TEMA 1: INTRODUCCIÓN AL DERECHO INFORMÁTICO

1.1.Introducción.- En la actualidad los términos informática, telemática, ofimática ... están introducidos en el lenguaje popular. Parece que todos intuimos, de una forma u otra, la gran incidencia que tiene el desarrollo tecnológico en la actividad diaria. Sin embargo estos términos no están generalmente bien empleados ni se utilizan en beneficio del desarrollo social.

Aunque la evolución de la informática, entendida como la ciencia de tratamiento automático de la información, es uno de los fenómenos que más ha influido en el vertiginoso cambio social que estamos viviendo, no implica en absoluto su conocimiento ni su aprovechamiento en beneficio de la humanidad.

Debemos, por tanto, adaptarnos a los nuevos métodos que nos proporcionan las técnicas asociadas al ordenador y adecuar la actividad jurídica al desarrollo tecnológico. Por otro lado, de todos es sabido que la información da un gran poder a quien la posee, pero no basta con poseer la información, es necesario también saber manejarla. Actualmente el desarrollo alcanzado en los sistemas de telecomunicación que han permitido que una misma información sea accesible a un gran número de personas está cambiando radicalmente la forma de vida. Si unimos la informática con las posibilidades que ofrece de almacenamiento, tratamiento y recuperación de la información registrada en soportes magnéticos, permite controlar esa información y puede llegar a convertirse en un instrumento de presión y control de masas.

Por todo ello, el interés en regular el mundo de la informática y de aprovechar sus posibles aplicaciones al Derecho, crece llegando a límites insospechados. El impacto que el nuevo entorno de la información puede

tener sobre la sociedad es tan grande que no permite a los juristas vivir ajenos a él.

No hay que olvidar tampoco que en el mundo tecnológico y en su relación con el económico (así en principio se regulaba el hardware, debido a que un buen "aporte económico", y cuando se empezó a comercializar los software fue cuando se empezó a regular este otro campo) se mueven diversos e importantes intereses que el derecho se ve obligado a regular. Parece lógico, por tanto, que el Derecho puede proporcional a la informática una regulación jurídica que es necesaria para su desarrollo. Es lo que se conoce como derecho informático.

El fenómeno informático y su relación con la disciplina jurídica. El fenómeno de la comunicación a través de Internet, el desarrollo de programas para procesar información , y la manufactura y perfeccionamiento de las tecnologías necesarias para hacer esto y muchas otras cosas posibles, no son ajenas al ámbito del derecho.

El estado tutela la actividad creadora del hombre, protegiendo ésta a través de lo que en el ámbito jurídico se denomina **propiedad Intelectual** e Industrial.

El derecho debe regular los nuevos fenómenos.

Por ejemplificar de alguna manera, podemos pensar en:

- la disposición de un bien, sin el consentimiento del propietario del mismo, realizada mediante equipos informáticos.
- El apoderamiento de información contenida en registros electrónicos.
- Destrucción de la información

El Derecho de la Informática puede abarcar un campo de estudio, por lo que la clasificación tradicional en público, social y privado no restringe científicamente esta disciplina.

Conceptos de Derecho Informático.-

El Derecho de la Informática ha sido considerado por algunos autores, como "el conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones". Otros autores lo definen como "conjunto de leyes, normas y principios aplicables a los hechos y actos derivadas de la informática"

Podríamos conceptuar el derecho de la Informática como el conjunto de normas jurídicas que regulan la creación, desarrollo, uso, aplicación de la informática o los problemas que se deriven de la misma en las que existe algún bien que es o deba ser tutelado jurídicamente por las propias normas.

Todavía hoy es cuestionable si existe esta disciplina como tal, por ello, la mayoría de estudiosos de esta materia prefieren estudiar los siguientes puntos:

- Protección jurídica de la información personal
- Protección jurídica del software
- Flujo de datos fronterizos
- Convenios o contratos informáticos
- Delitos informáticos
- Valor de los documentos electromagnéticos (Firma digital)

1.2.Derecho informático: Sus notas distintivas.- El Derecho informático es una materia jurídica dirigida a la regulación de las nuevas tecnologías de la información, es decir, a la informática y a la telemática (combinación de las palabras "telecomunicaciones" e "informática". Disciplina que asocia las

telecomunicaciones con los recursos de la informática). Dentro del derecho informático también se encuentran las sentencias de los tribunales sobre materias informáticas y los razonamientos de los teóricos del Derecho que tienen por objeto analizar, interpretar, exponer o criticar el sector normativo que disciplina la informática y la telemática.

Las fuentes y estructura temática del Derecho Informático afectan a las ramas tradicionales del Derecho:

- Derecho público:
  - Flujo internacional de datos informatizados
  - Libertad informática (defensa frente a eventuales agresiones)
  - Delitos informáticos (tienden a crear un ámbito propio del Derecho Penal)
- Derecho privado:
  - Contrastes informáticos (hardware, software)
  - Protección jurídica de los programas

(Las fuentes y estructuras del Derecho informático no está aparte del "Derecho tradicional", así se inscriben en el ámbito del Derecho público el problema del a regulación del flujo internacional de datos informatizados, la libertad informática o la defensa de las libertades frente a posibles agresiones realizadas por las tecnologías de la información y la comunicación, o los delitos informáticos que tienden a configurar un ámbito propio en el Derecho penal actual. Mientras que en el Derecho privado estarían recogidas cuestiones tales como: los contratos informático, que pueden afectar lo mismo al hardware que al software, dichos contratos pueden ser de compraventa, alquiler, copropiedad, multipropiedad ... Dentro del Derecho privado están también recogidos los distintos sistemas para la protección jurídica de los programas de ordenados, temas que afectan a los

objetos tradicionales de los Derechos civil y mercantil. El hecho de que el Derecho informático afecta a distintas disciplinas dentro del Derecho ha suscitado un debate teórico sobre si se trata de una nueva disciplina jurídica o si por el contrario se trata de un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas. Pueden aducirse las siguientes razones a favor de la autonomía científica del Derecho de la Informática:

- Un objeto delimitado.- Existencia de un objeto delimitado constituido por la propia tecnología de las computadoras, cuyas implicaciones económicas, sociales, culturales y políticas son evidentes, por ello, el Derecho no puede desentenderse de su reglamentación. Una disciplina como la informática que va camino de incidir en casi todos los aspectos de la actividad humana forzosamente tenía que tener su hueco en el mundo del Derecho, 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 tengan una respuesta adecuada dentro de una normativa.

