que son hechos de las opiniones y manifestándolo así.*
- *. Considerar toda la información recibida como confidencial, comprometiéndose a no utilizarla en beneficio propio, de terceros, ni en perjuicio de los afectados.*
- ***NORMAS DE LA UJI***

La Universidad Jaime Primero de Castellón fijó las normas éticas por las que se regía la utilización de la red informática que posee, que las podemos ver seguidamente (NOTA: está en Valenciano):−−>[Author:RVH]

1. En favor de les llibertats públiques.

L'UJI vol potenciar els drets individuals i les llibertats públiques recollides en la Constitució i en l'Estatut d'Autonomia de la Comunitat Valenciana. Les normes de funcionament de la xarxa pretenen fer possible aquest enunciat optimitzant l'ús d'aquest mitjà de comunicació. Aquelles situacions conflictives que tanmateix es puguen presentar, en les quals hi haja drets personals o col.lectius que es puguen veure vulnerats les

resoldrà el Defensor de la Comunitat Universitària i la Comissió Deontològica, respectivament.

2. Activitat comercial a la xarxa de la universitat

La Universitat no por utilitzar ni permetre a altres l'ús de la seua xarxa per a activitats comercials.

3. Obtenció de fons i publicitat

Només es podran fer constar els patrocinis (per requeriment explícit de beques o ajudes a la docència i la investigació) en la xarxa de la Universitat sota la seua supervisió, i serà preceptiva l'autorització de la "/uji/comss/cewww.html", Comissió Editorial.

4. Cessió de serveis de xarxa

La cessió de serveis de xarxa de la Universitat a individus o organitzacions externes només la podrà autoritzar la Universitat de manera excepcional, i en cap cas amb ànim de lucre.

5. Ús del nom de la universitat

El nom de la Univesitat no es pot fer servir sense autorització de manera que suggerisca o done a entendre que aquesta dóna suport a altres organitzacions, als seus productes, serveis, etc. A aquest efecte es recorda que l'acord de l'Equip de Govern núm. 138.5 estableix que: <<qualsevol utilització general o específica de la imatge o nom de la Universitat Jaume I, en els seus diversos aspectes, que tinga com a finalitat la difusió general de la institució o d'algun estudi, centre, servei, activitat o altres, fora de la Universitat, ha de ser aprovada i gestionada pel Servei de Comunicació i Publicacions, o d'acord amb aquest, independentment que siga gratuïta o no i de la presentació i del suport utilitzats..

6. Propietat intel.lectual

S'ha d'assumir que la major part dels materials publicats a la xarxa tenen drets d'autor si no es declara explícitament el contrari. Es poden utilitzar citacions breus si s'identifica l'autor i l'obra d'on s'han pres.

No es poden publicar a la xarxa materials que siguen propietat d'altres, és a dir, treballs amb drets d'autor, sense l'autorització explícita del seu titular (exemples: dibuixos, articles, fotografies, cançons, software, imatges digitalitzades d'obres publicades, etc.). Així ho estableix el text refós de la Llei de Propietat Intel.lectual (Reial Decret legislatiu 1/1996, de 12 d'abril) en els articles 17 i 20.2,e) .

Si es vol incloure informació que existeix en altres documents publicats al WWW, és millor fer servir enllaços que copiar−la.

7. Materials llicenciats

Cal anar amb molt de compte amb els materials llicenciats a la Universitat pels seus titulars (per exemple, articles de premsa, entrades d'enciclopèdies, etc.). L'ús d'aquests materials és restringit dins de la Universitat. Ningú té dret a incloure'ls en documents per publicar−los a la xarxa i/o redistribuir−los.

8. Dret a la intimitat i a la pròpia imatge

No es poden publicar a la xarxa informació, imatges o vídeos sense l'autorització de les persones que hi apareixen. Tothom té dret a restringir l'ús de la seua pròpia imatge.

9. Els valors de l'UJI

No es podran emetre missatges o imatges contraris als principis recollits en els Estatuts d'aquesta Universitat.

- ***CÓDIGO ÉTICO DE LA OAI***

La OAI es un órgano de coordinación entre el Consejo General de Colegios de Economistas de España y la Asociación de Doctores, Licenciados e Ingenieros en Informática al servicio de la difusión y consolidación de la actividad de la Auditoría Informática.

En lo que a su proyección internacional se refiere la OAI está vinculada con la ISACA (Information System Audit and Control Association) siendo un Capítulo (Chapter) de la citada Asociación. Uno de los aspectos más relevantes de la OAI es el ayudar a aquellos profesionales con el certificado internacional más prestigioso de auditor informático: "Certified Information System Auditor" − CISA, emitido por la ISACA.

La "Information Systems Audit and Control Foundation", Inc. Fija el siguiente Código de Ética Profesional para guiar la conducta profesional y personal de los miembros de la Asociación y/o los poseedores del título de Auditor Certificado de Sistemas de Información.

Los Auditores Certificados de Sistemas de Información deberán:

- Apoyar el establecimiento y el cumplimiento de normas, procedimientos y controles de sistemas de información.
- Cumplir las Normas de Auditoría de Sistemas de Información según las adopte la Fundación para Control y Auditoría de Sistemas de Información.
- Actuar en interés de sus empleadores, accionistas, clientes y público en general en forma diligente, leal y honesta y no contribuir a sabiendas en actividades ilícitas o incorrectas.
- Mantener la confidencialidad de la información obtenida en el curso de sus deberes. La información no deberá ser utilizada en beneficio propio o divulgada a terceros no legitimados.
- Cumplir con sus deberes en forma independiente y objetiva y evitar toda actividad que comprometa o parezca comprometer su independencia.
- Mantener su capacidad en los campos interrelacionados a la auditoría y sistemas de información mediante la participación en actividades de capacitación profesional.
- Ejercer sumo cuidado al obtener y documentar material suficiente sobre el cual basar sus conclusiones y recomendaciones.
- Informar a las partes involucradas del resultado de las tareas de auditoría que se hayan realizado.
- Apoyar la entrega de conocimientos a la gerencia, clientes y al público en general para mejorar su comprensión de la auditoría y los sistemas de información.
- Mantener altos estándares de conducta y carácter tanto en las actividades profesionales como en las privadas.

- ***JURAMENTO HIPOCRÁTICO DE CIENTÍFICOS, INGENIEROS Y EJECUTIVOS***

- Juro practicar mi profesión con conciencia y dignidad.
- Usare mis habilidades con el máximo respeto hacia toda la humanidad, la Tierra y todas sus especies.
- No permitiré que consideraciones de nacionalidad, ideas políticas, prejuicios o consideraciones materiales interfieran en mi trabajo y mi deber para con las presentes y futuras generaciones.

- Juro esto solemne, libremente y sobre mi honor.

Este juramento ha sido reproducido en la revista Astronomers and the Arms Race, P.O. Box 2218, Cambridge,

MA 02238. Ha sido recogido por Paul Codling, The Institute for Social Inventions, 24 Abercorn Place, London, England NW8 9XP. Mr. Codling ruega a aquellas personas que hagan este juramento se lo hagan saber por correo.

- ***DERECHO INFORMÁTICO***
- ***INTRODUCCIÓN***

Para encuadrar el contenido de este tema, referente a lo que debe conocer un ingeniero informático en lo que a derecho básico se refiere, conviene recordar que, en esencia, el estado puede intervenir de cuatro modos diferentes entre el propietario o proveedor de información y el usuario de la misma:

- **Proteger la información**, reconociendo el derecho de propiedad que posee su propietario. Es la función de las leyes de propiedad intelectual.
- **Evitar el uso no autorizado de información** recogida legítimamente. Éste es el objetivo de las leyes de protección de datos (especialmente datos personales y financieros).
- **Garantizar el derecho de acceso** a ciertas categorías de información de interés o beneficio para sus ciudadanos. Ésta es la función de las leyes de protección de la libertad de información.
- **Evitar la publicación o diseminación de información,** que considere va en detrimento de sus intereses. Esto puede ser por razones de seguridad, moralidad o conveniencia política. Es el área más difícil, dado que entraña el uso de la censura.

El estado se rige por leyes y tiene la capacidad de castigar a sus infractores, a nosotros nos interesaran por tanto las leyes que tienen que ver con el ejercicio de la profesión, los delitos que en su ejercicio se puedan cometer y leyes acerca del uso y/o explotación de las redes de comunicaciones, tanto de área local (*LAN*), de área metropolitana (*MAN*), o de área extensa (*WAN*), como es el caso de **INTERNET**.

El *derecho informático* es una disciplina jurídica integrada por las sentencias de los tribunales sobre materias informáticas y las proposiciones normativas, es decir, los razonamientos de la ciencia del Derecho dirigidos al análisis, interpretación, exposición, sistematización y crítica del sector normativo que regula la informática y la telemática (Diferenciemos los términos *informática jurídica* que tiene por objeto la aplicación de la informática al derecho y el *derecho de la informática*, que es nuestro interés ahora). En el concepto de derecho informático incluiremos las diferentes fuentes y estructuras temáticas en el ámbito del Derecho Público (regulación del flujo internacional de datos informáticos, libertad informática o los delitos informáticos) y del Derecho Privado (contratos informáticos, sistemas de protección jurídica de los programas de computadora, software).

El derecho informático posee idénticos títulos científicos para constituirse en disciplina autónoma como antes lo tuvieron otras materias jurídicas novedosas como, por ejemplo, el derecho *aeronáutico*, el derecho *espacial* o el derecho *comunitario*. Pueden, entre otras, aducirse las razones siguientes en favor de la sustantividad y autonomía científica del derecho de la informática.

- **a)** Existencia de un objeto delimitado constituido por la propia tecnología, cuyas implicaciones económicas, sociales, culturales y políticas son tan profundas como evidentes, hasta el punto de que el Derecho no puede desentenderse de su reglamentación. Una tecnología como la informática, que parece abocada a incidir en casi todos los aspectos de la actividad humana, forzosamente tenía que hallar su correlato normativo, pues el Derecho supone precisamente la principal técnica de organización de la vida social. De ahí que exista una demanda creciente de quienes se ven afectados por la informática, así como de quienes la utilizan, para que sus repercusiones y las relaciones que genera tenga puntual respuesta en un *corpus* completo y coherente de disposiciones capaz de responder en forma adecuada a esta nueva problemática.

Si la informática constituye el objeto inmediato del Derecho de la informática, su objeto mediato es la propia

información, que constituye un bien inmaterial, un producto autónomo y previo a todo el procesamiento y transmisión que de ella pueda realizarse. La información se desglosa en dos momentos: el primero tendente a dar forma y significado a un determinado mensaje; el segundo dirigido a su transmisión. Se trata de dos etapas de una función única que consiste en transmitir mensajes, conocimientos e ideas, es decir, la comunicación. Así, por ejemplo, los problemas que suscita la protección de los derechos de quienes han creado un programa informático, se insertan en el campo de los *derechos sobre la información*. En tanto que lo referente al flujo interno e internacional de datos y la protección de datos de carácter personal y de las libertades frente a la informática se englobaría en el *derecho a la información*. Ambos sectores conforman el objeto general del Derecho de la informática.

- **b)** Existencia de una *metodología* específica para abordar adecuadamente esta nueva disciplina jurídica. La comprensión correcta de los problemas planteados por las nuevas tecnologías de la información (informática) y de la comunicación (telemática) exige contar con unas categorías conceptuales y metódicas aptas para captar su alcance y significación.

La reglamentación jurídica de la informática deberá adaptarse a la situación de constantes cambios e innovaciones que caracterizan este sector. Por ello parece oportuno que su disciplina normativa responda a una técnica legislativa de cláusulas o principios generales. De este modo, la reglamentación a partir de unos estándares flexibles evita la necesidad de introducir variaciones constantes en las normas y permite a los órganos encargados de su aplicación adaptar los principios a las situaciones que sucesivamente se presenten. Otros aspecto que debe tenerse en cuenta es que la informática y la telemática rebasan los límites de las fronteras nacionales y, en consecuencia, el Derecho de la informática debe concebirse como un Derecho internacional, es decir, "un Derecho común a todos los países industrializados".

Al mismo tiempo el Derecho de la informática rebasa los términos de la dicotomía Derecho público/Derecho privado ya que, como se ha indicado, su problemática afecta a ambas ramas y se desglosa en normas de carácter constitucional o jurádico−fundamental (reconocimiento del derecho a la libertad informática y a la autodeterminación informática, protección de datos personales...); penal (establecimiento del aparato sancionador para punir las infracciones más graves del Derecho de la informática); civil (determinación de la responsabilidad civil de ciertas conductas de los contratos de utilización de los ordenadores, tutela del software, etc.); procesal (normas de procedimientos específicas para ejercitar las acciones que dimanan del Derecho de la informática, etc.). Esta interdisciplinariedad es un rasgo característico informador de esta rama del Derecho, si bien ello no significa que el Derecho de la informática tenga que concebirse como una amalgama de normas dispersas pertenecientes a diferentes disciplinas jurídicas, sino que entraña un conjunto unitario de reglas específicamente dirigidas a la regulación de un objeto bien delimitado que se enfoca desde una metodología propia.

- **c)** Existencia de unas *fuentes* legislativas, jurisprudenciales y doctrinales del Derecho de la informática, que en los países más avanzados han conducido a la planificación de cursos universitarios regulares encaminados a organizar su enseñanza, así como el trabajo continuo sobre el estudio de materiales normativos y que aquí vamos a tratar de resumir desde la óptica del Ingeniero Informático, dejando el resto para los profesionales del Derecho. Solamente señalar la importancia que para la sistematización y perfeccionamiento de las fuentes del Derecho de la informática corresponde a la doctrina. A ella le atañe la elaboración de esas disposiciones legales y de la jurisprudencia, así como el análisis crítico de sus eventuales lagunas, insuficiencias e imperfecciones. Urge también que la política legislativa contribuya a dotar del máximo rigor científico y técnico al sistema de fuentes del Derecho de la informática, antes de que una jungla de disposiciones dispersas y heterogéneas oscurezcan irremediablemente su estructura normativa.

