



# INSTITUTO DE LA DEFENSA PÚBLICA PENAL

# Introducción de las Nuevas Tecnologías en el Derecho

Lic. Omar Ricardo Barrios Osorio

## Módulos de Autoformación

Programa de Formación del Defensor Público

Módulo de Autoformación

**Introducción de las nuevas tecnologías en el derecho**

Autor

**Lic. Omar Ricardo Barrios Osorio**

1<sup>a</sup>. Edición, año 2010

(copyright) 2010 ©

Ciudad de Guatemala

Licda. Blanca Aída Stalling Dávila  
Directora General IDPP

Lic. José Gustavo Girón Palles  
Coordinador de UNIFOCADEP

Mediación Pedagógica

**UNIFOCADEP**

Tratamiento del Contenido

**M.A. José Gustavo Girón Palles**  
Coordinador UNIFOCADEP

Tratamiento del Aprendizaje

**Capacitadores UNIFOCADEP**  
Lic. Hugo Roberto Saavedra  
Lic. José Alfredo Aguilar Orellana  
Lic. Idonaldo Fuentes  
Lic. Hans Aaron Noriega

Revisión y Corrección

**Dr. Arturo Higueros García**

Tratamiento de la Forma

**Diseñador Gráfico**  
**Luis Fernando Hurtarte**



## Instituto de la Defensa Pública Penal



Módulo  
**Introducción de las nuevas tecnologías en el derecho**  
**(Aspectos técnicos y legales básicos)**

Guatemala, C.A.



## PRESENTACIÓN

La visión del Instituto de la Defensa Pública Penal incluye la profesionalización de las defensoras y defensores públicos. En 2010 dio inicio el sistema de carrera del defensor público, que en su plan de estudios comprende diversas áreas como la jurídica, de desarrollo humano, ética, y el área técnica que contiene este Módulo denominado “Introducción de las nuevas tecnologías en el derecho”.

Trata sobre la tecnología de la información y las comunicaciones, introduce al lector al derecho informático y la informática jurídica, los programas del ordenador y datos personales, los documentos y firmas electrónicas, delitos informáticos, el ciber delito y los delitos mediante el uso de las nuevas tecnologías. De ahí la importancia de derechos fundamentales como el acceso a la información pública y el derecho a la intimidad, en donde la informática es imprescindible no solo para el defensor público sino para el Sistema de Justicia ya que facilita el archivo y control de expedientes o casos que se atienden, y permite el acceso a todo tipo de información tanto a nivel de la Internet y facilita la comunicación fluida entre distintas sedes, unidades técnicas y administrativas del Instituto.

Mediante el uso de éstas tecnologías se realizan contrataciones, licitaciones, negocios, notificaciones y hasta demandas utilizando la firma electrónica. Se reciben declaraciones de testigos y se producen documentos electrónicos que producen prueba en diversos juicios.

De la protección de datos personales, del uso de programas informáticos se deducen derechos y obligaciones que al ser violados constituyen actos antijurídicos del derecho en general y hasta delitos. De ahí la importancia de una formación de las defensoras y defensores públicos en áreas técnicas que tienen relación con el derecho. Con toda seguridad, la publicación de este material educativo contribuye a la profesionalización integral del defensor público y de la sociedad Guatemalteca.

Licda. Blanca Aída Stalling Dávila  
Directora General



# Introducción de las nuevas tecnologías en el derecho

Instituto de la Defensa Pública Penal

## **Siglas y abreviaturas utilizadas**

Art.	Artículo
CANG	Colegio de Abogados y Notarios de Guatemala
CE	Comercio Electrónico
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional –UNCITRAL-
CONCYT	Consejo Nacional de Ciencia y Tecnología
CPRG	Constitución Política de la República de Guatemala
HTML	Hypertext Markup Language
HTTP	Hiper Text Transport Protocol
ICANN	Internet Corporation for Assigned Names and Numbers
LAIP	Ley de Acceso a la Información Pública
LDADC	Ley de Derechos de Autor y Derechos Conexos
Ley Modelo	Ley Modelo de la CNUDMI para el Comercio Electrónico
LGT	Ley General de Telecomunicaciones
LRCFE	Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas
OMC	Organización Mundial de Comercio
OMPI	Organización Mundial de la Propiedad Intelectual
ONU	Organización de Naciones Unidas
PC	Computadora Personal
PSI	Proveedor de Servicios de Internet
RD-CAFTA	Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos de América
TCP/IP	Transmision Control Protocol / Internet Protocol
URL	Uniform Resource Locutor
UNCITRAL	Siglas en inglés para identificar la CNUDMI.
WWW	World Wide Web