  Dentro de la informática tiene un especial interés la información (que constituye un bien inmaterial). La información se desglosa en dos momentos: El primero referente a dar forma y significada a un determinado mensaje, el segundo dirigido a su transmisión. Se trata de dos etapas de una función única que sería la comunicación. Desde el punto de vista jurídico se puede distinguir entre el contenido del a información, el sujeto que la produce y el destinatario del a misma. Se puede por tanto establecer entre el autor de la información y la información misma una relación de poseedor/posesión, por eso la

información puede ser objeto de transporte, depósito, alquiler ... Así nacen "los derechos sobre la información" que puede decirse que responden a los mecanismos del Derecho privado.

Por otro lado, y desde el punto de vista de la comunicación, se crea una relación necesaria entre el emisor y el receptor. Esta relación plantea importantes cuestiones jurídicas como ¿quién tiene la posición dominante en dicha relación?, ¿puede, quien tenga información, retenerla en lugar de comunicarla?... Surgen, de este modo, una serie de problemas que se insertan en la temática del Derecho público y que dan lugar un "Derecho de la información" que corre el riesgo de entrar en conflicto con los derechos sobre la información.

Por ejemplo, dentro del campo de los derechos sobre la información, estarían: los problemas que suscita la protección de los derechos de los creadores de un programa informático, los contratos para la utilización de los ordenadores ... En tanque que lo referente al flujo interno e internacional de datos y la protección de datos de carácter personal se insertan dentro del derecho a la información. Ambos sectores conforman el objeto general del Derecho de la informática.

- Una metodología específica.- Existe una metodología específica para abordar adecuadamente esta nueva disciplina jurídica. La reglamentación jurídica de la informática deberá adaptarse a la situación de constantes cambios e innovaciones que caracterizan este sector de la tecnología. Por ello, será conveniente que su disciplina normativa responda a unos 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 adoptar los principios a las situaciones que sucesivamente se presenten.

Otro de los aspectos a tener en cuenta, es que tanto la informática como la telemática rebasan los límites de las fronteras nacionales, por ello el Derecho de la Informática debe concebirse como un Derecho internacional, es decir, un Derecho común a todos los países industrializados.

Además (como hemos visto) , el Derecho de la Informática rebasa los términos de la dicotomía Derecho público/Derecho privado. Esta interdisciplinariedad es un rasgo característico del nuevo Derecho de la informática.

- Un sistema de fuentes.- Existencia de unas fuentes legislativas, jurisprudenciales y doctrinales del Derecho del a informática, que en los países más avanzados han conducido a la planificación de cursos Universitarios regulares encaminados a organizar su enseñanza, así como la continua celebración de congresos, coloquios y seminarios dirigidos al estudio de estos materiales normativos.

TEMA 2: PROTECCIÓN DE DATOS

2.1. Introducción.- Con este término no nos estamos refiriendo a la protección de los datos en sí, sino a la protección del a persona titular de esos datos. La persona, a lo largo de su vida, va dejando una estela de datos que se encuentran dispersos, pero que hoy en día con la ayuda de los modernos medios tecnológicos, es posible agrupar y tratar en forma conjunta estudiando a voluntad aquellos aspectos que de un determinado individuo nos interesa conocer.

Mediante la utilización de las técnicas informáticas y de la transmisión de datos entre ordenadores, se puede ejercer un control social y, sin que la persona llegue a enterarse, interferir en su vida.

La complejidad de la sociedad actual nos obliga a proporcionar más o menos voluntariamente determinados datos personales a instituciones públicas o privadas para facilitarnos un servicio determinado con mayores garantías de eficacia. Estos datos son introducidos en ordenadores donde pueden ser procesados y utilizados de forma que escapan a nuestro control.

Por otro lado, la ayuda que proporcionan las comunicaciones y la transferencia de datos entre ordenadores, permite el cruce de ficheros y registros informáticos de manera rápida y sencilla. No cabe duda por tanto, que la persona titular de los datos puede perder totalmente el control sobre la utilización de los mismos y el tratamiento que se los pueda someter.

Todos estos datos, organizados mediante los sistemas de almacenamiento y recuperación dela información deben estar protegidos contra el acceso malintencionado o no, de quienes no están autorizados para ello.

La protección se realiza sobre el dato, para que éste no pueda ser tratado nada más que para aquellos fines y por aquellas personas autorizadas a ello.

Esta necesaria protección es un límite a la utilización de la informática ante el terror de que pueda agredir a la intimidad de los ciudadanos personal o familiarmente y de alguna manera pueda coartar el ejercicio de sus derechos.

Definición.- Entendemos por **protección de datos** "el amparo debido a los ciudadanos contra posible utilización por terceros, en forma no autorizada de sus datos personales, susceptibles de tratamiento automatizado, para de esta forma, confeccionar una información que identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad".

Puntos de interés.-

Se trata de proteger a las personas ante el manejo o manipulación, no autorizada de sus datos personales, pero siempre que estos datos sean susceptibles de tratamiento automatizado o se encuentren en un soporte susceptible de tratamiento automatizado. Es una protección jurídica ante la potencial agresividad de la informática. Si los datos no se encontraran en un soporte susceptible de este tratamiento, no tendría sentido esta protección. Es debido a las características y consecuencias del tratamiento informático de los datos, donde nace esta necesidad de protección. Luego, hay que tener en cuenta, como primordial el efecto que sobre los datos puede tener el tratamiento informático.

En segundo lugar, el resultado de la elaboración de los datos, mediante el procesamiento, debe ser identificable con el titular de los mismos, llegando, incluso a conocer nuevas características de su personalidad o de su entorno ínitimo como consecuencia del mismo.