En las sociedades avanzadas del presente la protección de datos personales tiende, en definitiva, a garantizar el *equilibrio de poderes y situaciones* que es condición indispensable para el correcto funcionamiento de una comunidad democrática de ciudadanos libres e iguales. Para su logro se precisa un adecuado ordenamiento

jurídico de la informática, capaz de armonizar las exigencias de información propias de un estado avanzado con las garantías de los ciudadanos. Pero estas normas de Derecho informático exigen, para su plena eficacia, impulsar la consciencia y el compromiso cívicos de hacerlas una experiencia tangible en la vida cotidiana. Es tarea de todos contribuir a evitar una paradoja dramática: compensar nuestro retraso en la incorporación al desarrollo tecnológico con la vanguardia mundial en la piratería del *software*, la delincuencia informática, y las agresiones informáticas a la libertad.

Otro tema de no dudada importancia, es la proliferación de acciones delictivas que se amparan en el vacío legal que constituyen las nuevas redes de comunicaciones que actualmente están a disposición tanto a los profesionales de la informática, como a los usuarios finales de la misma. Un gran problema al cual se enfrenta el Derecho Informático: la globalidad indiscutible de este tipo de redes, que hace de la cooperación internacional del derecho un arma cada vez más eficaz y necesitada para combatir este tipo de delitos.

Podemos observar la visión que tiene un profesional del derecho sobre la rama de esta disciplina perteneciente a la informática en el Anexo VIII.

Una vez analizados los aspectos generales del derecho informático, vamos a centrarnos en los aspectos mas significativos y afianzados, al día de la fecha, con la salvedad de que es muy posible que en los próximos años, otros capítulos hayan aparecido tan importantes o más, como los que a continuación se recogen.

- ***PROTECCIÓN A LA INTIMIDAD EN INFORMÁTICA***

Como hemos dicho más arriba, el profesional informático maneja información y ésta tiene unas connotaciones que hay que situar debidamente, una de ellas tiene que ver con el derecho a la intimidad de las personas.

- ***DERECHO A LA INTIMIDAD***

El *derecho a la intimidad*, que incluye el honor, la persona, la familia y la propia imagen, tiene en la actualidad un tratamiento jurídico de origen norteamericano: la **privacidad** (privacy), que es una libertad positiva, consistente en ejercer un derecho de control sobre los datos referidos a la propia persona, que han salido ya de la esfera de la intimidad para convertirse en elementos de un archivo electrónico privado o público.

La privacidad es necesaria para relaciones de intimidad y confianza. En una sociedad en que los individuos no tienen privacidad, la amistad y la confianza no se pueden desarrollar. Si se desea tener tales relaciones, se debe tener privacidad. Es un delicado problema: conciliar el poder estatal y el interés público, con los derechos inviolables de la persona sobre la base de un espíritu democrático y del Estado de Derecho. Es por ello que se requiere prevenir los posibles abusos y peligros que la informática puede generar.

La mayoría de los estados han legislado o están legislando en este sentido. España, como joven democracia, previó estos problemas y la Constitución (art. 18.4) ya hizo esa previsión de los posibles abusos y peligros que la informática puede generar, vinculándolos a los del título Primero: los derechos y deberes fundamentales. A tenor de ello "la ley limitará" el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Este precepto implica un mandato ineludible al legislador para que establezca los mecanismos legales precisos a fin de crear las condiciones necesarias para que tales garantías resulten real y efectivamente aplicables.

La información sobre las personas se utiliza para tomar decisiones importantes que afectan profundamente a las personas. La información sobre lo que se almacena en una base de datos se puede utilizar para decidir si una empresa contrata o no, si o no se concede un préstamo, si o no se llamará a la comisaría de policía para un interrogatorio, un arresto o una persecución; si o no se recibirá una educación, un alojamiento, etc.. El respeto a la intimidad se extiende hoy, en los países de civilización política democrática, a una esfera bastante amplia

de la vida privada. No sólo a los informes íntimos, sino también a algunos comportamientos personales, a los elementos distintivos de la personalidad, a las opiniones religiosas y políticas. Los datos de este género se denominan *sensibles* para distinguirlos de los que están a disposición del público.

Se entiende que la privacidad es una necesidad básica, esencial para el desarrollo y mantenimiento de una sociedad libre, así como para la madurez y estabilidad de la personalidad individual. En consecuencia, se ha de considerar la consagración del derecho de toda persona frente a las agresiones contra sí mismo, su hogar, su familia, sus relaciones y comunicaciones con los demás, su propiedad y sus negocios. Así concebido, este derecho incluye la protección frente a utilizaciones no autorizadas de su imagen, de su identidad, su nombre o sus documentos personales.

Nuestra Constitución, en su tratamiento del término *privacidad*, hace una diferencia con el término *intimidad*, dice el texto "Nótese que se habla de la privacidad, y no de la intimidad: aquélla es más amplia que ésta, pues en tanto que la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona (el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo) la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad, que aisladamente consideradas, pueden carecer de significación intrínseca, pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste **tiene derecho a mantener reservado**".

- ***DERECHO A LA PROTECCIÓN DE DATOS***

Es preciso enmarcar los conceptos "informática y privacidad" dentro de un equilibrio entre los derechos de quienes utilizan información sobre individuos (normalmente departamentos gubernamentales y corporaciones o empresas) frente a los derechos de aquellas personas sobre las cuales se obtiene información. La **privacidad** se ha denominado también *libertad informática*, que consiste en el derecho a la autotutela de la propia identidad informática, es decir, la que resulta de la recogida y de la confrontación de los datos personales insertos en un programa.

La protección de datos es una aplicación específica de principios de privacidad (sólo reconocida como un concepto legal desde finales del siglo XIX) a tecnologías de la información, y tiene como propósito la protección de la autonomía individual sobre los datos personales. Las leyes de los "gobiernos transparentes" normalmente toman la forma de derechos públicos de acceso a registros del gobierno con el propósito de hacer el gobierno más responsable ante el gobernado.

La protección de datos ha sido un tema central desde el principio de los setenta coincidiendo con el uso masivo de sistema informáticos. Diversas leyes han sido promulgadas por muchos Estados para la protección de los datos personales. Las características comunes de los conceptos europeos sobre protección de datos privados están recogidas en el **Convenio 108** del Consejo de Europa, redactado en Estrasburgo en 1981. Este Convenio ha sido firmado por más de treinta países y está abierto a la adhesión de países no europeos, y trata, fundamentalmente, de la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (ratificado por España en 1984).

Las características comunes de los conceptos europeos sobre la protección de datos privados son los siguientes:

- Regulación mediante ley;
- El almacenamiento de datos sólo es permitido para fines específicos. De ello se deducen:
- Limitaciones en cuanto a volumen ("no más datos de los necesarios para ese propósito particular").
- Limitaciones con respecto al tiempo ("Borrar los datos después de alcanzar el propósito perseguido");
- Las personas a quienes corresponden los datos tienen derecho al acceso a los mismos y a enmendar sus datos personales;

- Ejecución de la ley y control, en concreto:
- Autoridad para la supervisión, independiente del gobierno.
- La utilización de datos está supeditada a un permiso o registros.
- Los usuarios de los datos están obligados a tomar medidas que garanticen la seguridad de los datos.

Estos llamados *principios fundamentales de la protección de datos* constituyen el mínimo de derechos, que deberán contemplar los siguientes preceptos:

- Obligaciones de las partes.
- Calidad de los datos.
- Clases especiales de datos.
- Seguridad de los datos.
- Garantías complementarias para el interesado.
- Excepciones y restricciones.
- Sanciones y recursos.
- Ampliación de la protección.

En España se ha constituido recientemente la **Agencia De Protección de Datos**, organismo público que se encarga de hacer cumplir los preceptos legales comentados anteriormente, como los que se incluyen en la **LEY ORGÁNICA DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL**, también llamada **LORTAD**, y cualquier otra legislación vigente de ámbito nacional y/o Europea.

A continuación describiremos detalladamente la citada Agencia Española, para comprender cuales son sus funciones y comentaremos la **LORTAD**.

- ***AGENCIA DE PROTECCIÓN DE DATOS***
- *¿QUE ES LA AGENCIA DE PROTECCION DE DATOS?*

Es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada. Actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Su finalidad principal es velar por el cumplimiento de la legislación sobre protección de datos personales informatizados y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos.

La agencia de protección de datos además mantiene una pagina web , de donde ha sido extraída esta información (www.ag−protecciondatos.es), para dar publicidad a la existencia de ficheros automatizados de datos de carácter personal inscritos en el **Registro General de Protección de Datos (RGPD)** de forma pública y gratuita. Una de las funciones primordiales de este REGISTRO es la de velar por la publicidad de los ficheros con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos, que la Ley reconoce a todos los ciudadanos. En concreto, se trata de facilitar la información necesaria a cualquier persona que necesite conocer:

- La existencia de los ficheros de datos de carácter personal y su dirección de acceso.
- Sus finalidades.
- La identidad del responsable del fichero.

- *INSCRIPCIÓN DE FICHEROS EN EL RGPD*

Toda persona o entidad que proceda a la creación de ficheros automatizados de datos de carácter personal, deberá notificarlo previamente a la Agencia de Protección de Datos. Igualmente, deberán comunicarse los cambios que se produzcan en cualquiera de los datos notificados a la Agencia.

- **¿Cómo se notifica la existencia de un fichero al RGPD?**

Si el fichero es de **titularidad privada:**

Deberá cumplimentar un formulario de notificación del tratamiento automatizado de datos de carácter personal de titularidad privada.

Si el fichero es de **titularidad pública:**

- La creación, modificación o supresión de ficheros automatizados de las Administraciones Públicas sólo podrá hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente, indicando:

    - Finalidad y usos del fichero.
    - Personas o colectivos sobre los que se pretende obtener datos o que estén obligados a suministrarlos.
    - Procedimiento de recogida.
    - Estructura básica del fichero y descripción de los tipos de datos.
    - Cesiones de datos previstas.
    - Órganos de la Administración responsables del fichero.
    - Servicios o unidades ante los que pudiesen ejercitar los derechos de acceso, rectificación y cancelación de datos de los afectados.

- El órgano competente de la Administración responsable del fichero, trasladará una copia de la disposición de creación del fichero al Registro General de Protección de Datos, junto con un formulario de notificación del tratamiento automatizado de datos de carácter personal de titularidad pública.

También, cabe la posibilidad de proceder a la inscripción en soporte magnético, que se puede adquirir en la Agencia de Protección de Datos, en el Paseo de la Castellana 41, 3ª planta, de 9 a 14 horas; así mismo, puede solicitarse por fax al número 308.46.92, en cuyo caso se enviará contra reembolso.

- **¿Qué ocurre si no se notifica la existencia de un fichero?**

En este caso podría incurrirse en falta grave, tal y como señala la Ley Orgánica 5/1992, quedando sujeto al régimen sancionador previsto en esta Ley.

- *INFRACCIONES*

Según la LORTAD las infracciones están clasificadas en:

- LEVES
- GRAVES
- MUY GRAVES

Además incluyen también las prescripciones y las sanciones que se aplican.

- **LEVES**
- No proceder a la rectificación o cancelación de errores o inexactitudes.
- No cumplir las instrucciones del Director de la A.P.D. ni facilitar información.
- No conservar actualizados los datos.
- Cuestiones meramente formales o documentales que no constituyan infracción grave o muy grave.
- **GRAVES**
- Creación de ficheros de titularidad pública sin la autorización de disposición de carácter general publicada

en el BOE o diario oficial correspondiente.
- Creación de ficheros privados con finalidades distintas de las que constituyen el objeto legítimo de la empresa.
- Recoger datos sin el consentimiento expreso de los afectados, cuando éste sea exigible, o sin facilitarles información sobre sus finalidades.
- Incumplimiento de los preceptos de protección, siempre que no constituya infracción muy grave.
- Impedimento u obstaculización del derecho de acceso y la negativa a facilitar la información que sea solicitada.
- Mantener datos inexactos o no efectuar rectificaciones o cancelaciones, cuando resulten afectados derechos de personas.
- Vulneración del deber de guardar secreto, cuando no constituya infracción muy grave.
- Mantener ficheros sin las debidas medidas de seguridad.
- No remitir a la A.P.D. las notificaciones previstas en la LORTAD o sus disposiciones de desarrollo.
- No proporcionar en plazo, los documentos e informaciones requeridos.
- Obstrucción a la función inspectora.
- **MUY GRAVES**
- Recogida de datos de forma engañosa y fraudulenta.
- Cesión de datos fuera de los casos permitidos.
- Recabar datos, sin el consentimiento expreso del afectado, que versen sobre ideología, religión o creencias.
- Recabar datos sobre salud, origen racial o vida sexual, sin el consentimiento expreso del afectado o sin que lo disponga una ley.
- Crear ficheros cuya única finalidad sea recabar datos sobre ideología, religión, creencias, origen racial o vida sexual.
- No cesar en el uso ilegítimo de los tratamientos automatizados cuando sea requerido para ello.
- Transferencia de datos a países cuyo nivel de protección no sea equiparable y sin la autorización del Director de la A.P.D.
- Tratamiento de datos con menosprecio de los principios y garantías, cuando se atente contra los derechos fundamentales.
- Vulneración del deber de guardar secreto sobre los datos relativos a ideología, religión, creencias, origen racial, salud y vida sexual.