# Introducción de las nuevas tecnologías en el derecho

Instituto de la Defensa Pública Penal

## ÍNDICE

	<b>Página</b>
Introducción	13

## Capítulo I

### **LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES (Aspectos básicos)**

Contenido del capítulo	17
Objetivos específicos	19
1. La sociedad de la información y la sociedad del conocimiento	21
2. La Informática	22
3. La información y los datos	22
3.1. Los tipos de datos	
3.2. Unidad de medida de los datos informáticos	
3.3. Almacenamiento de los datos o información	
4. Los Sistemas de Información	25
4.1. Elementos de un Sistema de Información	
4.2. El ordenador o computadora	
4.3. Las redes de computadoras	
4.4. Dispositivos de almacenamiento de los datos o información	
4.5. El sistema informático del IDPP	
5. Introducción a las Tecnologías de la Información y Comunicaciones –TIC-	29
5.1. Las telecomunicaciones	
5.2. El ciberespacio	
5.3. La digitalización	
6. Aspectos básicos sobre la Internet	32
7. Aplicaciones y relación de la Internet en el Derecho	33
8. Los nombres de dominio (ND)	38
8.1. Estructura de un nombre de dominio	
8.2. La administración y el registro de un nombre de dominio	
8.3. Conflictos derivados del registro o uso de nombres de dominio	
<b>Ejercicios de Autoaprendizaje</b>	<b>43</b>

## Capítulo II

Página

### INTRODUCCIÓN AL DERECHO INFORMÁTICO Y LA INFORMÁTICA JURÍDICA

Contenido del capítulo	47
Objetivos específicos	49
1. El Derecho Informático	51
2. Contenido del Derecho Informático	51
3. La Informática Jurídica	53
4. Clasificación de la Informática Jurídica	53
5. La Informática Jurídica de Gestión	54
6. La Informática Jurídica Documental	57
7. La Informática Jurídica Decisional	
8. El uso de Internet para el profesional del Derecho	61
8.1. La Internet como medio de comunicación	
8.2. El acceso a fuentes de información	
8.3. La comercialización de los servicios profesionales	
8.4. La Internet como objeto de estudio del Derecho.	
8.5. Estudios e investigación jurídica on line (en línea)	
Ejercicios de Autoaprendizaje	65

## Capítulo III

### LOS PROGRAMAS DEL ORDENADOR Y LOS DATOS PERSONALES

Contenido del capítulo	69
Objetivos específicos	71
1. Los Programas del Ordenador (Software)	73
2. Aspectos legales de los programas del ordenador	73
3. Clasificación de los Programas del Ordenador	75
4. Procedimientos para solucionar controversias derivadas de los derechos sobre los programas del ordenador.	81

**Página**

5. Los datos personales	83
5.1. Definición de datos personales	
5.2. Los datos personales públicos	
5.3. Los datos personales privados	
6. La protección de datos personales; especial referencia a la protección por el uso de TIC	86
6.1. El derecho a la protección de los datos personales	
6.2. El Habeas Data	
6.3. Riesgos tecnológicos para la protección de los datos personales	
6.3.1. La tecnovigilancia	
6.3.2. Los correos electrónicos y su responsabilidad	
7. Aplicación de la Ley de Acceso a la Información Pública en el ámbito informático	93
<b>Ejercicios de Autoaprendizaje</b>	99

## **Capítulo IV**

### **LOS DOCUMENTOS Y LAS FIRMAS ELECTRÓNICAS**

Contenido del capítulo	103
Objetivos específicos	105
1. El comercio electrónico y el gobierno electrónico	107
1.1. El comercio electrónico	
1.2. El gobierno electrónico	
2. Los documentos electrónicos, mensajes de datos y/o comunicaciones electrónicas	112
2.1. Los documentos electrónicos	
2.2. Definición de documentos electrónicos y mensaje de datos	
2.3. Situaciones distintas entre documentos creados mediante ordenadores	
2.4. Los documentos electrónicos privados y públicos	
3. Las formas de manifestar la voluntad en el ámbito electrónico	117
4. Aspectos esenciales de la firma electrónica	118
4.1. La firma en el contexto actual	
4.2. Definición de firma	
4.3. La firma autógrafa	
4.4. Objeto y características de la firma autógrafa	
4.5. Clasificación de las firmas	
4.6. La seguridad y la firma electrónica	

	Página
4.7. Definición de la firma electrónica	
4.8. Sujetos que participan en la firma electrónica	
4.9. Los certificados de la firma electrónica	
4.10. ¿Cómo funciona la firma electrónica?	
4.11. Clases de firmas electrónicas	
5. Aspectos relevantes de la Ley de Comunicaciones y Firmas Electrónicas	125
<b>Ejercicios de Autoaprendizaje</b>	<b>127</b>
 <b>Capítulo V</b>	
<b>LOS DELITOS INFORMÁTICOS, EL CIBERDELITO Y LOS DELITOS MEDIANTE EL USO DE LAS NUEVAS TECNOLOGÍAS</b>	
Contenido del capítulo	131
Objetivos específicos	133
1. Los delitos informáticos y los cibercrimenes	135
2. Definición de delitos informáticos	135
3. Los sujetos responsables en los delitos tecnológicos	135
4. Clasificación de los delitos informáticos	137
5. Los delitos informáticos en el Código Penal	138
5.1. Delito de alteración de programas	
5.2. Delito de reproducción de instrucciones o programas de computación	
5.3. Programas destructivos	
5.4. Destrucción de registros informáticos	
5.5. Uso de información	
5.6. Manipulación de la información	
5.7. Registros prohibidos	
6. Delitos cometidos utilizando las TIC como medio o instrumento	145
7. Otros delitos relacionados con las TIC	146
8. El cibercrimen	147
9. Proyectos o iniciativas de ley con relación a los delitos informáticos	147
9.1. Iniciativa de Ley contra el cibercrimen	
9.2. Iniciativa de Ley de delitos informáticos	
<b>Ejercicios de Autoaprendizaje</b>	<b>151</b>
<b>BIBLIOGRAFÍA</b>	<b>153</b>