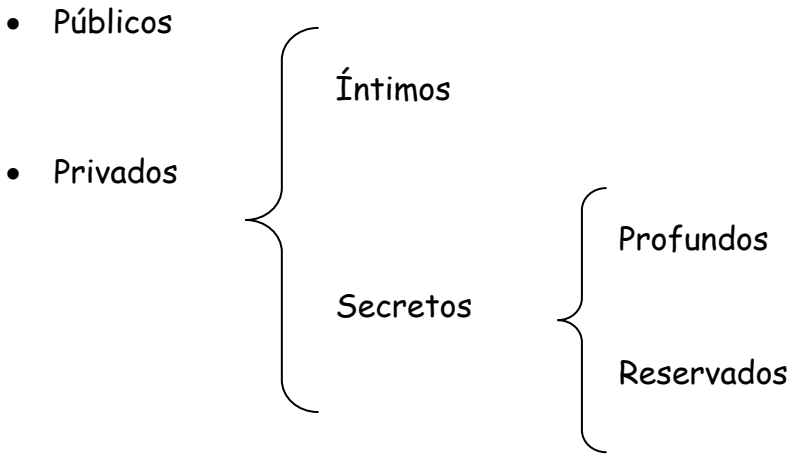
Y en tercer lugar, tiene que darse un manejo de los datos, sin permiso del titular, o para fines diferentes a los que el titular autorizó o se vio obligado a dar los datos.

En resumen tres son las características básicas con las que delimitamos la llamada protección de datos:

a) Que los datos sean susceptibles de tratamiento automatizado, o se encuentren en un soporte susceptible de este tipo de tratamiento.
b) Posibilidad de identificar el resultado del tratamiento de los datos con el titular de los mismos.
c) Manejo o acceso a o datos sin permiso o sin conocimiento del titular independientemente si esto se hace de manera malintencionada o no.

2.2. Clasificación de los datos personales.- Los datos personales pueden clasificarse en categorías de acuerdo con el mayor o menor grado de secreto que tengan asociados por su propia naturaleza, es decir, atendiendo a su confidencialidad. (Entendemos por confidencialidad el mayor o menor grado de secreto con el se van a guardar y tratar los datos personales).

Los datos personales pueden ser:



Los datos personales, son datos que pertenecen a la persona y que son propios de él, pero no todos estos datos pertenecen a la intimidad, así por ejemplo: nombre, apellidos, profesión, son datos personales pero son datos de protección más débil. Por ellos decimos que los datos personales pueden ser públicos o privados:

- Públicos.- Aquellos datos personales que son conocidos por un número cuantioso de personas sin que el titular pueda saber, en todos los casos, la forma de difusión del dato ni puede impedir que, una vez conocido, sea libremente difundido, siendo frecuente su difusión como si no se tratara de datos personales (nombre, apellidos, edad).
- Privados.- Aquellos datos que tienen reguladas las situaciones en las que la persona se ve obligada a darlos siendo la conciencia social favorable a impedir su difusión y respetar la voluntad de secreto de su titular.

Vemos por tanto, que la diferencia básica entre datos públicos y privados, está basada en el mayor o menor grado de secreto a los que lo somete la conciencia social, dependiendo del dato de que se trate.

Ahora bien, los datos privados pueden ser íntimo y secretos, dependiendo también de la mayor o menor confidencialidad a los que se les somete:

- Íntimos.- Aquellos datos que el individuo pueda proteger de su difusión frente a cualquiera, pero que de acuerdo a un fin determinado esté obligado –por mandato legal- a dar periódica o regularmente de sus obligaciones cívicas. (p.ej: Datos bancarios).
- Secretos.- Aquellos datos que el individuo no está obligado a dar a nadie, salvo casos excepcionales, expresamente tasados y regulados en las leyes (p.ej: sólo en presencia de mi abogado).

En ambos casos, los datos privados estarán sujetos a un régimen especial de protección para que sin permiso del titular nadie pueda darlos a conocer a quien no esté autorizado para ello.

Los datos secretos (habíamos dicho con anterioridad) serán a su vez:

- Profundos.- (salud, sexo ...)
- Reservados (ideología, creencia ...). Estos datos, bajo ningún concepto, ni por ningún motivo, está obligado el titular a darlos a conocer a terceros, si no es así su voluntad. No admiten excepciones.

Como resumen, podemos decir que los datos personales son públicos cuando, de acuerdo con el valor que les atribuye la conciencia social, son conocidos por cualquiera y privados aquellos que de acuerdo con ese valor, solamente serán conocidos o por voluntad del titular o en circunstancias especiales (tasadas por las leyes).

Dentro de la categoría de privados, son íntimos los que el titular debe proporcionar periódica y regularmente en el cumplimiento de sus obligaciones cívicas y secretos aquellos que no está obligado a proporcionar si no es su voluntad o en casos excepcionales muy específicos y regulados. De estos últimos hemos determinado reservados aquellos que bajo ningún concepto el titular está obligado a entregar.

El conjunto de leyes se puede considerar dividido en tres generaciones:

a) Al principio se trataba de crear algunos instrumentos con los que establecer límites a la utilización de la informática. Nos encontrábamos con grandes centros de información fáciles de proteger.

   La protección se basaba en la autorización previa de los bancos de datos y su posterior control

b) Comienza la informática distribuida. La protección y seguridad de los datos contenidos en los ficheros y de los propios ficheros se hace más difícil. El grupo de leyes que aparecen ahora reconoce los derechos de acceso y control.
c) La aparición de los ordenadores personales y el hecho de que exista una gran difusión de los bancos de datos dificultan la confidencialidad de la información . Se incide a partir de ahora en la seguridad tanto en los propios bancos de datos como en las líneas de comunicación, proponiendo medidas tanto físicas como lógicas.

2.3.- Leyes de protección de datos en los distintos países.- (Fotocopias)

Efecto internet.-

.Los problemas de orden jurídico que presenta internet son numerosos y afectan prácticamente a todas las ramas de derecho.

.Está pidiendo no un "Derecho supranacional" sino un Derecho de ámbito mundial.

.Efectos perturbadores:

- Aspecto fiscal: Dificultad de control de operaciones mercantiles
- Aspecto financiero –dinero electrónico- Desaparición de bancos centrales.

.Se está intentando coartar la libre circulación (tarea muy difícil)

TEMA 3.- LEY ORGÁNICA 15/1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL. (LOPD)

Esta ley supone una sustancial modificación del régimen sobre protección de datos de personas físicas que se contenía en la extinta LORTAD (Ley Orgánica 5/92 de 29 de Octubre).