Prescripción:

- Leves: 1 año
- Graves: 2 años.
- Muy graves: 3 años.

- *SANCIONES*

Según la gravedad:

- Leves: 100.000 a 10.000.000 ptas.
- Graves: 10.000.001 a 50.000.000 ptas.
- Muy graves: 50.000.001 a 100.000.000 ptas.

En el caso de utilización o cesión ilícita de datos que atenten contra los derechos fundamentales, el Director de la A.P.D. podrá requerir a los responsables de los ficheros, tanto públicos como privados, la cesación de la utilización o cesión ilícita de los datos. Si se desatiende el requerimiento, se podrán inmovilizar los ficheros mediante resolución motivada.

NOTA: Las infracciones y sanciones así como las funciones de la A.P.D. no son de aplicación a los ficheros cuyos responsables sean:

- Las Cortes Generales.
- El Defensor del Pueblo.
- El Tribunal de Cuentas.
- El Consejo General del Poder Judicial.
- El Tribunal Constitucional.
- ***LA LORTAD***

Cuando se promulga la LORTAD, Ley Orgánica 5/1992 de 29 de Octubre de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (Ver Anexo I) se cumple un doble objetivo: Obedecer el mandato constitucional contenido en el artículo 18.4, así como el artículo 4 del Convenio de Estrasburgo para la protección de las personas con respecto al tratamiento de los datos de carácter personal. En consecuencia, se puede decir que en España los derechos de protección de datos y a la intimidad del ciudadano están cubiertos y amparados por la ley. Para el cumplimiento de esta finalidad se estructura un sistema de garantías y medidas cautelares, que pretende recoger las orientaciones del Derecho comparado en materia de protección de datos personales. La exposición de motivos de la LORTAD concibe la protección de los bancos de datos personales desde una perspectiva funcional; no se limita a su tutela en cuanto nuevos depósitos de informaciones, "sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el papel personal".

El texto de la LORTAD (Ver Anexo I) se halla integrada por una Exposición de Motivos, 48 artículos distribuidos en 7 Títulos, 3 disposiciones adicionales, una disposición transitoria, una disposición derogatoria y 4 disposiciones finales. En su *estructura normativa* pueden distinguirse dos sectores básicos:

- Una *parte general o dogmática* dedicada a la proclamación de la libertad en la esfera informática en la pluralidad de sus facultades y manifestaciones, e integrada por los Títulos:
    - **I**, en el que se formulan las disposiciones generales de la Ley referidas a su objeto, ámbito de aplicación y definiciones;
    - **II**, donde se contienen los principios de la protección de datos con referencia expresa a las exigencias de: calidad de los datos, información y consentimiento de los afectados, protección especial de datos sensibles y relativos a la salud, seguridad de los datos, deber de secreto y garantías para la cesión de los mismos;
    - **III**, referido a los *derechos* que dimanan del reconocimiento de la libertad informática y que se desglosan en: la impugnación de valoraciones basadas exclusivamente en datos automatizados, y en las facultades de información, acceso, rectificación y cancelación; asimismo se consignan los instrumentos para la tutela de esas facultades y el derecho a la indemnización.

- Una *parte especial u orgánica* en la que se establecen los mecanismos organizativos y/o institucionales a que deben acomodarse o que deben supervisar el funcionamiento de las bases de datos a fin de garantizar la libertad informática. Se incluyen aquí los Títulos:
    - **IV**, que prevé unas Disposiciones sectoriales para reglamentar *los Ficheros de titularidad pública*, donde se contemplan los requisitos para su creación, modificación o suspensión, los supuestos de cesión de datos entre las Administraciones Públicas, el régimen de ficheros de los cuerpos de seguridad y las excepciones a los derechos; y los *Ficheros de titularidad privada*, que contiene previsiones normativas en orden a su creación, notificación e inscripción registral, comunicación de cesión de datos, régimen de datos sobre abonados a servicios de telecomunicación, prestación de servicios de tratamiento automatizado de datos personales o sobre solvencia patrimonial y crédito, ficheros con fines publicitarios o relativos a encuestas o investigaciones, así como los códigos tipo para la estructura, funcionamiento,

seguridad y garantías de los ficheros privados;

- **V**, que disciplina *el movimiento internacional de datos* y donde se acoge el principio básico de reciprocidad del Convenio 108, que supedita el flujo internacional de datos, necesario para el desarrollo cultural, económico y de la seguridad mutua de los Estados, a la existencia en el país receptor de los datos personales de garantías similares a las del transmisor, en este caso a las que se establecen el la LORTAD; salvo excepciones motivadas por acuerdos internacionales, o se trate de prestar o solicitar auxilio judicial o sanitario internacional, o se refiera a transferencias dinerarias conforme a su legislación específica;
- **VI**, donde se regula la naturaleza y régimen jurídico de la *Agencia de Protección de Datos*, y se especifican las competencias de su director, del Consejo Consultivo y el objeto del Registro General; al tiempo que se prevén las relaciones de esta institución con las correspondientes de las Comunidades Autónomas.
- **VII**, íntegramente consagrado a tipificar el sistema de infracciones y sanciones previstos por la LORTAD. Se trata de un conjunto de supuestos genéricos de responsabilidad administrativa por infracciones, leves, graves y muy graves, que pueden dar lugar a sanciones disciplinarias, para responsables de ficheros públicos, o pecuniarias en el caso de ficheros privados. En ambos supuestos, para infracciones muy graves, se contempla la posibilidad de inmovilizar los ficheros.

La LORTAD requirió un órgano de fiscalización y control bajo el nombre de *Agencia de Protección de Datos* y su estatuto propio fue aprobado por el Gobierno en 1993 (BOE 4−V−1993); tiene como misiones velar por el cumplimiento de la ley, dictar instrucciones, sancionar infracciones de carácter administrativo previstas en ella, atender las reclamaciones de los interesados y redactar la memoria anual.

En opinión de los expertos, la LORTAD presenta en su haber dos aspectos abiertamente positivos: la definición de los principios básicos, y el reconocimiento y tutela jurídica de la libertad informática y un aspecto negativo: sus constantes y significativas excepciones.

Entre los principios básicos que informarán la actuación de los bancos de datos con soporte informático que procesen informaciones personales, se encuentran: la calidad de los datos, la transparencia (obliga a informar a los afectados por la recogida de datos personales sobre la finalidad, obligatoriedad, consecuencias y derechos que implica su tratamiento automatizado), el consentimiento (como garantía de los afectados), la tutela reforzada de los datos sensibles (evitar tratos discriminatorios por motivos de razón, salud, vida sexual), la seguridad (frente a la alteración, pérdida o acceso indebido a los datos personales, el secreto y la cesión (limitada al uso para fines legítimos y con el previo consentimiento del afectado).

El otro aspecto positivo de la LORTAD consiste en el reconocimiento y tutela jurídica de la *libertad informática*. Su función se cifra en garantizar a los ciudadanos una facultades de información, acceso y control de los datos que les conciernen.

En el *debe* de la LORTAD se recogen significativas excepciones que limitan el alcance práctico del ejercicio de las libertades informáticas. Se establecen excepciones relevantes referidas a: la información de los afectados; a su consentimiento; a las garantías de los datos sensibles; a la posibilidad de que las Fuerzas de seguridad del Estado puedan informatizar datos sensibles sin control judicial, fiscal o de la propia Agencia de Protección de datos; a los límites al ejercicio de los derechos de acceso, rectificación y cancelación a los bancos de datos públicos; así como a la restricción del derecho a la información y acceso de los ciudadanos a los datos que les conciernen elaborados por las Administraciones Públicas por motivos tan vagos como "las funciones de control y verificación" de las mismas y a la supeditación general de la tutela a cuanto afecte a la Defensa Nacional, Seguridad Pública, interés público o intereses de terceros dignos de protección.

Para ubicar los comentarios anteriores, hay que asumir que las sociedades actuales precisan de un equilibrio entre el flujo de informaciones, que es condición indispensable de una sociedad democrática y exigencia par la actuación eficaz de los poderes públicos, con la garantía de la privacidad de los ciudadanos. Ese equilibrio precisa de un **"Pacto social informático"** por el que el ciudadano consiente en ceder al estado datos personales, a cambio del compromiso estatal de que los mismos se utilizarán con las debidas garantías. Ese reto social, jurídico y político constituye el horizonte a alcanzar por la LORTAD; y a todos, en cuanto ciudadanos deseosos de una convivencia en libertad, nos importa que no defraude el logro de ese objetivo.

Al ser la LORTAD una Ley Orgánica, de carácter general, ha dado lugar a una serie de reglamentos que desarrollan sus preceptos. De entre ellos hay que destacar el Real Decreto 1332/94 (Ver Anexo III) que especifica una serie de obligaciones para los responsables informáticos. Como un ejemplo del cumplimiento de estos preceptos, el Anexo IV muestra la resolución de Septiembre de 1994, de la Universitat Jaume I, acerca de los ficheros que utilizan sus servicios informáticos.

- ***LEGISLACIÓN EUROPEA***

También la Unión europea elaboró una propuesta de Directiva del Consejo presentada por la Comisión en 1990, que fue objeto de una nueva redacción en 1992, siendo adoptado el texto definitivo por el Parlamento Europeo y el Consejo, el 24 de octubre de 1995 (Directiva 95/46/CE). Dicha Directiva (Ver Anexo II) se refiere a **"la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos"**. En ella se pretende armonizar la fluidez de la transmisión de datos en el seno de la UE para la mayor eficacia de los poderes públicos y desarrollo del sector privado, con la defensa de los datos personales. Para ello se prevé la existencia en cada Estado miembro de una autoridad independiente para garantizar la tutela de los datos personales y velar por la aplicación correcta de la Directiva. Asimismo se contempla la existencia de una autoridad comunitaria denominada *Grupo de Protección de las personas* que estará integrada por representantes de las autoridades de control nacionales y un representante de la Comisión, los cuales contribuirán a la interpretación homogénea de las normas nacionales adoptadas en aplicación de la directiva, así como informarán a la Comisión de los conflictos que puedan surgir entre la legislación y las prácticas de los Estados miembros en materia de protección de datos personales.

A su vez, el *Acuerdo de Schengen* suscrito inicialmente por Alemania, Francia y los países del Benelux en 1985 y desarrollado por un Convenio de aplicación de 1990, se han adherido otros Estados de la Unión europea (España, Italia, Grecia, Portugal...). Dicho tratado internacional se refiere a la supresión gradual de controles entre las fronteras comunes de los países signatarios. Para ello se regula el flujo de informaciones personales en función de la cooperación policial. El objetivo principal del Sistema de Información Schengen (SIS) era la comunicación de informaciones para el control de las personas "indeseables" y/o "inadmisibles" dentro de las fronteras del "espacio Schengen". Para el logro de ese objetivo entró en funcionamiento una gran base de datos policiales situada en Estrasburgo y sometida a la legislación francesa de protección de datos personales. Al igual que el Convenio del consejo de Europa exige que para la transmisión de esas informaciones existan en cada país receptor normar internas sobre protección de datos personales que satisfagan los principios del citado Convenio del Consejo de Europa.

- ***PROTECCIÓN DEL SOFTWARE***

En nuestra sociedad estamos acostumbrados a ver en todo tipo de productos los símbolos ©, **TM** ó ®. Sabemos lo que significan: existe una protección sobre ese producto. Pero, ¿se puede proteger de igual forma el Software?. Existen multitud de razones que nos incitan a pensar que sí, que al igual que se protegen obras musicales, libros, etc..., se debe de poner alguna protección legal a cualquier

reproducción, modificación, usurpación de ideas, etc... con respecto al Software.

- ***PIRATERÍA INFORMÁTICA***

La piratería realmente comienza con la aparición de los ordenadores personales puesto que, hasta ese momento, se trabajaba únicamente en grandes ordenadores en los que se utilizaban programas hechos a medida que difícilmente podían aprovecharse de un caso particular a otro.

En España, hasta hace unos años, no había una conciencia clara de lo que suponía la copia ilegal de un programa ni de sus posibles consecuencias. En la actualidad, la cuestión es diferente debido en parte a asociaciones como BSA (Business Software Alliance) y SEDISI (Asociación Española de Empresas de tecnologías de la Información). En cuanto a cifras, se estimaba que en 1993 se dejaron de ingresar más de un billón y medio de pesetas debido a la piratería, la tercera parte correspondiente a Europa. En España, en concreto, se hablaba de cerca de cincuenta mil millones, siendo sólo legal el 14% de los programas utilizados. En 1994, la cifra descendió en España a unos treinta mil millones de pesetas situándose el porcentaje de programas legales en el 27%. Actualmente la piratería del Software en España está en niveles insospechados hasta el momento, a la cabeza de Europa, debido en parte a la proliferación y abaratamiento de dispositivos capaces de efectuar la reproducción a bajo coste y tiempo reducido.

En general piratería, es copiar para utilizar o comercializar sin autorización cualquier cosa que tenga derechos de autor. Aquí lógicamente sólo se ha hablado de piratería informática; sin embargo, también lo es, por ejemplo, fotocopiar un libro, un delito tan punible como copiar un programa, teniendo además en cuenta que las editoriales son empresas mucho más modestas que las multinacionales del software. En España, los escritores están defendidos por CEDRO (Centro Español de Derechos Reprográficos) y asociaciones como ACTA (Asociación de Autores Científico−Técnicos y Académicos) que defiende los intereses de los autores de libros técnicos de cualquier rama de la ciencia, incluida, claro está, la informática.