## INTRODUCCIÓN

Los abogados y abogadas litigantes cada día exploramos nuevas áreas del conocimiento humano en nuestro ejercicio diario; semanas atrás conocemos un caso de lesiones culposas y tenemos que estudiar aspectos de Medicina y Biología lo que deriva al final en una especialidad como la medicina forense; ayer asesoramos en un caso de estafa y defraudación tributaria y nos adentramos en la Auditoría y en la especialidad tributaria; hoy nos presentan un caso de reproducción ilegal de programas de ordenador o una afectación al derecho de la intimidad en una página web y nos corresponde adentrarnos en la Informática, pero sobre todo, en el mundo de Internet, y otra vez, a conocer las bases técnicas y legales de esta área del conocimiento; pero ¿en qué actos de la vida diaria se utilizan las tecnologías?, es más sencillo preguntar en qué ámbitos no utilizamos las tecnologías de la información y comunicaciones –TIC- o en su caso, ¿en mi ejercicio profesional cómo aplico las tecnologías?

El presente capítulo tiene por objeto brindar las soluciones iniciales a los abogados y abogadas defensores públicos, desarrollando una temática que brinda los aspectos iniciales y fundamentales para entender elementos técnicos y legales de las TIC.

Los contenidos se agruparon conforme a una relación ordenada e influida por la experiencia y los estudios en esta temática. En el capítulo I, se proporcionan los elementos técnicos y la terminología informática relacionada con la temática.

El capítulo II parte de los elementos y los estudios doctrinarios en la relación Informática y Derecho, como base para la comprensión de los fenómenos sociales que se ven influidos por esta convergencia, además de iniciarse con la influencia que genera Internet en el Derecho. La importancia de los programas de ordenador y de los datos personales que se utilizan en las redes y en los sistemas informáticos se explica en el capítulo III. La digitalización de las actividades y de los actos que realizan las personas por medio de las TIC, se explica en el capítulo IV.

En las bases documentales que se proporcionaron para el desarrollo del presente modulo, no se solicitó el tema de los Delitos Informáticos, pero por su importancia y el crecimiento de las conductas ilícitas, se incluyó esa temática en el capítulo V.

Es innegable que Internet ha cambiado muchos aspectos de nuestras vidas, del trabajo, la profesión, formas de comunicación y hasta relaciones sociales, pero esa experiencia de adentrarse en el ciberespacio puede ser aprovechada en conjunto como una herramienta para establecer un ejercicio profesional que fomente el Estado de Derecho que todos deseamos.



## CAPÍTULO

# 1

### LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES – Aspectos básicos –

Lo que caracteriza a la revolución tecnológica actual no es el carácter central del conocimiento y la información, sino la aplicación de ese conocimiento e información a aparatos de generación de conocimiento y procesamiento de la información/comunicación, en un círculo de retroalimentación acumulativo entre la innovación y sus usos...

Los empleos de las nuevas tecnologías de las telecomunicaciones en las dos últimas décadas han pasado por tres etapas diferenciadas: automatización de las tareas, experimentación de los usos y reconfiguración de las aplicaciones.

En las dos primeras etapas, la innovación tecnológica progresó mediante el aprendizaje por el uso. En la tercera etapa, los usuarios aprendieron tecnología creándola y acabaron reconfigurando las redes y encontrando nuevas aplicaciones...

Las nuevas tecnologías de la información no son sólo herramientas qué aplicar, sino procesos qué desarrollar. Los usuarios y los creadores pueden convertirse en los mismos. De este modo, los usuarios pueden tomar el control de la tecnología como en el caso de Internet.

Manuel Castells, 2005



## CONTENIDO DEL CAPÍTULO

En las ciencias jurídicas, hemos estudiado instituciones y conceptos como delito, gobierno, contrato, firma, entre cientos de ellos, además de prepararnos para desarrollar procesos y procedimientos y cada una de sus etapas o actos, como elaborar un memorial de demanda hasta una sentencia, recibir una notificación o participar en un audiencia de declaración de testigos por mencionar solo unas ideas; pero las definiciones y procedimientos se han investigado y realizado desde que la esencia del Derecho mismo existe, realizándose en forma oral y escrita, utilizando nuestra voz, escribiendo un memorial a mano, máquina de escribir mecánica o eléctrica hasta llegar al uso de un procesador de textos, herramienta básica en una computadora personal. Hasta ahí, la influencia de la tecnología se limitaba a facilitar nuestras actuaciones como abogadas y notarias o abogados y notarios, redactando y almacenando en forma digital nuestros clásicos expedientes procesales llenos de hojas de papel, todo impreso en formato átomos; pero la tecnología se desarrolla en forma constante y logra facilitar los procesos de comunicación, nos logró conectar en forma fácil y accesible a través de computadoras y redes que se encuentran instaladas en nuestro trabajo, centro de estudio y ahora en nuestro hogar, inclusive, nos conectó a través del desarrollo de la telefonía móvil o celular, ese conjunto de elementos electrónicos y señales digitales para conectarnos, transmitir la información y datos, se representa en un concepto: Las Tecnologías de la Información y Comunicaciones, denominadas TIC.