Es de destacar el esfuerzo que supone esta norma por introducir firmemente en la cultura jurídica actual unos valores sobre la defensa de la intimidad y privacidad de los ciudadanos y consumidores, a los que reconoce un **conjunto de derechos**. Por otro lado, la ambigüedad y falta de precisión de muchos términos y situaciones descritas en la Ley, hace que su aplicación sea difícil y que las empresas y profesionales afectados tengan que adoptar medidas técnicas y legales para asegurar su cumplimiento.

La Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de Diciembre, (en adelante LOPD) impone una serie de obligaciones legales para aquellas personas físicas o jurídicas que posean ficheros con datos de carácter personal.

Así mismo, desde el 26 de Junio de 1999 está en vigor el Reglamento de Seguridad (R.D. 994/99 de 11 de junio) que desarrolla la mencionada Ley Orgánica y que establece la obligación de las empresas de poner en marcha diversas medidas destinadas a garantizar la protección de dichos datos, afectando a sistemas informáticos, archivos de soportes de almacenamiento, personal, procedimientos operativos, etc.

Esta nueva ley es susceptible de críticas:

- Positivas: Introducción en la cultura jurídica actual de una serie de valores sobre la defensa de la intimidad y privacidad de los ciudadanos.
- Negativas: Ambigüedad y falta de precisión de muchos términos y situaciones descritas en la ley.

A diferencia de USA, la Unión Europea (UE) manifiesta una especial sensibilidad por la protección de la intimidad y datos personales de sus ciudadanos.

A pesar de estas diferencias entre USA y UE resulta necesario alcanzar un acuerdo satisfactorio.

Es previsible que se dicten normas especiales de desarrollo de la LODP, específicamente aplicables al ámbito de las nuevas tecnologías y que los organismos encargados de observar el cumplimiento de la misma presten especial atención a este medio.

P.ej: Los formularios que aparecen en muchas páginas de internet dan lugar a registros de datos especialmente susceptibles de tratamiento, cayendo de pleno, dentro del ámbito de aplicación de la Ley (artículo 2).

- OBLIGACIONES LEGALES DE LA NORMATIVA DE PROTECCIÓN DE DATOS

Inscripción de los ficheros en el Registro General de la Protección de Datos. Artículo 26 LOPD. Artículos. 5 y 6 R.D 1332/1994, de 20 de Junio.

Redacción del documento de seguridad. "*El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de seguridad de obligado cumplimiento para el personal con acceso a los datos*

automatizados de carácter personal y a los sistemas de información" R.D 994/1999, de 11 de Junio.

Redacción de **cláusulas de protección de datos**. Artículo 5 LOPD.

Auditoría. Artículo 17 R.D. 994/1999, de 11 de Junio.

Demás **medidas de seguridad de índole técnica y organizativas** necesarias para garantizar la seguridad de los datos objeto de tratamiento. Artículos 9 y 10 LOPD y R.D 994/1999, de 11 de junio.

Redacción de los **contratos, formularios y cláusulas** necesarias para la recogida de datos, los tratamientos por terceros y las cesiones o comunicaciones de datos.

Extensión del ámbito de aplicación.-

La LOPD cuenta con un ámbito sustancialmente más amplio que la derogada LORTAD.

De acuerdo a las disposiciones de la Directiva 95/46/CE, la LOPD se extiende a supuestos antes excluidos, como ficheros no automatizados.

El autor Emilio del Peso diferencia entre:

*Datos organizados: accesibles directamente mediante un nombre clave

*Datos no organizados: para buscar un dato es preciso buscar uno a uno.

Teniendo en cuenta esta distinción, podemos decir que:

.La LORTAD se refería a datos organizados automatizados

.La LOPD se refiere a datos organizados.

Limitación de los supuestos de exclusión.-

La LORTAD contenía hasta 5 supuestos de exclusión:

1. Partidos políticos
2. Sindicatos
3. Iglesias
4. Titularidad pública

En la LOPD (art. 2.2) se prevén exclusiones para:

1. Ficheros domésticos (mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas)
2. Materias clasificadas
3. Relativo a investigación sobre terrorismo y delincuencia organizada.- En este último caso el responsable del fichero debe comunicar su existencia a la APD (Agencia de Protección de Datos).

Por lo tanto, desde la entrada en vigor de esta Ley Orgánica, se puede afirmar que cualquier fichero, informático o no, tanto empresarial como de otra índole, siempre que almacene datos de personas físicas identificadas o identificables, se encuentra dentro del ámbito de aplicación de la normativa. En el artículo 3 se incluyen las definiciones de los términos que se usan a lo largo de la ley:

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: Aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su

pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación.

Principios.- La ley establece una serie de principios básicos que deben tenerse en cuenta en las tres fases por las que puede atravesar el proceso de los datos:

- Recogida
- Tratamiento
- Comunicaciones y cesiones

1.- Calidad de los datos (artículo 4)

Calidad de los datos.

1. (RECOGIDA DE DATOS). Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. (USO DE LOS DATOS) Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

2.- Información en la recogida de datos (art. 5)

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Excepciones:

a) Si los datos proceden de fuentes accesibles al público (art.3), y se destinen a la actividad de publicidad. No obstante deberá informarse en cada comunicación al interesado del origen de los datos, de la identidad del responsable y de los derechos que le asisten.
b) No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan.

3.- Consentimiento del afectado (art. 6)

Trata del alcance de la obligación de requerir el consentimiento del afectado, que se impone con carácter general para todos los datos.

Existen una serie de excepciones, siempre que no se vulneren los derechos y libertades fundamentales del interesado:

- Recogida de datos para el ejercicio de las funciones de las Administraciones Públicas, en el ámbito de sus competencias.
- Cuando se refieran a las partes en una relación de negocio (contrato de arrendamiento, contrato de trabajo), siempre que sea necesario para el cumplimiento de la relación de que se trate.
- Cuando la finalidad del tratamiento de los datos sea proteger un interés vital del interesado.
- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo.

Aún en estos 4 supuestos, se reconoce al afectado el derecho de quedar excluido del tratamiento de los datos, siempre que una Ley no disponga lo

contrario y existan motivos fundados y legítimos relativos a una concreta situación personal.