Como veremos mas adelante, en nuestro país, La Ley de Protección Intelectual de 1987 ya amparaba los derechos de los autores de programas informáticos aunque al ser muy general dejaba sin cubrir algunos huecos, que dieron lugar a una ley más adaptada a este asunto en concreto llegaría en 1993. Esto se traduce en una nueva ley mucho más completa y eficaz para luchar contra la piratería que la Ley de Propiedad Intelectual. Las asociaciones antes mencionadas disponen de un teléfono donde se puede llamar para realizar cualquier consulta y también denunciar a las empresas sospechosas de utilizar o comercializar programas ilegales. Como experiencia piloto, dichas asociaciones pusieron en marcha un programa de recompensas para quienes aportasen información sobre empresas que usan o comercializan programas ilegales, siempre que se llegase a demostrar la veracidad de la denuncia con la consiguiente condena para la empresa. Además se han llevado a cabo numerosas acciones policiales de desmantelamiento de redes de piratería informática afincadas en las grandes ciudades, e incluso se han puesto en la calle a inspectores de piratería informática, que visitan un establecimiento en calidad de cliente, comprobando el cumplimiento de la normativa al respecto.

- ***CONTRATOS INFORMÁTICOS***

La alusión al contrato evoca el supuesto previsto del Código Civil, es decir, la relación jurídica bilateral por la que **"una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o prestar algún servicio"**. Este tipo legal básico se proyecta a los contratos informáticos con importantes peculiaridades, ya que pueden afectar al hardware y/o al software, dando lugar a una rica tipología en la que pueden distinguirse contratos de compraventa, alquiler, leasing, mantenimiento y servicios.

La complejidad "objetiva" de estos contratos procede de la inevitable conjunción del *hardware* y del *software*, en la estructura del ordenador (una máquina física que sólo es operativa si cuenta con un programa que le permita cumplir sus fines). De ahí, surge una importante serie de problemas ya que, en la actualidad, quien fabrica el equipo físico del ordenador no siempre coincide con quien crea los programas. El usuario adquiere una máquina confiando que pueda prestarle determinados servicios, pero el logro de esta finalidad depende de la adecuación entre el soporte físico y los programas. Si el resultado apetecido no se produce, el adquirente tenderá a esgrimir las facultades que le otorga su contrato, sea frente al constructor del *hardware*, o el del *software*. Ello da lugar a una variada casuística de responsabilidad contractual cuyos perfiles y consecuencias se expanden y complican. Una de sus notas más relevantes es la paulatina pérdida de protagonismo contractual del ordenador, en cuanto máquina, y la correlativa valoración de sus servicios. La especificidad del objeto y estructura de los contratos informáticos, que incluyen una serie de facultades y obligaciones diversas pero interdependientes, determina que se les repute como una categoría de contratos especialmente complejos. No existe, por tanto, un contrato informático, sino un sistema de contratos informáticos.

Esta situación se ha visto potenciada con la extensión capilar propiciada por la microinformática. Ahora el contratante de informática ya no son sólo las grandes empresas, como lo fueron en la etapa que corresponde a las tres primeras generaciones de ordenadores; con la difusión de los PC y Workstation, que hacen que los usuarios sean innumerables, supone un nueva concepción de las obligaciones del contrato informático. Este nuevo entorno subjetivo de los contratos informáticos los proyecta hacia la problemática general de la tutela de los consumidores y usuarios.

Los problemas específicos que suscitan los contratos sobre los programas de los ordenadores nos sitúan ante los distintos medios para la protección jurídica del *software.* Conviene advertir, que el interés por esta materia es muy reciente, pues durante años se infravaloró respecto al hardware, la importancia económica del software y además, las casas constructoras de equipos informáticos temieron que el establecimiento de una tutela jurídica del soporte lógico fuera una rémora para el desarrollo industrial del sector. Sobre el cambio de actitud que se ha experimentado en esta esfera resulta ilustrativa la posición de IBM, que tras haber boicoteado por mucho tiempo la patentabilidad del *software*, tras sufrir la "piratería" de determinadas casas constructoras japonesas y embarcarse en los consiguientes procesos judiciales, ha pasado a ostentar el liderazgo de quienes abogan en favor del reforzamiento de los mecanismos de garantía.

- ***COPYRIGHT Y CONTROL DE MARCAS***

El marco legal que regula el copyright y las denominadas marcas registradas corresponde al de la propiedad intelectual y al de derechos de autor. El *software*, por definición, es un conjunto de acciones o instrucciones que, en consonancia con un *hardware* asociado, produce resultados al usuario del mismo. Por ello, se considera que es producto de una actividad intelectual, y esta sujeto a las leyes de derechos de autor y de la propiedad. Por esa razón, la legislación que afecta a la protección del *software* (la cual veremos más adelante) procede de la que regulaba antiguamente los derechos de autor de obras musicales, de libros, etc... Pero eso sí, con algunas particularidades. Actualmente, respecto al *software*, sólo es posible proteger por derechos de autor programas originales, pero no las ideas sobre las que se basan, ni los interfaces en que se apollan. De hecho, no fue posible por parte de Netscape proteger por patente la idea del navegador de Internet, totalmente pionera en el marco informático y de comunicaciones, aunque sí su producto Netscape Navigator.

Actualmente poseer el derecho de autor de un programa *software* no representa un concepto económico muy marcado para el autor, en cuestión de ingresos derivados de dicho derecho, ya que por las características de obsolescencia del *software*, éste solo será rentable durante no mucho tiempo (2 ó 3 años a lo sumo). Contrasta este hecho con la duración que se le concede a la protección de esta entidad, que viene a ser de 20 años (dependiendo del país donde se encuentre uno) después del

establecimiento de la protección. Como se puede apreciar, aún queda mucho por recorrer en este aspecto de la normativa en cuanto a copyright y control de marcas en el *software*.

- ***PRINCIPALES INSTRUMENTOS PARA LA PROTECCIÓN DEL SOFTWARE***
- *INSTRUMENTOS DE PROTECCIÓN JURÍDICA GENÉRICOS*

Los juristas suelen mostrarse refractarios a la innovación de categorías e instituciones para reglamentar situaciones nuevas, lo que equivaldría a una prueba de rigor y economía intelectual de los operadores del derecho al resistirse a introducir nociones superfluas o artificiosas. En su contra, podría objetarse una cierta tendencia hacia la pasividad y el inmovilismo, por la que consideran preferible no reglamentar un sector, antes que precipitarse en su regulación. Esta discusión se esta reproduciendo, en estos momentos a la hora de aplicar el derecho en Internet, que es objeto de grandes discusiones y debates (ver Anexo VII). Sin poder adelantar el resultado final, parece claro que las nuevas tecnologías acabaran imponiendo nuevas categorías jurídicas para conseguir una regulación socialmente aceptable y compatible con los futuros desarrollos.

Esto explica que las primeras tentativas para la protección del soporte lógico de los computadores tendiera a remitirse a instituciones y principios jurídicos tradicionales. Así, se recurrió, a tenor de los supuestos y circunstancias, a la vía de la responsabilidad civil y penal, bien a través del resarcimiento de daños por culpa civil extracontractual, o de las normas sobre la competencia desleal, de la tutela del secreto industrial e incluso se recurrió también a cláusulas de tutela del software, incluidas en los acuerdos contractuales, lo que sigue siendo una práctica vigente.

Sin embargo estos instrumentos de garantía solo constituyen un soporte jurídico rudimentario para garantizar la creciente importancia económica del software y, en todo caso, han resultado inadecuados para conseguir una protección directa y autónoma de los progresos en cuanto bienes jurídicos.

- *PROTECCIÓN A TRAVÉS DEL DERECHO DE PATENTES*

Un paso importante en el perfeccionamiento de las técnicas de tutela del soporte lógico se da cuando la doctrina y la jurisprudencia de los países tecnológicamente más avanzados estiman que, del mismo modo que se admitía la protección del *hardware* de los ordenadores como un "bien material" o producto industrial mediante el derecho de patentes, cabía extender esa forma de protección al *software* en cuanto expresión de un "bien inmaterial", que por su vinculación necesaria con el equipo físico, o por su propia condición de invento industrial, podía ser patentado.

Entre las ventajas del sistema de patentes se aduce la amplitud de su protección y que asegura al autor del programa un monopolio temporal (veinte años) para su explotación, garantizándole que, durante este período, nadie podrá producir, comercializar o utilizar el programa sin su consentimiento. Transcurrido dicho plazo se considera que tal programa pasa a engrosar el patrimonio científico y económico de la sociedad, por lo que puede ser objeto de libre utilización.

Las principales dificultades que entraña este sistema surgen de los requisitos de la patentabilidad, ya que para que le programa pueda ser patentado precisa reunir las características de: a) **novedad**, es decir, debe representar objetivamente una innovación; b) **materialidad**, que exige que el objeto de patente no sean meras ideas o proyectos, sino realidades tangibles susceptibles de traducirse en resultados prácticos, c) **industrialidad**, la patente se concede sólo a creaciones que tienen una aplicación en la producción o transformación de productos y entrañan un avance tecnológico.

Para algunos juristas, el *software* reuniría todos y cada uno de estos requisitos. Por el contrario, han sido cada vez más numerosos quienes impugnan que en los programas se den las notas de: la innovación, porque las más de las veces un programa tiene que ser una derivación o modificación de

otros anteriores; la materialidad, porque él es básicamente el producto de una actividad mental, (se trata de algoritmos) de un procedimiento lógico de elaboración de informaciones que precisamente por ello, tiene una autonomía respecto al equipo físico (salvo en el caso del *firmware*, o *software* de base, o de la memoria ROM, que son programas integrados en los propios circuitos electrónicos); y la industrialidad, ya que el *software* carece de los certificados de operatividad y de sistemas de mantenimiento característicos de los objetos industriales patentables.

Se indica también, desde estas posiciones críticas, la inadecuación del actual sistema de registro de patentes para la inscripción del *software*, que quiere un procedimiento de registro más flexible, simple y rápido.

Estas tesis contrarias a la patentabilidad del *software* han hallado un respaldo decisivo en el *Convenio para la Patente Europea* suscrito en Munich en 1973, donde se establece de forma categórica que: "no son invenciones los programas de ordenadores". Si bien, el texto del Convenio limita la exclusión a los programas en cuanto tales, pero deja abierta la posibilidad de patentar las máquinas que impliquen la utilización de programas electrónicos.

A partir del Convenio las sucesivas reformas del derecho europeo de patentes se orientan en la misma dirección. Así ocurre con la Patents Act británica de 1977, la ley francesa de 1978, la italiana de 1979, la de la República Federal de Alemania de 1981 y la ley española de Patentes de 1986 que establece que no se considerarán invenciones y por tanto, no serán patentables "los programas de ordenadores". A tenor de lo expuesto no puede extrañar que se haya tendido a la búsqueda de otras vías par la protección jurídica del software.

- *PROTECCIÓN A TRAVÉS DEL DERECHO DE AUTOR*

El derecho de autor, o *copyright* en la terminología anglosajona, consiste en la protección jurídica de los aspectos morales y patrimoniales de las creaciones originales del ingenio humano sea en el campo científico, literario o artístico.

Desde mediados de la década de los sesenta el registro de *copyright* norteamericano admitió la inscripción de programas de ordenadores siempre que se acreditara su originalidad y se depositaran copias en un lenguaje que fuera inteligible. A partir de entonces la actitud dominante de la doctrina y la jurisprudencia estadounidense tendió a extender, para la protección del *software*, la disciplina del derecho de autor. En este clima, el Congreso de USA al promulgar la *Copyright Act* de 1976, que reformaba la anterior ley de 1909, creó una Comisión de estudio para la tutela de los programas de los ordenadores, cuya labor cristalizó en la *Computer Software Copyright Act* de 1980, que modificó el texto de 1976 en los siguientes términos: a) Define el *software* y admite expresamente su tutela por las disposiciones del *copyright*; b) Se condiciona dicha protección al carácter original del programa; c) Prohibe no sólo la reproducción, sino también la utilización de los programas protegidos, d) Se admite, sin embargo, que los usuarios legitimados puedan realizar las copias y adaptaciones de los programas que estimen precisas para su uso interno.

El ejemplo jurídico norteamericano ha influido notablemente en otros sistemas. Quienes abogan por seguir este modelo aducen en su favor: la similitud de los programas con las restantes obras de ingenio protegidas por el derecho de autor; la amplitud de este procedimiento de tutela; su duración, que abarca hasta los cincuenta años desde la muerte de su autor; su carácter universal sin sujeción a límites territoriales; así como la simplicidad y rapidez de los trámites con que operan los registros de *copyright.*

Ahora bien, el sistema no está del todo exento de dificultades y objeciones. Entre ellas cabría aludir a lo problemático que resulta parangonar los programas de los ordenadores con las obras literarias o

artísticas. Así, frente al requisito objetivo de innovación exigido para la patentabilidad el derecho de autor requiere el rasgo subjetivo de la originalidad creativa, cualidad que difícilmente puede predicarse, en el mismo sentido de una obra literaria o artística, de un programa. De otro lado, se indica que el derecho de autor sobre las obras de arte se refiere a la defensa de su forma, no a la de su contenido, lo que supondría dejar en precario la defensa de los programas en los que forma y contenido se confunden.

En todo caso existen controversias sobre si el derecho de autor puede ser una disciplina jurídica restringida a los de aplicación, o si puede extenderse también a los programas sobre soporte tipo ROM, escritos en código de máquina e integrados en circuitos, para los que, como ya se ha indicado, parece más adecuada la tutela por el sistema de patentes.