Pero, ¿qué efecto tienen en nuestro trabajo jurídico? Se convirtieron en una parte intrínseca para realizar en forma óptima el mismo trabajo, desarrolló nueva figuras jurídicas y transformó otras; ahora trabajamos con los mismos conceptos del inicio de este párrafo, pero adicionando el elemento tecnológico como delito informático, gobierno electrónico, contrato celebrado en línea, firma digital y qué decir de los procedimientos de demanda firmada electrónicamente y enviada vía Internet, notificación electrónica en su domicilio digital, o bien participar en un audiencia de declaración de testigos en videoconferencia; sí, estamos cambiando, porque no solo debemos usar la tecnología, tenemos una participación activa en su desarrollo y evolución; por ello, los jurisconsultos debemos involucrarnos y no quedarnos aislados, en especial en el Derecho Penal en donde principios rectores de los procesos que diligenciamos todos los días como la economía procesal, la celeridad, y la inmediación procesal, que se desarrollan a través de los medios que nos proporcionan las TIC.





## Objetivos Específicos

- a) Proporcionar los conocimientos teóricos, técnicos y legales que permitan contar con las herramientas básicas de las Tecnologías de la Información y Comunicaciones.
- b) Aportar los fundamentos de la Internet y su estructura funcional para establecer su incidencia en la actividad del defensor público.



Introducción de las nuevas tecnologías en el derecho  
Instituto de la Defensa Pública Penal

## LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES (Aspectos básicos)

### 1. La sociedad de la información y la sociedad del conocimiento

Existen múltiples formas de estudiar o enfocar los cambios derivados del uso de las tecnologías basadas en la información digital, puntos de vista sociológicos, económicos, históricos, prácticos, entre otros; términos de uso actual como sociedad de la información o sociedad del conocimiento se utilizan de distintas formas. Se denomina sociedad de la información, a la actividad que realizan las personas al contar con acceso al uso de las Tecnologías de la Información y Comunicaciones combinado con la utilización adecuada de las mismas, permitiéndoles crecer y desarrollarse dentro de una organización social que cada día exige un mayor grado de formación y la correcta utilización de las fuentes de información y administración de las bases de datos.

En virtud de la idea anterior, la sociedad de la información no es sinónimo de la sociedad del conocimiento, es una organización social más compleja, derivada de una serie de cambios relacionados desde los productivos-económicos, pasando

por los tecnológicos (esencialmente en sus formas de procesamiento y almacenamiento<sup>1</sup>), hasta la forma de comunicación de sus integrantes, quienes actúan en conjunto para producir una conjunción de información y acceso a las bases de datos para convertirlas en una base de conocimientos en que todos se benefician, pero que a la vez aportan cambiando sus actitudes de individualización del saber a la pluralidad, es decir, aplicar la información a la realidad.<sup>2</sup>

Esa multiplicidad de ideas o enfoques sobre los conceptos referidos también tiene sus críticas o detractores, pueden incluso ser considerados como metáforas, alusiones e inclusive ficciones. Lo expresa en forma clara J. Gimeno Sacristán al indicar que la “expresión sociedad de la información es una de las metáforas que en estos momentos se utiliza para caracterizar lo que se considera que es una condición nueva de la realidad social; como si aludiera a rasgos asentados de la misma, sin aclarar exactamente en qué consiste y de qué manera una sociedad como la nuestra es en verdad de la información, en qué sentido y para quiénes lo es.” (2005).

También se atribuye el uso de los conceptos como una construcción de marketing para lograr mejores ventas en productos tecnológicos y despertar necesidades en los usuarios. Lo que sí puede considerarse relevante y necesario es la participación activa del Estado a través de los órganos competentes para fomentar y proporcionar

---

<sup>1</sup> Considero importante resaltar el almacenamiento digital de la información y su procesamiento en línea, porque ello derivó en un impulso acelerado de administración y accesibilidad del conocimiento.