4.- Datos especialmente protegidos (art. 7)

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Para los apartados 2 y 3 se establece una importante excepción, dado que se autoriza su tratamiento cuando resulte necesario para la prevención o diagnóstico médicos, presentación de servicios sanitarios ... siempre que el tratamiento lo realice el personal sanitario sujeto al secreto profesional.

En el art. 8, en relación con los datos referidos a la salud, se establece que el tratamiento de estos datos (de salud) se hará de conformidad a lo dispuesto en la legislación estatal o autonómica sobre sanidad.

5.- Comunicación y acceso a los datos (art. 11 y 12)

Estos artículos están dirigidos a regular las condiciones específicas de la utilización de datos recabados por otras personas.

La redacción de estos artículos es bastante confusa.

Se impone, en el art. 11, la obligación de informar al afectado de la comunicación de los datos para fines propios del cedente y cesionario,

excepto si el tratamiento responde a la libre y legítima aceptación de una relación jurídica cuyo cumplimiento y control implique una concesión de dicho tratamiento con ficheros de terceros. Ej: cesión de datos de trabajadores a las compañías aseguradoras.

El art. 12 se ocupa del acceso a los datos por parte de un tercero cuando el mismo sea necesario para la prestación de un servicio al responsable del fichero.

Régimen: Medidas de seguridad.-

En el RD 994/1999 de 11 de junio, se aprueba el reglamento de medidas de seguridad técnica de los ficheros automatizados que contengan datos de carácter personal.

En caso de comprobarse que no se cumplen estas obligaciones, se incurriría en responsabilidades administrativas.

Se definen 3 niveles de seguridad, en función de la infracción tratada y la mayor menor necesidad de garantizar la confidencialidad):

1. Nivel básico: Aplicable por defecto a cualquier fichero en el ámbito de aplicación.
2. Nivel medio: Relativos a la comisión de infracciones administrativas o penales, Hacienda pública, servicios financieros
3. Nivel alto: Ficheros con datos sobre ideología, religión, creencias, salud...

En este Real Decreto se enumeran las medidas técnicas de seguridad que deberán ser implantadas por el técnico encargado de los datos.

(1) Nivel básico:

- Elaboración por parte del responsable de los datos de una normativa de seguridad que se reflejará en un documento de obligado cumplimiento para el personal que tenga acceso.

El documento debe contener al menos:

- Ámbito de aplicación del documento
- Medidas y normas encaminadas a garantizar la seguridad
- Funciones y obligaciones del personal

- Estructura de los ficheros que contienen datos de carácter personal
- Procedimiento de gestión de incidencias
- Procedimiento de realización de copias de seguridad

- Este documento se mantendrá actualizado y se revisará cuando haya cambios que lo afecten.
- El contenido debe adecuarse en todo momento a las disposiciones vigentes en materia de seguridad.

(2) Nivel medio

El documento contendrá, además de lo reseñado para el nivel básico:

- Identificación de los responsables de seguridad
- Controles periódicos para verificar el cumplimiento de lo dispuesto en el propio documento
- Medidas a adoptar cuando se deseche un soporte.

(3) Nivel alto

Se introducen los siguientes requisitos:

- Cifrado de datos
- Registro de accesos
- Copias de seguridad en un lugar distinto de aquel en que se encuentren los equipos informáticos

Plazo de implantación de las medidas:

- Para el nivel básico: 6 meses
- Para el nivel medio: 1 año
- Par el nivel alto: 2 años

- NIVELES DE SEGURIDAD

La ley identifica tres niveles de medidas de seguridad, BÁSICO, MEDIO y ALTO, los cuales deberán ser adoptados en función de los distintos tipos de datos personales (datos de salud, ideología, religión, creencias, infracciones administrativas, de morosidad, etc).

	NIVEL BÁSICO
TIPO DE DATOS	• Nombre • Apellidos • Direcciones de contacto (tanto físicas como electrónicas) • Teléfono (tanto fijo como móvil) • Otros
MEDIDAS DE SEGURIDAD OBLIGATORIAS	• Documento de seguridad • Régimen de funciones y obligaciones del personal • Registro de incidencias • Identificación y autenticación de usuarios • Control de acceso • Gestión de soportes • Copias de respaldo y recuperación

	NIVEL MEDIO
TIPO DE DATOS	• Comisión infracciones penales • Comisión infracciones administrativas • Información de Hacienda Pública • Información de servicios financieros
MEDIDAS DE SEGURIDAD OBLIGATORIAS	• Medidas de seguridad de nivel básico • Responsable de Seguridad • Auditoría bianual • Medidas adicionales de Identificación y autenticación de usuarios • Control de acceso físico

	NIVEL ALTO
TIPO DE DATOS	• Ideología • Religión • Creencias • Origen racial • Salud • Vida
MEDIDAS DE SEGURIDAD OBLIGATORIAS	• Medidas de seguridad de nivel básico y medio • Seguridad en la distribución de soportes • Registro de accesos • Medidas adicionales de copias de respaldo • Cifrado de telecomunicaciones

Movimiento internacional de datos.-

No pueden realizarse transferencias temporales ni definitivas de datos de carácter personal a países que no proporcionen un nivel de protección equiparable al que presta esta ley, salvo autorización del Director de la Agencia de Protección de Datos (APD), que la otorgará sólo si se tienen las garantías adecuadas.

La APD ha desarrollado unas normas por las que se rigen los movimientos internacionales de datos (instrucción 1/2000, de 1 de diciembre).

AGENCIA DE PROTECCIÓN DE DATOS (APD)

La Agencia de Protección de Datos es un Ente de Derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones Públicas.

El **Director de la Agencia de Protección de Datos** dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años. Ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

Son **funciones de la Agencia de Protección de Datos**:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

El Registro General de Protección de Datos.

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos

a) Los ficheros de que sean titulares las Administraciones Públicas.

b) Los ficheros de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

INFRACCIONES Y SANCIONES.-

Se establecen una serie de sanciones a los responsables de los ficheros y a los encargados del tratamiento de los ficheros que contengan datos de carácter personal. Estas se clasifican en leves, graves y muy graves , atendiendo a la infracción cometida.

LEVES.-

1. No atender a una solicitud legal de rectificación o cancelación de datos personales.
2. No proporcionar información solicitada por la APD.