Se aduce, al propio tiempo, para hacer hincapié en las limitaciones de la tutela del *software* por esta vía, que el derecho de autor permite vetar la reproducción y comercialización de los programas, pero no evita su utilización. Se advierte además que el trámite de depósito de los programas en los registros de *copyright* puede constituir una ocasión para la facilitar su copia más o menos directa.

- *PROTECCIÓN A TRAVÉS DE MEDIOS ESPECÍFICOS*

Como hemos visto, la tutela del *software* a través de los distintos instrumentos de garantía jurídica tradicionales conduce a una disyuntiva insatisfactoria, porque o se distorsionan estas categorías e instituciones para adaptarlas a un objeto nuevo, para el que cuando surgieron no estaban pensadas, y en cuyo seno el software aparece como un cuerpo extraño; o se tiene que aceptar un régimen de protección precario e insuficiente. Estas razones han motivado un difundido estado de opinión doctrinal tendente a recabar instrumentos legislativos "*ad hoc"* adecuados para captar y defender las peculiaridades del *software*.

En estas coordenadas se orientan las "Disposiciones−tipo para la Protección del Software" promulgadas en 1978 por la Organización Mundial de la Propiedad Intelectual (OMPI) en Ginebra, donde se halla la sede de este organismo internacional, que constituyen un modelo obligado de referencia para cualquier iniciativa de política legislativa en este sector. En el texto de la OMPI pueden distinguirse tres grandes apartados:

- El primero se consagra a la **delimitación del objeto de la tutela**. Para ello se procede a una tipificación jurídica del software entendiéndose por tal: a) el "programa del ordenador" definido como "el conjunto de instrucciones que, una vez transferido a un soporte legible para la máquina, permite que una máquina para procesar informaciones desarrolle su función, realice su tarea o logre un resultado específico"; b) la "descripción del programa", es decir, "la presentación completa de operaciones en forma verbal, esquemática u otra, lo suficientemente detallada para determinar el conjunto de instrucciones que constituyen el correspondiente programa del ordenador", y c) la "documentación auxiliar", o sea, "toda otra documentación distinta del programa del ordenador, como, por ejemplo, descripciones de problemas, o instrucciones para el usuario". Se reconoce la propiedad de los derechos reconocidos en esta norma al autor del software, salvo que el programa sea resultado del trabajo de un empleado en el ejercicio de sus funciones, en cuyo caso la propiedad pertenece a la empresa. Como condición necesaria y suficiente para acceder a la protección de este texto normativo se exige la originalidad del programa, en el sentido de ser "el resultado del esfuerzo intelectual personal de su autor". Al tiempo que se puntualiza que el objeto de la tutela es la "forma" en que se expone el programa y no la "idea" sobre la que éste se funda.
- El **ámbito de protección** conforma el segundo núcleo temático de los artículos de esta norma dirigidos a: especificar los derechos del propietario para impedir la divulgación de su *software* o el acceso, copia, utilización o comercialización del mismo sin su consentimiento; así como tipificar las distintas modalidades de violación de los derechos del propietario, que corresponden a todas las

acciones contrarias a sus derechos establecidos (salvo el caso en que dos autores realicen independientemente dos programas idénticos o similares, o en los casos de utilización de programas en medios de locomoción extranjeros que atraviesen el espacio territorial de un estado).

- Los artículos de esta norma precisan los **instrumentos de tutela** de los programas. Se establece aquí la posibilidad de que el propietario del software pueda ejercitar una acción judicial civil para defender su derecho, así como el resarcimiento de daños e indemnizaciones correspondientes para las eventuales violaciones de sus derechos.

Se indica finalmente que la protección establecida en estas "Disposiciones−tipo" no excluye la posibilidad de aplicación de principios generales del derecho, u otras disposiciones referentes al derecho de patentes, derecho de autor o competencia desleal.

Como puede advertirse, esta norma implica una vía de superación de la debatida dicotomía, derecho de patentes/derecho de autor como fórmulas de protección jurídica del software, ya que intenta adecuar aspectos inspirados en ambos sistemas a la peculiaridad del objeto de protección. Así, el planteamiento general de la norma se aproxima a los esquemas del *copyright* (siendo de lamentar que por influencia de ese enfoque mantenga la fractura entre la "forma" y la "idea" o contenido del programa, limitando la tutela a la primera), pero se inspira en el derecho de patentes para abreviar la duración del período protegido, de forma que puedan conciliarse los intereses del autor con el progreso científico y tecnológico de la sociedad, y para prohibir la utilización del *software* por parte de terceros y no sólo su reproducción o difusión pública según dispone el derecho de autor.

- ***LA PROTECCIÓN DEL SOFTWARE EN EL DERECHO ESPAÑOL***

En relación con los distintos medios reseñados dirigidos a la protección del *software*, el ordenamiento jurídico español se inclinaba por una solución ecléctica. En efecto, mientras algunos países (por ejemplo, USA) han optado por incluir la protección jurídica de los programas en la normativa de propiedad industrial, y otros (por ejemplo Brasil) han adoptado una legislación específica, nuestro ordenamiento regulaba los programas en las normas de propiedad intelectual, pero introduciendo unas cláusulas específicas en atención a la propia naturaleza del *software*.

La Ley 22/1987, de 11 de noviembre, de Propiedad Intelectual (LPI) equipara los programas de ordenador a las obras literarias, artísticas o científicas, constituyéndolos como objeto de propiedad intelectual de forma expresa. A su vez, el art. 95 de dicha Ley indica que la regulación específica aplicable a los programas de ordenador será la prevista en el Título VII de ese texto legal, remitiendo al régimen general de la propiedad intelectual todo lo que no esté allí previsto.

Los aspectos más relevantes del sistema de protección jurídica establecido en esa norma pueden cifrarse en los siguientes términos:

- **A)** Respecto al *objeto* de la protección, merece destacarse la definición legal de los programas informáticos como: "toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y de fijación". Se ha considerado que esta tipificación de los programas en términos tan amplios y flexibles, evite su posible obsolescencia en el futuro. La protección de los programas se hace extensiva a la documentación técnica de los mismos y a los manuales de uso, así como a las versiones y programas derivados ya que, como cualquier otra obra de autor, para que el programa pueda tutelarse como propiedad intelectual es necesario que sea una creación original. No obstante, se ha puesto de relieve la dificultad que entraña el proyectar el requisito de la <<originalidad>> al ámbito del *software*. En el ámbito informático es problemático hablar de programas estrictamente <<originales>>, ya que, los distintos programas suelen ser

una sucesión o perfeccionamiento de otros programas anteriores ampliamente conocidos. de ahí la dificultad de distinguir en la práctica, lo que son versiones y programas derivados de los que constituye un nuevo programa original.

- **B)** En lo que atañe a los *derechos* que dimanan de la propiedad intelectual, la LPI distingue dos tipos: 1) *derechos morales,* facultades extrapatrimoniales irrenunciables e inalienables que se desglosan en poderes y atribuciones en orden a: a) la divulgación; b) la paternidad; c) la integridad, y d) la retirada de la obra del comercio, y 2) *derechos patrimoniales,* que hacen referencia a los denominados derechos de la explotación. La Ley no establece un régimen peculiar regulador de los derechos morales derivados de la autoría de programas informáticos, de lo que debe inferirse que para ellos rige la normativa general. Sí regula, en cambio, de forma específica los derechos patrimoniales en orden a su duración y contenido.
- **C)** Por lo que concierne a la *duración* de la protección del *software* se establece un plazo limitado a 50 años.
- **D)** Conforman el contenido patrimonial del derecho de autor de *software* el ejercicio exclusivo de las facultades de explotación que se desglosa en las de reproducción, distribución, comunicación pública y transformación. En concreto, se dispone que el autor, salvo pacto en contrario, no podrá oponerse a que el cesionario de derecho de explotación realice o autorice la realización de versiones del programa, ni de programas derivados. Ello es un cauce para evitar o reducir las trabas que los derechos de autor podrían implicar para el desarrollo de la ingeniería del software. La Ley refuerza la posición del titular del derecho de explotación, intentando evitar la piratería cuando dispone que la reproducción del programa para uso personal, requiere la autorización de éste, a no ser que se trate de la copia de seguridad.

Además, referente al software, nos podemos encontrar con la Directiva 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996 sobre la protección jurídica de las bases de datos (Ver Anexo V), donde se dicta una normativa para la protección de los derechos de autor de las bases de datos (notar que el ámbito es más amplio que únicamente las bases de datos informáticas) y además regula las condiciones de la manipulación (consulta, extracción y/o reutilización) de las citadas.

Para completar la actual situación, conviene resaltar que 4 años después de la entrada en vigor de la LPI, la UE promulgó en 1991 una Directiva sobre la Protección Jurídica de los programas (Ver Anexo VI). Con ella se pretendía contribuir a unificar el marco jurídico protector de éstos, dada la importancia económica de este sector y la disparidad normativa existente en los diversos Estados miembros de la UE. Según esta Directiva éstos deberían haber promulgado normas jurídicas para cumplir lo dispuesto en ella antes del 1 de enero de 1993. Con cierta demora en el cumplimiento de dicha obligación fue promulgada en 1993 la Ley de Incorporación al Derecho español de la directiva de referencia. De acuerdo con la Exposición de Motivos de esta Ley, "la incorporación de la Directiva al ordenamiento jurídico español no plantea excesivos problemas, ya que la gran mayoría de las disposiciones que recoge se contemplan, aunque con otra redacción". Las modificaciones más significativas introducidas por esta Ley respecto al régimen de protección del *software* establecido por la LPI las siguientes:

- En relación con la *titularidad,* introduce una importante variante al establecer que si el programa de ordenador es producto de una obra colectiva, tendrá la consideración de autor, salvo pacto en contrario, <<la persona física o jurídica que la edite y divulgue bajo su nombre>>. Con lo que, a diferencia del régimen derivado de la LPI, se reconoce la autoría de las personas jurídicas respecto a los programas de ordenador.
- En lo concerniente a la *duración* de la tutela, pues el plazo de protección se sigue fijando en 50 años, éstos no se computan desde la publicación del programa o desde su creación de no haberse publicado, sino desde la muerte del autor. Sólo en el supuesto de que el autor sea una persona jurídica, se computa a partir del año siguiente de la publicación o creación.
- También en lo que atañe a los medios de *protección,* esta Ley refuerza las garantías del titular del

derecho de autor, al facultarle para instar el cese de la actividad ilícita, exigir la indemnización proporcionada a los daños causados y solicitar del juez la adopción de medidas cautelares urgentes, pudiendo ser requeridos por la autoridad judicial los informes u ordenar las investigaciones que estime oportunas par la mayor eficacia del procedimiento probatorio.

En esta nueva ley, únicamente se permite hacer una copia de seguridad para ser empleada en caso de que se dañe el original, considerándose las restantes ilegales. La tenencia de programas "copiadores" o dispositivos para copiar programas protegidos es también ilegal. Amparándose en ella, un Juez puede ordenar que se efectúen registros por sorpresa en lugares donde se sospecha que puedan estar utilizándose programas ilegales, para evitar que las pruebas sean destruidas. En enero de 1994, SEDISI y BSA iniciaron una campaña para luchar contra la piratería que constaba de dos fases: una informativa para difundir la ley y concienciar a la gente y otra legal emprendiendo acciones contra quienes la incumplieran. En ese mismo año se efectuaron ocho registros sorpresa en empresas sospechosas del uso o comercialización de programas ilegales para lo que fue necesaria la formación a la Policía Judicial y Guardia Civil sobre técnicas de registro de ordenador y manejo de sistemas informáticos. Además de estos registros se realizaron una serie de redadas en mercadillos donde se tenía constancia de que había tráfico de programas ilegales.

Debe advertirse que para los atentados más graves contra la propiedad intelectual del *software* se prevén sanciones penales (art. 270 del nuevo Código Penal) Se prevé la sanción con pena de multa, a quien deliberadamente reproduzca, plagie, distribuya o publique, en todo o en parte de una obra literaria, artística o científica o su transformación en cualquier tipo de soporte, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios. Asimismo se prevé la sanción de quien, de forma intencionada, importe, exporte o almacene ejemplares de dichas obras sin la referida autorización, y a quien fabrique o disponga medios destinados a suprimir o neutralizar los dispositivos técnicos que protegen los programas de ordenador y que a continuación vamos a repasar brevemente.

- ***PROTECCIÓN Y DESPROTECCIÓN DE PROGRAMAS***

Hasta hace unos años eran numerosos los programas que se comercializaban con algún tipo de protección para impedir su copia. Hoy en día, esto sólo ocurre en contados casos puesto que la protección a menudo presenta una serie de inconvenientes para los usuarios; de hecho en las evaluaciones de productos se valora de forma negativa su empleo. Para evitar las copias ilegales de un programa se emplean diferentes técnicas tanto para impedir la copia de los disquetes como para conseguir que no se pueda trabajar en más de un ordenador por cada licencia adquirida. Otra forma de dificultar la copia ilegal, muy común en los juegos es la necesidad de introducir al comienzo una clave relacionada con un dato proporcionado y que puede encontrarse en algún manual adjunto.

Las técnicas de protección contra copia de los disquetes fueron las primeras en emplearse pero actualmente se utilizan poco, puesto que son las que plantean mayores problemas y son menos eficaces que otras. Esta protección se hacía originalmente formateando los disquetes en un modo no estándar, efectuando marcas láser, o mediante la técnica de los bits débiles, de tal forma que, empleando las herramientas que proporciona el sistema operativo, era imposible reproducir el disco en el mismo estado en que estaba.