<sup>2</sup> Manuel Castells indica al respecto de la sociedad del conocimiento: “Precisando un poco más, se trata de una sociedad en la que las condiciones de generación de conocimiento y procesamiento de información han sido sustancialmente alteradas por una revolución tecnológica centrada sobre el procesamiento de información, la generación del conocimiento y las tecnologías de la información. Esto no quiere decir que la tecnología sea lo que determine;...” (CASTELLS. 2002)

las herramientas necesarias para que la sociedad en general pueda acceder al uso de las TIC, y con ello, colaborar para cerrar la denominada brecha digital.<sup>3</sup>

## 2. La Informática

Conforme fueron avanzando las sociedades, las ciencias, los estudios y las investigaciones, se van acumulando volúmenes considerables de información y datos, por lo cual la administración de la data se hizo necesaria realizarla de procedimientos eficientes y óptimos surgiendo, así la Informática,<sup>4</sup> considerada en el inicio como una técnica para almacenar datos, pero en la década de los sesenta con el surgimiento de las computadoras basadas en la electrónica, se constituye como una ciencia a tal punto que en las universidades se incorporan estudios especializados, por ejemplo, en Guatemala, la Ingeniería en Sistemas, y Licenciaturas en Informática, entre otros.

Actualmente, el objeto esencial de la Informática es proporcionar los procedimientos y las técnicas que intervienen en el proceso de recopilación, utilización y procesamiento de datos a fin de tomar decisiones con la información o datos procesados. La Real Academia Española la define como el “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.” (RAE, 2009) La Informática puede definirse como la ciencia que estudia los procedimientos de automatización de los datos y la información, para posteriormente

procesarlos y acceder a ellos para la toma de decisiones.

### 3. La información y los datos

Siendo el objeto de la Informática el procesamiento de la información a través de la administración de los datos, es importante establecer qué debemos entender por estos conceptos. El diccionario de la Real Academia Española indica que la palabra información proviene del latín informatio, -onis- y significa la “acción y efecto de informar o informarse; averiguación jurídica y legal de un hecho o delito; comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.” (2009) En los procesamientos automatizados, la información se define como el conjunto de datos alfanuméricos, numéricos y/o lógicos, que representan la expresión y construcción de conocimientos que pueden utilizarse para la toma de decisiones. Podemos establecer que para que exista información es necesario proveerla de datos; el concepto de dato proviene del latín Batum que significa “lo que se da”; por este concepto puede definirse como una “unidad mínima de información, sin sentido en sí misma, pero que adquiere significado en conjunción con otras precedentes de la aplicación que las creó.” (Diccionario de Informática, 1995).

<sup>3</sup> En noviembre de 2007 se presentó el estudio denominado Agenda Nacional de la Sociedad de la Información y del Conocimiento de Guatemala.

<sup>4</sup> El término Informática tiene su origen en el idioma francés (1962); la palabra Informatique es un término formado por dos elementos (acrónimo) y traducida de forma académica significa INFORmación y AutoMATIQUE que significa información automática (BARRIOS, 2006).

### 3.1. Los tipos de datos

Existen varias formas de clasificar los datos, siendo una con relación a la información de las personas clasificándose en datos públicos, datos personales, datos reservados, entre otros, lo cual explicaremos en otra unidad. En el presente caso, nos interesa la clasificación de datos en el momento de almacenarse digitalmente como archivos electrónicos, o en las denominadas bases de datos utilizando programas de ordenador y los campos correspondientes.

Las clases de datos que se contemplan en la Informática al almacenarse por medio del uso de software son: datos alfanuméricos, datos numéricos y datos lógicos. Los primeros son datos que se almacenan en forma indistinta con el uso de letras, números o símbolos; son datos alfanuméricos los nombres de las personas, lugar de nacimiento, texto de escrituras públicas, número de cuentas bancarias. Los datos numéricos representan solamente números enteros o reales con los cuales pueden realizarse cálculos matemáticos, estadísticos, contables, y financieros.

Por último, los datos lógicos representan solamente dos valores o simplemente dos opciones, es decir, están limitados a ese número de probabilidades (verdadero o falso, soltero o casado). La explicación anterior es necesaria para comprender el “tamaño” o espacio del archivo electrónico en los dispositivos de almacenamiento.

### 3.2. Unidad de medida de los datos informáticos

Los datos al almacenarse en medios magnéticos o digitales por medio de programas de ordenador, se “guardan” mediante pulsos eléctricos o electromagnéticos, pero a cada dato almacenado se le denomina Byte, siendo esta última la unidad de medida identificable para el usuario en virtud que un Byte<sup>5</sup> representa una letra, un número o un símbolo.

El sistema de medidas es necesario, en especial, para describir el tamaño de un archivo, la capacidad de un dispositivo de almacenamiento, el espacio para instalar un programa de ordenador, la cantidad de memoria de trabajo (RAM) de un computador, entre otros; por lo anterior, el Byte también tiene medidas de conversión, similares analógicamente al sistema métrico decimal, pero la información almacenada digitalmente no parte del sistema decimal, sino del sistema binario. En la Informática, se puede determinar con exactitud el tamaño de un archivo, o de un dispositivo de almacenamiento, pero en la práctica es común utilizar las aproximaciones al sistema decimal por ser de mayor facilidad en su cálculo.

En la siguiente tabla de conversión, se muestran las formas de cálculos aproximados:

---

<sup>5</sup> Un Byte es representado por ocho bit; este último es la unidad más pequeña en que se divide un Byte y consiste en una representación lógica del lenguaje máquina por lo cual se describe solamente a través del sistema binario en un 0 (apagado o igual a 2 voltios) o un 1 (encendido o igual a 5 voltios). Bit es la contracción de los términos en idioma inglés BInary digiT.