3. No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no constituya infracción grave.
4. Recoger información de datos de carácter personal sin proporcional la información que se señala en esta ley (art. 5)
5. Incumplir el deber de secreto del art. 10 salvo cuando constituya infracción grave.

Sanción: Multa de 601,01 € a 60.101,21 € (100.000 a 10.000.000 de pesetas)

GRAVES.-

1. Crear ficheros de titularidad privada o recoger datos de carácter personal para su creación sin autorización de una disposición general.
2. Crear ficheros de titularidad privada o recoger datos de carácter personal para su creación con una finalidad distinta al objeto legítimo de la empresa.
3. Recoger datos de carácter personal sin consentimiento del afectado, cuando éste sea exigible.
4. Tratamiento indebido de los datos de carácter personal cuando no constituya infracción muy grave.
5. Impedir u obstaculizar el derecho de acceso.
6. Mantener datos de carácter personal inexacto cuando resulten afectados los derechos de las personas amparables por esta ley.
7. Vulnerar el deber de secreto sobre datos de carácter personal de ficheros que contengan datos de Hacienda Pública, Comisión de infracciones, Solvencia patrimonial ...
8. Mantener los ficheros con datos de carácter personal sin las debidas condiciones de seguridad.

9. No remitir a la APD las notificaciones que prevé la Ley o cuantos documentos requiera.
10. Obstaculizar la función inspectora.
11. No inscribir el fichero de datos de carácter personal en el Registro General de Protección de datos cuando lo requiera el Director de la APD.
12. No informar debidamente al afectado cuando los datos no los facilite el mismo.

Sanción: de 60.101,21 € a 300.506,05 € (10.000.000 a 50.000.000 pesetas)

MUY GRAVES.-

1. Recogida de datos engañosa y fraudulenta.
2. Comunicación o cesión de datos de carácter personal fuera de los casos permitidos
3. Tratamiento de datos de carácter personal especialmente protegidos sin atender al contenido del art. 7 de esta Ley.
4. Continuar con el uso ilegítimo de tratamiento de datos de carácter personal cuando hay sido requerido por la APD.
5. Transferencia internacional de datos a países que no proporcionen un adecuado nivel de protección.
6. Tratamiento ilegítimo de los datos de carácter personal
7. Vulnerar el deber de guardar secreto de datos de carácter personal especialmente protegidos (art. 7) así como los recabados para fines policiales.
8. No atender de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
9. No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Sanción: de 300.506,05 € a 601.012,10 € (50.000.000 a 100.000.000 de pesetas)

Esta cuantía de sanción se graduará atendiendo a la naturaleza de los derechos que se afectan, al volumen de datos, al beneficio obtenido, intencionalidad, reincidencia, daños y perjuicios ...

	SANCIONES
LEVES	Multa de 601,01 € a 60.101,21 € (100.000 a 10.000.000 de pesetas)
GRAVES	Multa de 60.101,21 € a 300.506,05 € (10.000.000 a 50.000.000 pesetas)
MUY GRAVES	Multa de 300.506,05 € a 601.012,10 € (50.000.000 a 100.000.000 de pesetas)

Es de vital importancia que las empresas que recojan datos de carácter personal se adecuen a la normativa de protección de datos ya que la Agencia de Protección de Datos es muy estricta e impone multas de elevada cuantía a todas aquellas que no la cumplan.

ADECUACIÓN DE FICHEROS PREEXSTENTES.-

El plazo en el que deben adecuarse los ficheros y tratamientos automatizados, estén o no inscritos en el Reglamento General de Protección de Datos, será de 3 años. En el caso de ficheros y tratamientos no automatizados deberán adecuarse en un plazo de 12 años a contar desde el 12 de octubre de 1995.

CLI (Comisión de Libertades e Informática)

Es una plataforma independiente de carácter no gubernamental, cuyo objetivo es promover el desarrollo y protección de los derechos individuales y colectivos, con especial referencia al derecho a la intimidad, frente al uso de las tecnologías informáticas y de las comunicaciones.

FIRMA ELECTRÓNICA.-

Real Decreto : Ley 14/199 de 17 de septiembre. Regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación.

Es de aplicación a los Prestadores de Servicios de Certificación.

Esta ley no altera las normas relativas a los contratos y otros actos jurídicos.

El anterior Real Decreto 14/1999 de 17 de Septiembre sobre firma electrónica será actualizado con una normativa que aunque contempla pocas novedades, aprovechará para aportar más seguridad jurídica. La novedad más sustancial y la que mas llama la atención a priori es la creación de un "**DNI electrónico"** cuya función principal es la de autentificarnos en las relaciones telemáticas que mantengan los ciudadanos españoles con la administración.

Definiciones legales.-

- Llamamos *firma electrónica* al conjunto de datos utilizados para identificar al autor del documento.
- *Firma electrónica avanzada:* aquella que permite identificar al signatario y que éste mantiene exclusivamente bajo su control.
- *Signatario.-* Persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o de tercero.

- *Datos de creación de firma.-* Son los datos únicos privados, que el signatario utiliza para crear la firma electrónica.
- *Dispositivo de creación de firma.-* Es un programa o una máquina que sirve para aplicar los datos de creación de firma.
- *Dispositivo seguro de creación de firma.* Idem pero reuniendo una serie de requisitos.
- *Datos de verificación de firma.-* Son los datos públicos que se utlizan para verificar la firma.
- *Dispositivo de verificación de firma.-* Programa (o máquina) que sirve para aplicar los datos de verificación de firma.
- *Certificado.-* Certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad.
- *Certificado reconocido.-* Es un certificado que contiene la información del art. 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos del artículo 12.
- *Prestador de Servicios de Certificación.-* Persona física o jurídica que expide certificados u otros servicios.
- *Producto de firma electrónica.-*Programa o máquina utilizado por el Prestador de Servicios de Certificación (PSC).
- *Acreditación voluntaria del PSC.-* Resolución que dicta el organismo público de supervisión.

PROTECCIÓN DE DATOS PERSONALES.- En el texto de la Ley se indica que el tratamiento de datos personales debe estar sujeto a lo dispuesto en la LORTAD, ya que esta Ley es anterior a la LOPD.

TEMA 4: PROTECCIÓN JURÍDICA DEL SOFTWARE

4.1. INTRODUCCIÓN

La problemática de los programas de ordenador es uno de los temas más debatidos en el Derecho Informático.