Las técnicas de formateo no estándar son las más antiguas y consistían en formatear el disquete alterando el número de sectores de alguna pista, por ejemplo, en un disquete de 31/2 y doble densidad lo normal son 9 sectores/pista; el tamaño de algún sector, normalmente 512 bytes/sector; o el orden lógico de los sectores dentro de la pista (en el disquete que acompaña al libro se puede encontrar un programa que permite formatear un disquete variando estos parámetros). De esta forma, los discos no podían ser copiados con el programa disk−copy del sistema operativo ni con las utilidades de copia de

disquetes, ya que estos sólo permiten copiar discos con valores estándar. En muchos juegos se empleaba esta protección e incluso a menudo los disquetes no contenían ficheros y la única forma de ejecutar el programa era arrancando el ordenador desde el disquete.

La protección por marca láser consistía en hacer una diminuta marca en una determinada posición del disco de tal forma que el programa, al ejecutarse, comprobaba si al leer el contenido de dicha posición se producía un error. Si no se producía el error era porque no se trataba del disquete original y el programa se interrumpía. Una protección similar puede hacerse de forma casera empleando una aguja y comprobando después cuál o cuáles han sido los sectores dañados. El siguiente paso es que el programa a proteger deberá verificar, cuando se ejecute, si se produce un error al leer tales sectores.

Las protecciones anteriores suelen ir unidas a la existencia de un contador con el número de licencias adquiridas que disminuye cada vez que se instala el programa. Esto puede ser un problema, puesto que al estar limitado el número de instalaciones, si se pierde o daña alguno de los ficheros de la aplicación, habría que volver a adquirir el programa.

Esta clase de protecciones no serían útiles si una vez que el programa está instalado en el disco duro pudiera copiarse y ser llevado a otro ordenador, situación que se evitaba haciendo que el programa requiriese para funcionar la introducción en la unidad de disquete uno de los discos protegido contra copia, el llamado disco llave, un método que está en desuso. Otro método es grabar cierta información en alguna zona del disco duro, por ejemplo en el último sector, que el programa consultará cada vez que se ejecute y, si no la encuentra, dejará de funcionar.

También está la opción de almacenar codificada la localización del programa en el disco cuando se instala y cada vez que se ejecuta comprobar si sigue siendo la misma. De esta forma, si se intenta pasar a otro ordenador no funcionará, puesto que es prácticamente imposible que, al volverlo a copiar, que instalado en las mismas posiciones. Esta técnica presenta el grave inconveniente de que, si se defragmenta el disco duro, el programa con toda probabilidad dejará de funcionar puesto que cambiará su localización. Antes de hacerlo habría que desinstalarlo, luego defragmentar y volverlo a instalar; éste, de hecho, es un problema real que ha ocurrido con más de un programa que utilizaba esta técnica al no avisar el fabricante de la situación.

Otro tipo de protección más eficaz y que presenta menos problemas es el uso de un dispositivo conectado a un puerto de comunicaciones (serie o paralelo), conocido como llave y, popularmente, como "mochila". Este método asegura que el programa protegido sólo se ejecutará en un ordenador a la vez. En las primeras protecciones de este tipo el contenido de la llave era una simple memoria PROM con cierta información que el programa protegido intentaba leer al ejecutarse y si no la encontraba se interrumpía. Estas memorias eran fáciles de duplicar pero, actualmente, son mucho más complejas. Las ventajas de las mochilas sobre otros métodos son que la llave es muy difícil que se estropee, que si se daña el programa instalado en el disco duro puede volverse a instalar sin problemas y que si se deterioran los disquetes del programa normalmente puede solicitarse una nueva copia al distribuidor sin tener que pueda instalar en más de un ordenador puesto que la llave garantiza que únicamente se utilizará en uno de ellos a la vez. No hay ningún problema cuando se tienen que usar dos programas que requieran llave puesto que es posible conectar una sobre la otra.

Hace unos años existía una gran variedad de programas comerciales para realizar copias de disquetes protegidos, popularmente conocidos como "copiones", o para saltarse la protección (incluso algunos realizados por empresas informáticas de gran prestigio). En el manual de estos programas se indicaba claramente que su finalidad es posibilitar a los usuarios hacer copias de seguridad de sus programas originales, por si sufriesen algún percance, aunque no era éste el uso normal que se les daba.

Un copión es un programa que intenta hacer una copia exacta de un disquete sea cual sea el formato

que se le ha dado e incluso simulando algunos tipos de errores que pueden formar parte de la protección. Para burlar las protecciones contra copia realizadas con marcas láser y técnicas similares existían programas residentes cuya misión era interceptar las interrupciones de acceso al disco y devolver la misma información que se obtendría si el disco estuviese realmente dañado, engañando de esta forma a la rutina de protección.

Popularmente, se denomina *crackers* a los individuos que se dedican a desproteger programas y dejarlos de forma que se puedan copiar con las órdenes del sistema operativo, aunque este término es más amplio y también se utiliza para referirse a quienes "rompen" o vulneran una protección por cifrado o la de acceso a un sistema. Lo normal es que lo tomen como un reto personal o lo hagan por afición y suelen firmar su acción con un seudónimo. Realmente, este tipo de *crackers* son una figura a extinguir ya que cada vez se protegen menos programas.

Es importante insistir en que de acuerdo con la legislación actual de protección de software se considera **una infracción la puesta en circulación o tenencia de estos programas copiadores y, en general, de cualquier sistema (programa o dispositivo) cuyo fin sea la desprotección.**

- ***REFLEXIONES FINALES***

Al hacer balance de los mecanismos de tutela del *software* se debe reconocer el carácter limitado de su eficacia, es un hecho notorio que en España, al igual que en los demás países tecnológicamente avanzados, el nivel de atentados impunes contra la propiedad intelectual es decisivamente superior al de los casos detectados y sancionados jurídicamente por vía civil o penal. Para que las normas de protección del *software* adquiriesen plena eficacia deberá darse la confluencia de dos factores; en el plano *jurídico* debería partirse de una adecuada técnica legislativa que tipificara de forma completa y correcta los diferentes supuestos de atentado al *software*, así como la actuación diligente de los tribunales. Sin embargo las medidas jurídicas no alcanzarían sus objetivos de eficacia sin la concurrencia de unos determinados datos *sociológicos*. Es sabido que la vigencia del Derecho depende de su arraigo social. La piratería del software será muy difícil de combatir y de desarraigar, mientras no exista una educación y consciencia cívicas contrarias a esa práctica. Hoy, por el contrario, los clubes de usuarios de ordenadores, las aulas informáticas, las propias redes telemáticas (Internet...), actúan de facto como canales institucionalizados para el intercambio ilegal de programas. Las "autopistas de la información", que constituyen un estimulante factor de desarrollo cultural y progreso, tienen su lamentable reverso en la potenciación, prácticamente ilimitada, de cesiones e intercambios ilícitos de programas. Por ello, en la medida en que su coste sea más accesible desaparecerá uno de los principales motivos que incitan a la piratería.

- ***PROTECCIÓN EN INTERNET***

INTERNET, red de redes, actualmente está propiciando el refugio de multitud de acciones punibles que de no ser por el vacío legal que impera el medio serían metódicamente reprendidas. El problema de base radica en la propia naturaleza de dicha red: desde sus albores, INTERNET se ha caracterizado por ofrecer libertad de expresión, no estar sujeta a control gubernamental ni comercial, es decir, INTERNET era de los internautas, que en su mayoría pertenecía a la comunidad científica (debido a que comenzó siendo una red entre Universidades norteamericanas).

Pero las cosas han cambiado mucho desde que INTERNET naciera. El número de usuarios ha crecido (y crece) exponencialmente, las empresas apuestan por esta red de intercomunicación global, incluso la administración la utiliza. INTERNET está de moda. Aparece pues un gran problema: INTERNET ha evolucionado tan rápidamente que no ha sido posible adecuar los instrumentos legales a tal crecimiento, y lo que antaño era una característica muy positiva de INTERNET (la libertad absoluta) actualmente es foco incesante de actividades que se escapan de toda ética humana (hoy en día es

posible encontrar en INTERNET desde páginas de grupos paramilitares hasta incluso instrucciones para fabricar una bomba atómica).

A continuación veremos cuales son los temas más importantes que actualmente el Derecho Informático trata de dar respuesta a la comunidad de usuarios de INTERNET.

- ***PROPIEDAD INTELECTUAL***

En principio, los derechos de propiedad intelectual se aplican en Internet como en cualquier otra parte. Ya existen en Internet textos, imágenes, trabajos gráficos, grabaciones de sonido y software a los que se puede acceder y pronto estarán también disponibles trabajos audiovisuales. Todo esto se beneficia de la protección aportada por el derecho de propiedad intelectual.

Una de las características de Internet es precisamente los problemas que origina respecto a la aplicación de los derechos de propiedad intelectual en una red global. Internet no está gobernada por ninguna autoridad central, ni existe organismo autorizado para rastrear copias ilegales. Aún más, los usuarios de Internet pueden copiar un trabajo y distribuirlo internacionalmente en cuestión de segundos.

Dadas las deficiencias del derecho común, los usuarios de Internet han desarrollado con rapidez códigos de conducta (autorregulación) y buenos modales de red (cibermodales). Esta reacción en los círculos de Internet tuvo como propósito inmediato asegurar el respeto a los derechos de propiedad intelectual con el fin de evitar la pérdida de control del autor sobre su trabajo. La autorregulación y los cibermodales por lo general obligan a los usuarios o a los operadores de sistemas de cómputo que desean copiar o distribuir un trabajo, a respetar todos los derechos del autor, patrimoniales y morales. Estas normas van más allá del derecho tradicional, pues a menudo estipulan la obligación por parte del usuario de solicitar autorización al autor antes de copiar o distribuir un trabajo, incluso en casos donde no se tiene la certeza de que la ley lo requiera.

- *TIPOS DE TRABAJOS PROTEGIDOS EN INTERNET*

Todos los tipos de trabajo en Internet están protegidos, suponiendo que cumplen las dos condiciones mencionadas con anterioridad.

- ♦ Los trabajos escritos están protegidos. Como resultado, el *correo electrónico quedará protegido*, sujeto al debate en torno a la necesidad de copia de seguridad. En cualquier caso, cuando un sistema de correo electrónico hace copias automáticamente y por lo tanto lo guarda, el problema, por lo general, no surgirá. Los archivos anexados al correo electrónico casi siempre implican textos escritos, que también pueden quedar protegidos. Los artículos colocados en los servidores FTP o Web en Internet también están protegidos, al igual que los artículos integrados a una base de datos o a, una página Web.
- ♦ Los trabajos musicales o audiovisuales colocados en Internet o que circulen por Internet están protegidos por los derechos de propiedad intelectual.
- ♦ Las imágenes digitalizadas que circulan por Internet pueden dividirse en dos categorías: la de las imágenes creadas por una computadora y las producidas por medio de la digitalización de documentos en papel. Las imágenes creadas por una computadora subsisten en una forma original que puede quedar protegida; la reproducción electrónica de esas imágenes puede, por lo tanto, constituir una infracción al derecho de propiedad intelectual. La digitalización de imágenes protegidas en un formato legible para una computadora también constituye una reproducción que infringe los derechos de autor, o al menos constituye una creación ilegal de un trabajo derivado. Si se ha puesto la suficiente creatividad en el proceso de digitalización, es posible que el nuevo trabajo obtenga derechos de autor por sí solo.

- La circulación de software en Internet está protegida por los derechos de propiedad intelectual que hemos visto. Esta protección es tan amplia que, en principio, restringe sustancialmente ciertos usos del software en la red.
- Las Bases de datos en Internet, presentan una problemática más compleja:

Principios de protección.

Internet contiene un gran número de bases de datos. En su mayoría son bases de datos en línea convencionales, por lo general disponibles por Telnet, o bases de datos en línea compuestas con páginas Web y elementos que éstas incorporan. En todos estos casos, es necesario distinguir entre tres elementos dentro de una base de datos: el software que gestiona, los datos (el contenido) y la propia base de datos (el contenedor).

El software está sujeto a protección específica ya hemos visto. El contenido estará protegido por sí mismo, independientemente de la base de datos, pues constituye un trabajo protegido por los derechos de propiedad intelectual. Como resultado, el creador de una base de datos debe obtener la autorización del autor de los datos para poder utilizarlos. No obstante, si el contenido no está protegido el creador de la base de datos puede utilizarlo como desee. Todavía más, la Directiva de 1996 (Ver Anexo V) adopta un ordenamiento de las bases de datos de forma que el creador tenga los derechos sobre el contenido y pueda prohibir su extracción sustancial o rehuso por una tercera parte. (Nota: El Consejo de Ministros del 24 de Octubre de 1997 aprobó la remisión a las Cortes Generales del Proyecto de Ley de Incorporación al Derecho español de la citada Directiva 96/9/Ce del Parlamento Europeo y del consejo sobre la protección jurídica de las bases de datos). La finalidad de esta directiva es la armonización de las legislaciones de los Estados miembros en materia de protección de derechos de autor respecto a las bases de datos, ya que considera que actualmente se encuentran insuficientemente protegidas, con la consiguiente incidencia negativa en el funcionamiento del mercado interior. Se definen como bases de datos las colecciones de obras, datos u otros elementos "dispuestos de manera sistemática y accesible individualmente por medios electrónicos o de otra forma".

Pero ¿cuál es el estado legal del contenedor, de la selección y las opciones involucradas en la presentación de la base de datos? ¿Está protegido por sí mismo el proceso de crear una base de datos?

En Estados Unidos, las bases de datos están protegidas, puesto que se les considera como originales en su presentación o composición. En particular, la base de datos debe tener un mínimo de creatividad. En este caso, no se considera que un directorio telefónico sea lo suficientemente original en su compilación.