Abrev.	Medida	=	Aproximado	Exacto
B	Byte	=	Un carácter (Letra, número o símbolo)	8 bits (0–1)
KB	Kilobyte	=	1,000 Bytes	1,024 Bytes
MB	Megabyte	=	1,000 KB	1,048,576 Bytes
GB	Gigabyte	=	1,000 MB	
TB	Terabyte	=	1,000 GB	

### 3.3. Almacenamiento de los datos o Información

En Informática, se ingresan datos y cuando están procesados, o se toman decisiones con ellos, se denomina información; para ordenarlos y acceder posteriormente en ellos se almacenan en archivos, siendo estos últimos identificados como archivos informáticos y se definen como el espacio de memoria permanente de un dispositivo que almacena información en forma digital. Al almacenarse, grabar, guardar o salvar (save) un conjunto de datos que conservan relación entre sí, es necesario realizarlo en un archivo (file). El archivo debe identificarse con un nombre, el cual queda almacenado en un directorio o carpeta (inclusive pueden existir subdirectorios), en el cual no podrán existir dos archivos con idéntico nombre. Por ejemplo si un abogado defensor redacta un memorial en un procesador de textos que contiene un recurso de apelación, en el momento de grabarlo lo hará identificándolo con un nombre: recurso 1 o apelación especial 1. Si redacta otra, lo guardará con otro nombre: recurso 2 o apelación especial 2. Esto le permite ir almacenando en orden sus archivos y la carpeta podrá recibir un nombre como recursos 2009; también es

conveniente que el usuario al trabajar sobre un archivo base, grabe el nuevo con un nombre distinto para no afectar su original anterior para poder contar con una copia electrónica de su actividad laboral, archivo electrónico de procesos, y en el caso de los notarios y notarias, inclusive un protocolo digital, por ejemplo,

Archivo	Nombre del Archivo	tamaño	fecha
	Recurso 1	240KB	01-01-2009
	Revisión medida 2	126KB	31-12-2009

Carpeta (Mis Documentos)	Nombre del Archivo	tamaño	fecha
	Actas		03-07-2007
	Recursos2009		13-02-2009
	Caso-Miranda2010		20-03-2010

#### 4. Los Sistemas de Información

En el presente tema, nos referimos a un sistema de información automatizado o informático, es decir, que se utilizan TIC en su operación y se conocen como Sistemas de Procesamiento de Información (Information Process Systems –IPS- por sus siglas en inglés). La importancia de ello deriva que los ordenamientos legales utilizan varios términos para identificar a un sistema de información o informático. Un ejemplo lo encontramos en el Código Tributario (Decreto Número 6-91 del Congreso de la República) que establece en el artículo 93, segundo párrafo:

También constituye resistencia a la acción fiscalizadora de la Administración Tributaria cualquier acción u omisión que le obstaculice o impida el acceso inmediato a los libros, documentos y archivos, o al sistema informático del contribuyente que se relacionan con el pago de impuestos, así como la inspección o verificación de cualquier local, establecimiento comercial o industrial, oficinas de depósitos, contenedores, cajas registradoras y medios de transporte, en los casos en que la Administración Tributaria deba requerir el acceso inmediato, para evitar el riesgo de la alteración o destrucción de evidencias.

Otro ejemplo lo encontramos en la Ley de Acceso a la Información Pública (Decreto Número 57-2008 del Congreso de la República):

**Artículo 39. Sistemas de información electrónicos**

Los sujetos obligados establecerán como vía de acceso a la información pública, entre otros, los sistemas de información electrónicos.

Un sistema informático o sistema automatizado de información se define como el conjunto de elementos tecnológicos que tiene como objeto, realizar procedimientos sobre datos o una base de datos, ejecutados por personas, denominados comúnmente usuarios y que tienen buscan optimizar la administración de la información y los recursos para la toma de decisiones, garantizar la integridad de la data, e inclusive, su transmisión y comunicación. En la legislación nacional, existen definiciones, por ejemplo, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas (Decreto Número 47-2008 del Congreso de la República) establece:

##### Artículo 2. Definiciones

Para los efectos de la presente ley, se entenderá por:

###### Sistema de Información:

Todo sistema que sirve para generar, enviar, recibir, archivar, o procesar de alguna otra forma, comunicaciones electrónicas.

#### 4.1. Elementos de un Sistema de Información

Existen diversos criterios en cuanto a los elementos de un sistema de información, pero en forma básica se integran por: hardware, software, usuarios, información o datos, y la documentación técnica.



El hardware es el conjunto de elementos físicos que integran un computador (monitor, CPU, teclado, impresora, entre otros). Por ello, comúnmente se denomina el elemento físico o tangible. El software es el conjunto de programas de ordenador que se utilizan en computación para procesar los datos e información (sistemas operativos, paquetes, utilitarios, etc.) y que interactúan entre el usuario y el hardware. El usuario u operador es la persona o conjunto de personas que utilizan las funciones y aplicaciones del sistema informatizado. El acceso o uso que se autorice a cada uno de los usuarios se determina por el administrador del sistema. La información es el conjunto de datos que se utilizan en el sistema para desarrollar un trabajo o actividad específica.