Es un problema relativamente reciente ya que hasta hace poco se infravaloraba la importancia económica del software.

Fue IBM, en los años 60, la primer que hizo facturaciones separando hardware y software.

Existen intereses para que se lleve a cabo la protección jurídica del software, como:

1. Interés por parte de la empresa dedicada a elaborar software, sobretodo teniendo en cuenta el capital invertido en investigación y la facilidad con que se hacen copias de software.
2. Interés del programador, porque se reconozca la "paternidad" del software a efector de promoción profesional, aunque los derechos de explotación pertenecen a la empresa para la que trabaje.
3. Interés genérico para el avance de la investigación para evitar incidir en repeticiones.

Los programas son bienes inmateriales, difíciles de encuadrar dentro de lo que existe, ya que se tienen características que los identifican con la actividad industrial y otras que lo acercan más al ámbito de la propiedad intelectual.

Así, si se considera a los programas (software) como invenciones que implican una actividad inventiva susceptible de aplicación industrial, estarían sujetos a la legislación sobre patentes (Ley 11/1986 de 20 de marzo).

Si los consideramos una creación original, literaria, artística o científica, estará protegida por la Ley de la Propiedad Intelectual (RD Legislativo 1/1996 de 12 de abril).

La tendencia va dirigida a encuadrar el software en el segundo grupo (Propiedad Intelectual):

- En USA se intentó patentar un programa que traducía cifras en representación decimal a código binario equivalente. El Departamento de patentes rechazó la protección bajo patentes, ya que los algoritmos deben tratarse como parte integrante de un proceso mental (creación abstracta).
- En Francia, ya en 1967, se excluía expresamente al software de la protección ofrecida por los derechos de patentes.
- En nuestra legislación se excluyen expresamente los programas de ordenados de la Ley de Patentes (art. 4.1), sin embargo sí se han patentado procedimientos completos, en los que una parte se desarrolla por medio de un programa de ordenador.

Ventajas de proteger el software con las leyes de la Propiedad Intelectual:

1. El plazo de protección es mayor que los derechos de propiedad industrial
2. Copias no autorizadas.- Es necesario recalcar la facilidad con la que se pueden hacer copias o utilizar un programa como base para desarrollar uno nuevo bajo otro nombre y por personan que no tienen ningún derecho sobre él.
3. Nacimiento de la protección en forma automática.- La protección intelectual nace en el momento en que la idea es expresado en un soporte, sin necesidad de someterla a ningún formalismo para que sea objeto de protección.

4. Pocas obligaciones por el titular.- El titular no necesita realizar ninguna acción para estar protegido por las disposiciones de las Leyes de Propiedad Intelectual.

Legislatura Comunitaria.-

El Consejo de las Comunidades Europeas adoptó una directiva (14 de mayo de 1991) sobre la protección jurídica de programas de ordenador, con el fin de unificar los criterios en los países miembros.

LOS PROGRAMAS DE ORDENADOR EN LA NORMATIVA SOBRE LA PROPIEDAD INTELECTUAL.-

Hecho generador.- La Propiedad Intelectual de un obra, corresponde a su autor por el solo hecho de su creación.

Autor.- Persona natural que crea alguna obra literaria, artística o científica. No obstante, el beneficiario puede ser otra persona jurídica según prevé esta misma ley.

Objeto (art. 10).- Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro:

a) Libros, folletos, escritos
b) Composiciones musicales
c) Obras teatrales
d) Obras cinematográficas
e) .....
i) Programas de ordenador

Derechos de explotación.- Corresponde al autor el ejercicio exclusivo de los derechos de explotación de su obra (reproducción, distribución, comunicación pública y transformación).

TÍTULO IV: Programas de ordenador

Objeto de protección.-

Definición (**Programa**).- Un programa es una secuencia de instrucciones o indicaciones destinadas a ser utilizadas directa o indirectamente en un sistema informático para realizar una tarea o para obtener un resultado determinado.

La expresión "programas de ordenador" comprende también la documentación preparatoria (documentación técnica y manuales de uso).

La protección se aplica a cualquier forma de expresión de un programa y se extiende a versiones sucesivas y a programas derivados de ellos, excepto los creados con el fin de ocasionar efectos nocivos.

Cuando los programas formen parte de una patente o un modelo de utilizada gozarán de la protección del régimen jurídico de la propiedad industrial.

También se protegen las ideas y principios en los que se basan.

Titularidad de los derechos.-

Se considera autor a la persona o grupo de personas naturales que lo hayan creado o la persona jurídica que se contemple como titular de los derechos de autor.

Los derechos de autor sobre un programa que sea resultado de la colaboración entre varios autores corresponderán a todos ellos en ls proporción que determinen.

"*Cuando un trabajador asalariado cree un programa de ordenador en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondiente al programa de ordenador así creado, tanto el programa fuente como el programa objeto, corresponderán exclusivamente al empresario, salvo pacto en contrario".*

Duración de la protección.-

1. Cuando el autor sea una persona natural, la duración de la protección es toda la vida del autor + 70 años después de su muerte.
2. Cuando el autor sea una persona jurídica → 70 años desde el 1 de enero del año siguiente a la divulgación lícita.

Derechos de explotación.-

El titular tendrá derecho a realizar o autorizar:

a) Reproducciones totales o parciales
b) Traducción, adaptación, arreglo o cualquier otra transformación
c) Cualquier tipo de distribución pública, incluido alquiler del programa o de sus copias.

Se entiende que cuando se produzca una cesión del derecho de uso de un programa, ésta tiene carácter no exclusivo e intransferible.
En la Unión Europea, la primer venta de una copia de un programa por el titular de los derechos agotará el derecho de distribución de dicha copia, excepto el derecho de controlar los alquileres que se hagan con esa copia.

Límites a los derechos de explotación.-

-No necesitan autorización del titular la reproducción o transformación (incluso la corrección de errores), cuando dichos actos sean necesarios para la utilización legítima del usuario.
-No podrá impedirse la realización de una copia de seguridad por parte de un usuario con derechos.
-El autor, salvo acuerdo, no puede oponerse a que el titular de los derechos de explotación realice o autorice la realización de versiones sucesivas o programas derivados del mismo.