En consecuencia, las bases de datos más profesionales no estarán protegidas por los derechos de propiedad intelectual, ya que no son originales ni en su selección ni en su composición. Sin embargo, esto no significa que el creador de tales bases de datos quedará privado de todos los derechos legales. En ciertos casos, podría demandar protección de derechos de autor sobre el contenido, y se beneficia de inmediato bajo las leyes europeas, por el derecho a prevenir la extracción ilegal del contenido de la base de datos.

Otro tema de importancia es el estado legal de las páginas Web. Una página Web contiene numerosos enlaces de "hipertexto" que se refieren ya sea a trabajos, documentos o a una arborescencia a otros enlaces de hipertexto. Será necesario considerar separadamente el estado legal de un enlace de hipertexto y de una página Web. En realidad, un enlace de hipertexto es un URL (localizador universal de recursos) y, por lo tanto, no es sujeto de protección por derecho de propiedad intelectual

Al igual que las páginas Web, los enlaces de hipertexto apuntan a documentos ya sea en el mismo o en otro sitio, puesto que constituyen una estructura de acceso a información que casi siempre es original y debería estar protegida como una base de datos.

- *CONTRATOS ENTRE AUTOR Y USUARIO*

Los servidores o usuarios que desean llevar a cabo un acto que está regulado por las leyes de propiedad intelectual deben obtener la autorización del poseedor de los derechos, ya sea explícita o implícitamente.

♦ **Autorización explícita.**

La autorización para distribuir un trabajo, otorgada por su autor a un servidor, debe, en forma ideal, tomar la forma de un contrato, éste es, el camino más seguro para el servidor. De hecho, respecto a la aplicación de la legislación tradicional de los derechos de propiedad intelectual a Internet, un contrato claro y preciso es, una mejor alternativa que la algunas veces impredecible interpretación ofrecida por la jurisprudencia. Estos contratos siempre serán interpretados restrictivamente en favor del autor (por ejemplo, si cede su derecho de reproducción respecto a la impresión de un libro, esto no significa que haya cedido el derecho de reproducción que implica almacenar un libro en una computadora). De forma similar, la cesión de derechos patrimoniales no incluye la cesión de derechos morales, que son inalienables en muchos países.

Respecto a los usuarios, es difícil cerrar un contrato entre cada uno de ellos y el autor en Internet. La autorización explícita tendrá entonces la forma de una nota agregada por el autor, por lo general, al inicio de actividades, especificando los límites (por ejemplo, uso no comercial) dentro de los que se puede utilizar su trabajo.

Existen dos tipos de autorización de software que deben anotarse: *shareware* y *freeware*. El shareware es una forma amplia de publicar programas, la cual permite al creador ahorrarse los usuales costos de mercadotecnia mediante la distribución de su trabajo a través de una red de ordenadores. El autor permite a los usuarios de la red descargar el software y probarlo por algún tiempo. Si el usuario desea seguir utilizando el software, debe enviar un pago al autor; no hacerlo constituye una violación a los derechos de propiedad intelectual. En lo que se refiere al freeware, el usuario no tiene ninguna obligación legal de pagar.

♦ **Autorización implícita.**

La autorización también puede ser implícita. En el contexto de un grupo, por lo común se considera que quien envía una carta al grupo tiene autorización implícita de reproducirla a todos los miembros del grupo. A la inversa, no existe ninguna autorización implícita para que se envíe esa carta a otros colectivos. Se considera que el autor ha autorizado a todos los usuarios de su trabajo a que lo envíen por correo electrónico.

En cuanto al establecimiento de enlaces de hipertexto entre páginas Web, está desarrollándose una doctrina por medio de la cual la construcción de una página Web implica la autorización implícita del autor para que otros creadores de páginas establezcan enlaces a su página, pues la vida en el Web se basa en la posibilidad de unir páginas en cualquier parte mediante enlaces de hipertexto. Es claro que esta teoría podría generar problemas. Un trabajo protegido, reproducido legalmente en una página Web en virtud de la defensa del uso legal, podría quedar unido por un enlace de hipertexto establecido por otro autor en un contexto completamente diferente, como el comercial, donde esta defensa de uso legal ya no se aplica. Esta es la razón por la cual probablemente las reglas de comportamiento recomiendan pedir autorización al autor de una página Web antes de enlazarla a otra página.

Sin embargo, el estado legal de esta autorización implícita no es el mismo en USA que en Europa. Mientras la jurisprudencia estadounidense tiende a admitir con facilidad la doctrina de la autorización implícita, sobre todo en Internet, la europea es más renuente a adoptarla. De hecho, Europa siempre ha adoptado un punto de vista más dogmático sobre los derechos de propiedad intelectual y, por lo tanto, está menos dispuesta a aceptar la cesión implícita.

¿Significa esto que la mayoría de los usuarios de Internet, quienes sólo en contadas ocasiones tienen autorización explícita para descargar un archivo específico, pueden incurrir en penalizaciones? Seguramente no, ya que pueden ser exonerados de la responsabilidad potencial al aplicar ciertos mecanismos legales comunes referentes a obligaciones, como la buena fe, falta de claridad de ley o la renuncia implícita de un derecho. Pese a eso, hay que insistir en que, siempre la mejor solución es la autorización clara y explícita.

- *COPYRIGHT Y CONTROL DE MARCAS*

La posición legal sobre los derechos de autor y marcas en INTERNET coincide con lo dictaminado al respecto en otros ámbitos de aplicación. Es decir, no pueden ser vulnerados los derechos de autor sin previo consentimiento del mismo.

Ahora bien, se plantean una serie de problemas al tratarse de un medio electrónico que permite vulnerar con facilidad estos derechos legítimamente obtenidos. Por ejemplo, por el mero hecho de acceder a las diferentes páginas Web se produce el hecho (transparente para el usuario) de copia de las mismas y de sus diferentes componentes (ya sean imágenes, sonidos, etc...) sean del tipo que sean. Esta copia local de información no se produce por la voluntad del usuario de infringir las leyes al respecto, sino es más bien una característica técnica del sistema (el backup para que el funcionamiento mejore en sucesivos accesos). Entonces, ¿constituye una violación de los derechos de autor el proceder de dicha forma?. Una opinión muy difundida estriba en que como es el autor quien publica dicha información en la Web, es él mismo quien vulnera sus propios derechos, quedando el usuario exento de dicha carga legal. Pero claro, y si no es el autor quien publica esa información, el usuario es tan culpable por realizar esa copia local de información como el que la publicó, aunque no sea consciente de ese hecho el usuario final. Es muy popular ya en INTERNET encontrar infinidad de archivos en un nuevo formato musical, llamado MP3, que comprime el sonido con unos índices muy aceptables de calidad para la velocidad actual de la Red. Estos ficheros a menudo son el resultado de vulnerar los derechos de autor de obras musicales originales, que son publicados indiscriminadamente y sin control, y que plantean el problema legal de no ser una copia exacta (sino una compresión) del original, por lo que esa pequeña diferencia técnica se convierte a menudo en una razón para escapar del control legal de la copia.

Por otro lado, los enlaces de hipertexto que poseen las páginas Web plantean también un problema legal. ¿Es ilegal hacer referencia a una página protegida por los derechos de autor?, ¿tiene la responsabilidad el autor de dicha página de dar el permiso para la inclusión de ese enlace?, ...

Todos estos temas plantean problemas legales que poco a poco serán solventados por reglamentación específica para INTERNET. De momento debemos quedarnos con los llamados cibermodales para encontrar algún ápice de regulación en INTERNET de estos temas.

Actualmente podemos encontrar diversos foros de discusión que tratan de profundizar en estas cuestiones. Como ejemplo citaremos el foro sobre el Copyright abierto por el prestigioso diario The New York Times (CyberTimes Law Journal), que puede consultarse en el Anexo VII.

- ***PRIVACIDAD Y ENCRIPTACIÓN***

Afortunadamente INTERNET, desde que la LORTAD fue promulgada, entra dentro de los preceptos de la ley. Y es que la privacidad en INTERNET se garantiza fundamentalmente gracias a la existencia de la encriptación, proceso por el cual la información se transforma de forma que no es posible la comprensión de la misma a no ser que se posea la clave para su desprotección. Numerosos estándares han surgido para garantizar que las comunicaciones entre usuarios de la Red se realicen de forma segura.

Pero no todo está tan claro en todo este tema de protección de la privacidad. Y es que los mecanismos de encriptación por ley deben estar regulados por la administración. Esto quiere decir que cualquier código de encriptación que se utilice en una comunicación electrónica, ha de estar forzosamente depositado a priori en la administración, por motivos de seguridad nacional. Y claro, este hecho es susceptible de valoración (aunque parezca lógico) por la comunidad internauta, ya que si se vulneran los derechos de privacidad por aquellos que nos los imponen, se produce una pérdida de confianza en el sistema y como no, una merma de las posibilidades infinitas (sobretodo de índole comercial) de la Red. Por ello actualmente no parece que explote el llamado comercio electrónico o e−busines (término utilizado inicialmente por la empresa IBM). Todavía queda mucho por hacer en este tema.

También nos podemos referir a las publicaciones del diario The New York Times en esta cuestión, haciendo alusión al foro de discusión abierto en dicho diario y que plantea estos y otros problemas que se encuentran por el hecho de utilizar la Red de Redes, y que podemos también consultar en el Anexo VII.

- ***LIBERTAD DE EXPRESIÓN (FREE SPEECH)***

El término de libertad de expresión se ha utilizado hasta la saciedad en referencia a INTERNET. Y es que desde sus comienzos, INTERNET pretendía ser un medio de comunicación no regulado y donde se podían expresar las opiniones de forma libre, independientemente del país de origen de quien la expresaba. Solucionaba en parte el problema a la libertad de expresión que se encontraba en algunos países. Si se utilizaba INTERNET (inicialmente para comunicación de la comunidad Universitaria e intelectual) se podía decir lo que se quisiese sin miedo a represalias legales.

La idea de esta libertad de expresión parecía coherente y lógica, pero cuando INTERNET sufre la explosión demográfica con la que actualmente cuenta, se produce un hecho que no se ha de ignorar: la globalidad intrínseca de INTERNET, por lo que la Red está compuesta por multitud de individuos de diferentes etnias, culturas, sociedades que pueden estar contrapuestas, etc... donde se producen inevitablemente fricciones. En este nuevo marco se ha de intentar llegar a un consenso ético (ya que legislar la conducta de todos los grupos sería imposible) de comportamiento por parte de la comunidad cibernauta para que no se llegue a extremos de intolerancia insospechados que puedan producir una involución a la Red INTERNET. Como precedente legal citaremos el caso que se ha resuelto en contra de un ciudadano norteamericano, quien ha sido recientemente encarcelado por 3 años por utilizar INTERNET para exponer las diferencias personales con Bill Gates (Presidente de la corporación Microsoft) y por amenazar de muerte a un Juez que había fallado anteriormente en contra de aquel.

Parece claro que el tema traerá mucha polémica, sobretodo por la supuesta pérdida de esta libertad de expresión a la que se ve avocada INTERNET si no se controla a tiempo.

- ***REGULACIÓN DE CONTENIDOS***

La regulación de contenidos en la red se puede entender también como una forma de control a la libertad de expresión, aducida anteriormente. Pero es de notar algunas características que la diferencian de esta:

- El control de la libertad de expresión se enmarca más hacia la comunicación entre individuos de la Red.
- Los contenidos que puedan poner en peligro la seguridad nacional.
- Los contenidos que pueden perjudicar a algún colectivo legalmente legitimado.
- Los derechos básicos de intimidad de las personas físicas
- Etc...

Y es que, principalmente las consecuencias han obligado a tomar medidas al respecto. De todos es sabido que INTERNET es un medio muy utilizado para la publicación de material pornográfico que tiene como principales perjudicados a jóvenes menores de edad. También es foco para la organización y expansión de grupos sectarios, racistas y/o paramilitares. Muchos otros ejemplos de utilización poco ética de este medio han conducido, a causa del vacío legal que impera, a establecer mecanismos autoreguladores del problema. Como ejemplo podemos citar, con todo respeto a los afectados, la masiva respuesta internauta que se dio contra la organización paramilitar ETA cuando se produjo el asesinato de Miguel Ángel Blanco, bloqueando el servidor donde se alojaban sus páginas Web e incluso modificándolas para poner los lazos azules sobre ellas. Este tipo de control parece más efectivo que un control gubernamental, pero muchas veces incurre también en delito por atentar a la propiedad intelectual y a la intimidad de las personas.

En E.E.U.U. se promulgó una ley conocida como CDA o Communications Decency Act (1996), que pretende fijar unos términos de regulación de los contenidos de INTERNET, y hace referencia explícita a la prohibición entre otras cosas, de la publicación de material visual de individuos menores de 18 años (cualquiera que sea la razón), y de la publicación de material sexual, excrecional o de órganos.

En Europa todavía queda mucho por andar en este tema. De momento podemos confiar en la autoregulación o los denominados cibermodales para asegurar que los derechos básicos de los ciudadanos no sean violados en INTERNET, pero sin cesar en buscar una ley coherente y lógica que regule dicho comportamiento.

- ***DELITOS INFORMÁTICOS***
- ***CONCEPTO DE FRAUDE Y DELITO***

Fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. La definición de delito es más compleja y han sido muchos los intentos de formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible, dada la íntima conexión que existe entre vida social y jurídica de cada sociedad y cada siglo, ya que ambas se condicionan íntimamente.