Cabe agregar que la información es un activo de difícil valoración o tasación, por lo que es importante establecer las medidas de seguridad del sistema sobre la administración y accesibilidad a los datos. La documentación técnica o manuales, son las instrucciones, procedimientos e información necesaria para la correcta operación de una o varias de las aplicaciones de los programas de ordenador que integran el sistema informático. Un sistema informático debe incluir los mecanismos y los procedimientos de seguridad a utilizar para la protección de la información, en especial los relacionados con copias de seguridad o backups, accesibilidad por nivel de usuarios, evaluaciones de seguridad; cobran actual relevancia los aspectos legales del sistema, donde se analizan aspectos como derechos

de autor del sistema informático, propiedad, responsabilidades sobre la data que se administra, procedimientos de licenciamiento, responsabilidades laborales y administrativas de los usuarios, entre otros.

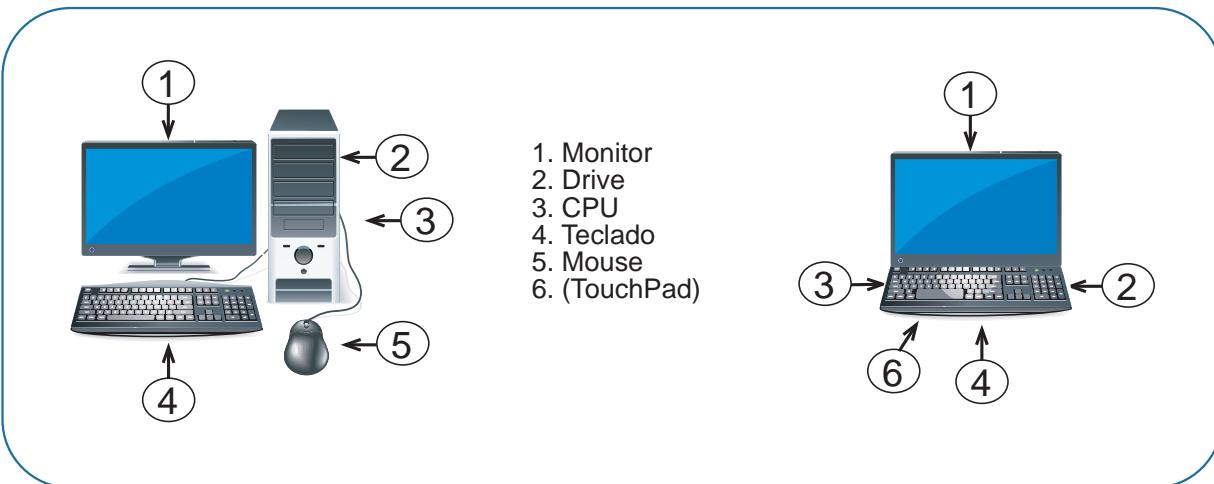
#### 4.2. El ordenador o computadora

En los sistemas informáticos, el ordenador o computadora es uno de los elementos más visibles; se define como el equipo o máquina utilizada por la informática que puede ser considerada como herramienta, medio de comunicación o centro de entretenimiento, por medio de la cual se procesan los datos que se proporcionan y brinda los resultados (información) como se ha programado. Los elementos esenciales de una computadora son el hardware, software, dispositivos periféricos y los dispositivos de almacenamiento.

El hardware y el software fueron definidos en el punto anterior; los periféricos son los dispositivos que pueden ser conectados al CPU<sup>6</sup> y que permite la comunicación entre él y el usuario; existe una gran variedad, siendo los principales, el monitor, el teclado, el mouse y la impresora, sin excluir una amplia variedad que complementa la función de cada sistema como escáner, lápiz óptico, cámaras, micrófonos, lectores de impresión dactilar, entre otros.

<sup>6</sup> CPU (Central Processing Unit): Siglas en inglés que identifican a la Unidad Central de Proceso o por decirlo de otra forma el “cerebro” de la computadora. Este término se utiliza de forma común para identificar al gabinete o case de una computadora en donde se encuentran instalados la tarjeta madre, microprocesador, memoria de trabajo, puertos para conectar los periféricos entre otros.