Protección registral.-

-Los datos sobre programas de ordenados y sobre sucesivas versiones o programas derivados, podrán ser objeto de inscripción en el Registro de la Propiedad Intelectual.

Infracción de los derechos.-

-Poner en circulación una o más copias sabiendo que no son originales.
-Tener, con fines comerciales, una o más copias de naturaleza ilegítima.
-Poner en circulación o tener, con fines comerciales, algún instrumento cuyo uso sea facilitar la supresión o neutralización de cualquier dispositivo técnico utilizado par proteger el programa.

CÓDIGO PENAL.-

Recoge los delitos relativos a la Propiedad Intelectual.

Art. 270.- Señala que será castigado con prisión de 6 meses a 2 años o multa de 6-24 meses, quien, con ánimo de lucro y en perjuicio de terceros, reproduzca, plagie, distribuya o comunique públicamente en todo o en parte, una obra literaria, artística o científica en cualquier tipo de soporte o comunicada a través de cualquier medio, sin autorización de los titulares de los derechos.

La misma pena a quien almacene, importe o exporte ejemplares de dichas obras sin la referida autorización.

En este mismo artículo se señala que se castigará con la misma pena a quien tenga o distribuya dispositivos técnicos para suprimir la protección de programas de ordenador sin autorización del autor.

Art. 271.- Se impondrá pena de:

- Prisión de 1 a 4 años
- Multa de 8 a 24 meses
- Inhabilitación profesional de 2 a 5 años

Cuando ocurra alguna de las siguientes circunstancias:

a) Que el beneficio obtenido posea especial trascendencia económico
b) Que el daño causado revista especial gravedad

En estos casos el juez podrá decretar el cierre temporal o definitivo de la industria o establecimiento del condenado.

BSA (Business Software Alliance)

Business Software Alliance (BSA) es la principal organización dedicada a promover un mundo en Internet seguro y legal.

BSA forma a los usuarios de ordenadores sobre los derechos de autor del software y sobre la seguridad cibernética, apoya la política pública que fomenta la innovación e incrementa las oportunidades de negocio y lucha contra la piratería de software.

BSA aglutina a las principales compañías del sector que ofrecen programas y servicios informáticos: Adobe, APP Systems, Lotus, Microsoft ...

Las campañas que BSA lleva a cabo en cada país, con el fin de erradicar el delito informático, tienen 3 vertientes muy definidas:

- Difundir las leyes de protección jurídica de programas de ordenador y promover y apoyar el cumplimiento de las leyes.
- Incrementar la conciencia pública de los beneficios que reporta el uso de programas originales, informando sobre las desventajas de la utilización de copias ilegales.
- Emprender acciones legales contra aquellas organizaciones que comercializan copias ilegales de programas, así como contra las que los compran o utilizan.

GNU (la otra cara de la moneda)

Este proyecto surgió a mediados de los 80 en el MIT (Massachussets Institute of Technology).

En un principio (años 70), el software que se desarrollaba se vendía con acceso a sus fuentes (soft libre) con las ventajas: conocimiento, mejora, ayuda (colaboración entre usuarios).

Esto cambió en la década de los 80, ya que aparecieron empresas con otra filosofía: "Si usted comparte con el vecino, usted es un pirata. Si desa algún cambio ruéguenos para que lo hagamos nosotros".

Lo que pretendía este proyecto era la creación del software libre, que lo será cuando el usuario posea las siguientes libertades:

(1) Para ejecutar el programa con cualquier propósito
(2) Para modificar el programa y adaptarlo a sus necesidad, lo que requiere la posibilidad de acceder a las fuentes, ya que en caso contrario se hace excesivamente complicado.
(3) Poder redistribuir copias, tanto gratis como por un canon.
(4) Libertad para distribuir versiones modificadas, de forma que la comunidad pueda beneficiarse de sus mejoras.

Este proyecto partió del sistema UNIX porque era un sistema multiusuario y multitarea, y estaba extendido entre los usuarios desde hacía muchos años.

Algunas partes de GNU no están programadas directamente para el proyecto y se tomaron algunas ya desarrolladas como X Windows.

Al comenzar la década de los 90 ya se disponía de todos los componentes principales de GNU, ya fueran programados para el proyecto o disponibles como soft libre, exceptuando el kernel (núcleo del sistema operativo).

En este momento cuando el finlandés Linus Torvalds comenzó a desarrollar el kernel Linux.

Combinando Linux con el resto del sistema GNU, se tiene un sistema operativo completo. Es lo que se denomina GNU/Linux, aunque habitualmente se suele encontrar (erróneamente) como Linux.

Clases de software.-

1. Free software.- Permite al usuario copiar, modificar, distribuir copias del programa (código fuente disponible). No quiere decir que sea gratuito.
2. Soft de dominio público.- Es soft no protegido bajo copyright. No es lo mismo que soft libre. Dominio público es un término legar y significa ausente de copyright.
3. Soft bajo copyleft.- Copyleft usa la ley del copyright pero le da la vuelta para servir a lo opuesto del propósito usual, i.e, en lugar de ser un medio para privatizar el software, se transofmra en un medio de mantener el software libre. La idea es que le damos a cualquiera el permiso de ejecutar el programa, copiarlo, modificarlo, distribuir versiones modificadas, pero no se le da el permiso de agregar restricciones propias (por tanto, las versiones modificadas también deben ser libres). La implementación específica de copyleft, que se utiliza para la mayoría del software GNU, es la licencia pública general (licencia GPL), ej: GNU GPL.

4. Software libre (que no está bajo copyleft).- Es el caso de compañías que han utilizado software libre (como X Windows) y lo han convertido en software propietario.
5. Software semi-free.- Permite a los usuarios, usar, modificar y redistribuir para propósitos sin ánimo de lucro (estrictamente no es free software)
6. Software propietario.- El uso, modificación y redistribución, está prohibido y requiere la adquisición de un permiso.
7. Software shareware.- Permite a los usuarios probar y realizar copias pero requiere que todos los que decidan usar el programa adquieran una licencia de uso. Suele distribuirse sin fuentes y no permite modificarlo ni redistribuirlo.
8. Software comercial.- Desarrollado como un negocio.

Observación: ¡El software libre puede ser comercial!