El artículo 1º del Código Penal dice que "*son delitos o faltas las acciones y omisiones dolosas o culposas penadas por la Ley*". Esta noción de delito es especialmente formal, y no define cuáles sean sus elementos integrantes. En cualquier caso, sus elementos integrantes son:

- El delito es un acto humano, es una acción (acción u omisión).
- Dicho acto humano ha de ser antijurídico, ha de estar en oposición con una norma jurídica, debe lesionar o poner en peligro un interés jurídicamente protegido.
- Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.
- El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y un acción es imputable cuando puede ponerse a cargo de una determinada persona.
- La ejecución u omisión del acto debe estar sancionada con una pena.
- ***FRAUDES Y DELITOS INFORMÁTICOS***

Así que si de forma genérica definimos, **delito es una acción antijurídica realizada por un ser humano, tipificada, culpable y sancionada con una pena.** Podíamos definir **delito informático** como toda acción (acción u omisión) culpable, realizada por un ser humano que cause un perjuicio a personas, sin que, necesariamente, se beneficie el autor, o que, por el contrario, produzca un beneficio a la víctima, tipificado por la ley, que se realiza en el entorno informático y está sancionado con una pena; de lo anterior, se desprende claramente que se producen hechos ilícitos informáticos que podemos considerar que son fraudes, pero que nunca podremos calificar de delitos.

Contemplado el fraude informático en un sentido amplio se pueden formar varios grandes grupos de figuras delictivas claramente diferenciadas:

- **Fraude informático propiamente dicho.**
- **Protección del derecho a la intimidad.**
- **Propiedad intelectual informática.**
- **Acciones físicas contra la integridad de los ordenadores.**
- **Las acciones de los "hackers".**
- **Los virus informáticos y programas análogos.**
- **La sustracción de tiempo de ordenador.**

Se observara que los grupos 2) y 3) derecho a la intimidad y la protección de programas ya los hemos tratado anteriormente, en las seciones 2.3 y 2.2 respectivamente, por lo que ahora nos referiremos a los cinco grupos restantes.

Respecto al grupo 1) el número de posibles fraudes es amplísimo, y sólo está limitado por la imaginación del autor, su capacidad técnica y las medidas de seguridad de la instalación. Los diferentes fraudes los podemos englobar en cuatro grandes grupos básicos:

- ♦ Intervención en los datos de entrada al sistema.
- ♦ Incorporación de modificaciones no autorizadas en los programas.
- ♦ Modificación fraudulenta de la información almacenada en el sistema.
- ♦ Intervención en las líneas de transmisión de datos.

Existen diferentes clasificaciones de los diferentes fraudes, entre ellas, la denominada PARKER que, a pesar del tiempo transcurrido desde que se hizo, podemos decir que aún tiene vigencia, aunque con motivo de la aparición de Internet aparecen nuevas versiones de estos mismos delitos y alguno de ellos esta ya un poco trasnochado. Esta clasificación es:

- Introducción de datos falsos (data diddling)
- Caballo de Troya (Trojan Horse)
- Técnica del Salamí (Salamí techniques o Rouding down)
- Uso no autorizado de un programa "llave" (Superzapping)
- Trampas (Trap Doors)
- Bombas lógicas (Logic Bombs)
- Ataques asíncronos (Asynchronous Attacks)
- Recogida de información residual (Scavenging)
- Filtración de datos (Data Leakage)
- Trasiego de personas (Piggybacking and Impersonation)
- Pinchado de líneas (Wiretapping)
- Simulación y modelado de delitos (Simulation and modeling)

El grupo 4) recoge las acciones físicas contra los propios ordenadores, caso del robo y del sabotaje. El robo, principalmente, se da en unidades o elementos hardware fácilmente transportables, por ejemplo: pantallas, teclados, impresoras, modems, etc., y, menos, en grandes ordenadores. El sabotaje se presenta de muy diversas maneras: destornillador en el ventilador de la unidad central, silicona en un cajero automático, vaso de bebida en una CPU, bomba de plástico, incendio provocado, etc. Obviamente este tipo de acciones no son exclusivas del mundo informático ya se dan también en otros entornos industriales. Para su tipificación hay que remitirse al Código Penal en el que están previstos.

Capitulo aparte merece el grupo 5) relacionado con los "hackers", que ha tenido especial relevancia debido a sus "hazañas", ya que se han logrado introducirse en sistemas supuestamente sofisticados. Se denominan "hackers" a fanáticos de la informática, generalmente jóvenes, que tan sólo con un

ordenador personal, un módem, gran paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informatizado de una empresa o entidad pública, saltándose todas las medidas de seguridad, y leer información, copiarla, modificarla, preparando las condiciones idóneas para realizar un fraude, o bien destruirla.

Podemos considerar que hay dos tipos:

- ♦ Los que sólo tratan de llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad.
- ♦ Los verdaderos delincuentes, que logran apoderarse por este sistema de grandes sumas de dinero o causar daños muy considerables.

Ambos tipos son peligrosos, pues vienen a ser en nuestra época como los piratas de tiempos pasados, cuya peligrosidad mayor estaba en la inseguridad que creaban en el tráfico marítimo. En est caso, la inseguridad la crean en el sistema vertebral de nuestra economía.

El grupo 6) tiene que ver con los virus informáticos (un virus, en biología, es un agente productor de enfermedades contagiosas, comúnmente invisible y filtrable, por lo que el nombre elegido es bastante adecuado). Existen dos tipos de virus: Benignos (molestan, pero no dañan), Malignos (destruyen información o impiden trabajar). Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, incluso, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

El último grupo tiene que ver con el hurto de uso del tiempo de ordenador. Consiste en la utilización sin autorización de un ordenador por un empleado o por un tercero durante cierto tiempo, sin moverlo, beneficiándose de ciertos servicios. Puede llegar a tener una cierta importancia económica.

- ***PECULIARIDADES DE LA CRIMINALIDAD INFORMÁTICA***

Como en otros sectores del Derecho informático, la regulación jurídica de la criminalidad *por o contra* el ordenador presenta determinadas *peculiaridades* debidas al propio carácter innovador que las tecnologías de la información y la comunicación presentan.

- En el plano jurídico−penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales (atentado terrorista contra el ordenador que regula el tráfico aéreo) o la aparición de nuevos delitos impensables antes del descubrimiento de las nuevas tecnologías (virus informáticos, accesos indebidos a procesamiento de datos para alterar su funcionamiento, penetración a sistemas por vías telemáticas, etc.). Por ello la criminalidad informática obliga a revisar los elementos constitutivos de gran parte de los tipos penales tradicionales. Cabe imaginar el estupor de un penalista del pasado siglo ante la mera alusión, hoy tan frecuente en el lenguaje referido a la criminalidad informática, de situaciones tales como: la posibilidad de que existan fraudes en los que el engaño se realiza sobre una máquina y no sobre una persona, de robos de servicios de ordenador, que se realizan sin fuerza en las cosas; o de hurtos de tiempo de ordenador, que se realizan sin fuerza en las cosas, o de hurtos de tiempo de ordenador sin que exista un ánimo de lucro, sino un mero propósito lúdico por quien lo realiza, y sin que se prive al titular de la cosa de su posesión; o hurtos de información, que pueden llevarse a cabo mediante las nuevas redes de comunicación, que atentan contra los derechos de autor y perjudican la competitividad; o hurtos de datos confidenciales o de carácter personal, que ponen en peligro los principios básicos de una sociedad.
- Por tratarse de un sector sometido a constantes fluctuaciones e innovaciones tecnológicas, sus categorías son asimismo efímeras y cambiantes. El hurto de tiempo de ordenador fue uno de los supuestos de criminalidad informática en las primeras etapas de este sector jurídico informático. Pero en la medida en que la evolución informática ha permitido sustituir los ordenadores voluminosos, costosos y accesibles sólo a aquellas empresas o entidades de enorme potencial económico, por los

ordenadores de la cuarta generación, esos supuestos delictivos han perdido importancia. Hoy toda persona puede tener acceso a un ordenador personal que le permite realizar operaciones que hace 20 años eran privativas de equipos muy costosos y sofisticados. Con ello ha dejado de tener relevancia práctica y trascendencia jurídica la utilización de tiempo de un ordenador.

- De otro lado, la criminalidad informática se caracteriza por las dificultades que entraña descubrirla, probarla y perseguirla. Se ha hecho célebre la imagen de Parker de que los sistemas informáticos son como "queso de Gruyère", por las enormes oquedades y lagunas que quedan siempre abiertas a posibles atentados criminales. A la dificultad de descubrir las conductas informáticas delictivas se añade la facilidad de penetrar en algunos de los sistemas informáticos y la personalidad especial de algunos de los delincuentes que pueden considerarse como un subtipo de la delincuencia de "cuello blanco". Conviene también reseñar, al considerar estas peculiaridades político−criminales, que en ocasiones, se han avanzado índices de probabilidad delictiva en relación con la informática. Hace algunos años adquirió notoriedad el estudio realizado por dos especialistas norteamericanos en esta materia. En ese análisis se simbolizaban las Probabilidades de Crimen Informático = P (CI), en función de tres variables: Deshonestidad = D (es decir, la inclinación al delito del personal informático); Oportunidad = O (o sea, la falta de medidas de seguridad en los equipos informáticos); y Motivación = M (que se refiere a los conflictos personales o laborales que pueden incitar a delinquir a los empleados informáticos).
- Si se asigna a cada variable un valor de 0 a 10, se pueden establecer las siguientes ecuaciones:
    - ♦ Personal informático de máxima deshonestidad: d = 10;
    - ♦ Carencia de cualquier medida de seguridad informática: O = 10;
    - ♦ Motivos poderosos en todo el personal para atentar contra los sistemas informáticos: M = 10.

La propia *precariedad y anacronismo* del sistema jurídico penal refuerza la tendencia a no denunciar estos delitos, para evitar la alarma social o el desprestigio que de su conocimiento podría derivarse. Por ello, las más de las veces, las víctimas prefieren sufrir las consecuencias del delito e intentar prevenirlo para el futuro, antes que iniciar un procedimiento judicial. Esta situación dificulta el conocimiento preciso del número de delitos perpetrados y la planificación de las adecuadas medidas legales sancionadoras o preventivas.

- ***PRESPECTIVAS DE FUTURO***

La insuficiencia de los instrumentos penales del presente para evitar y castigar las distintas formas de criminalidad informática supone un reto para la política criminal de los próximos años, a las cuales no pueden ser ajenas los profesionales informáticos. La dificultad de tipificar penalmente situaciones sometidas a un constante cambio tecnológico, la manifiesta insuficiencia de las sanciones en relación con la gravedad y el daño de los crímenes informáticos y la propia inadecuación de los medios penales tradicionales para remediar esta situación determinan que el Derecho penal informático sea un ejemplo manifiesto de *Derecho penal simbólico*.

A modo de conclusión, hay que decir que la amplitud de los atentados perpetrados desde o contra la informática exige una respuesta jurídica adecuada y tecnológicamente solvente. La aparición de la informática distribuida y las redes aumentan exponencialmente el muestrario de delitos, que se producen o se van a producir. Aunque es una evidencia asumida, que el Derecho siempre va por detrás de la sociedad o de la tecnología, no es menos cierto que desde la óptica de la profesión y de la deontología del Ingeniero Informático hay que movilizar urgentemente al Derecho informático, que tiene la obligación de propiciar un programa de política criminal informática, tendente a la propuesta de planteamientos y soluciones normativas que estén a la altura de este reto inaplazable.

- ***TIPOLOGÍA DE TRABAJOS PROFESIONALES***

Un Ingeniero Informático ha de salir preparado para enfrentarse a toda la diversidad de trabajos profesionales con que cuenta la profesión, y que cada vez se amplia (y se ampliará) más, siempre que

el curso de los avances tecnológicos así lo guíe.

Hoy en día la diferencia entre un programador y un analista ha quedado muy difuminada con la aparición del PC, puesto que se ha roto la idea de equipo.

Ahora, con la aparición de las redes y SSDD ha vuelto de otra forma el trabajo en equipo.

Además, en muchos establecimientos de las empresas de T.I. (Tecnología de la Informática), el ascenso de programador a analistas involucra muy poco o ningún cambio en la cantidad de programación requerida para el trabajo, y de hecho se pasa muy poco tiempo realizando el análisis. En estas situaciones, analista es un titulo indicativo del nivel de salario.

Un Ingeniero Informático no ha de conformarse con trabajar de programador pues esta no es su finalidad, aunque puede hacerlo.

Hoy en día cualquier persona puede acabar siendo un programador si se lo propone pues existen muchos medios para conseguirlo, pero este no es el objetivo que ha de perseguir un Ingeniero.

El Ingeniero Informático en España engloba 2 conceptos anglosajones:

- *Electronic Engineer*: que es capaz de diseñar sistemas electrónicos relacionados con las comunicaciones y ordenadores.
- *System Engineer*: Cuya formación profesional es la que se da en Ingeniería del Software.

La Ingeniería Informática abarca un gran abanico de posibilidades, desde el la ingeniería del software, hardware, control y la telemática: analista, diseñador, creador de animaciones, redes, robótica, diseñador de bases de datos,...

Cada uno de ellos tendrá un trabajo profesional diferente, según las preferencias de cada uno, cada ingeniero se orientara en una de las muchas posibilidades que ofrece esta ingeniería, pero todos tendrán la misma base, que al final es lo importante. No se trata de ser especialista en una sola rama, sino ser conocedor del máximo ámbito de materias, relacionadas siempre con la informática, de forma que si surge un problema, aunque no este relacionado con el trabajo que se está realizando, se tenga la base necesaria para solucionarlo, o tener los suficientes conocimientos para poder enfrentarse a él.

Página 34

Comprobar Anexo.

Comprobar Anexo.

Comprobar Anexo.