Gráfico  
Partes Básicas de un Ordenador o Computadora Personal



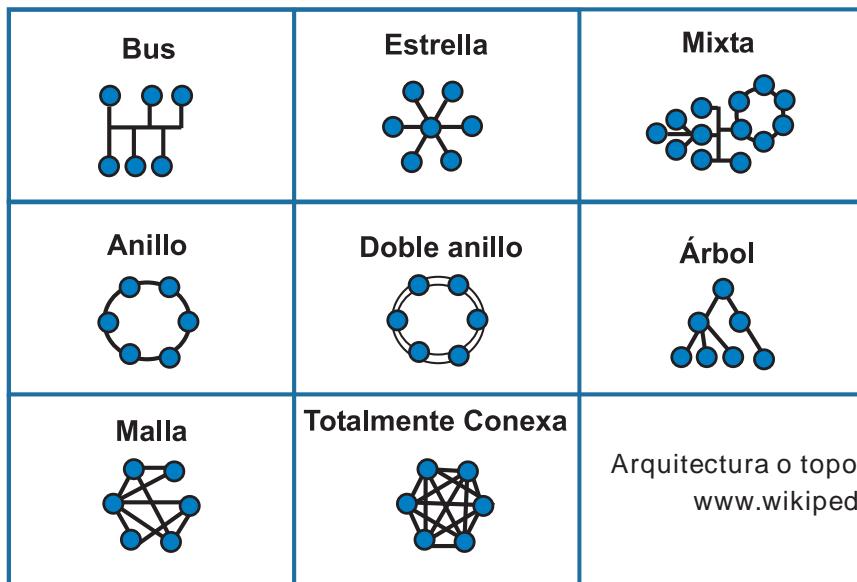
#### 4.3. Las redes de computadoras

La necesidad de distribuir la información u optimizar el uso de los dispositivos periféricos como impresoras, escáner, etc. hizo necesario que las computadoras pudieran conectarse entre ellas, dando origen a las denominadas redes de computadoras o redes informáticas. Una red es un conjunto de computadoras interconectadas o con una computadora principal denominada servidor (server) con el objeto de compartir recursos; las computadoras conectadas a un servidor se denominan terminales. Se define además, como el “conjunto de nodos y enlaces que proporciona conexiones entre dos o más puntos definidos para facilitar la telecomunicación entre ellos.” ([www.uit.org](http://www.uit.org); 2000)

Regularmente, se clasifican las redes acorde al espacio físico en donde se ubican, y se distinguen dos clases de redes LAN (Local Area Network) o redes de área local y WAN (Wide Area Network) o redes de área amplia. También puede clasificarse por la forma de conectar los dispositivos de comunicación en tradicionales o convencionales (guiadas) las cuales utilizan cables (red alámbrica) y las redes inalámbricas (no guiadas)<sup>7</sup>. Otra clasificación es por la topología utilizada como las redes en bus, estrella, anillo, malla o árbol.

<sup>7</sup> Las tecnologías más aplicadas actualmente son:

WI-FI: -Wireless Fidelity- Estándar para redes inalámbricas; y,  
Bluetooth: Estándar global de comunicaciones inalámbricas.



#### 4.4. Dispositivos de almacenamiento de los datos o información

Es común ver que los usuarios se preocupen por adquirir un ordenador de gran velocidad y amplia memoria, complementando con programas de ordenador de última edición, pero se olvidan que el elemento principal en un computador es la data que se almacena, por lo cual los dispositivos de almacenamientos cobran gran relevancia en cuanto a capacidad, durabilidad, velocidad de acceso, pero en especial, en cuanto a la seguridad de acceso y a las copias de seguridad. Existe una gran variedad que comprende, entre otros, los dispositivos fijos (como los discos duros) y los portátiles (disquete o CD); existen según la tecnología utilizada (dispositivos digitales o electromagnéticos); existen dispositivos que se adquieren por la capacidad de almacenamiento (tamaño para almacenar archivos), así como por su fiabilidad de almacenamiento (permanentes o

regrabables). Es importante en el ámbito legal describirlos en forma correcta, en especial para aspectos de inventario, y seguridad hasta cuando se ofrecen como medios de prueba en un proceso.

#### 4.5. El sistema informático del IDPP

Los sistemas de información se diseñan para cada usuario, empresa o ente público en el que se utilizará con base en el análisis del sistema realizado. En la mayoría de casos, se encuentra en constante desarrollo integrando nuevos programas, creando nuevas aplicaciones, o en su caso, mejorando las existentes.

## 5. Introducción a las Tecnologías de la Información y Comunicaciones –TIC–

En el ámbito legal, como en cualquier otra actividad, se aprovecharon las ventajas que proporciona el uso de las computadoras y las técnicas que proporciona la Informática, pero cuando las computadoras logran conectarse con otras, transmitir la data, comunicar la información y acceder a miles de servidores, se crea una gama de nuevos servicios y aplicaciones en constante desarrollo, lo cual se debe a las Tecnologías de la Información y Comunicaciones. Las denominadas TIC son el resultado de la convergencia de dispositivos, herramientas electrónicas y programas informáticos encargados de procesar información y su correspondiente transmisión; por ello podemos definir las TIC como el conjunto de conocimientos y elementos tecnológicos en materia de informática y telecomunicaciones que se utilizan simultáneamente para el procesamiento de toda clase de datos y su correspondiente transmisión por medio de redes de cable o inalámbricas, fax, televisión, radio, satélites, etc. El concepto de TIC “abarca todo aquello que implique la creación, procesamiento y transmisión de señales digitales y está conformada por hardware, software, cibernética, sistemas de información, redes, chips inteligentes, criptografía, robótica, inteligencia artificial y realidad virtual.” (Morton, 2001)

Con relación a las TIC encontraremos muchos términos relacionados como telecomunicaciones, ciberespacio, digitalización e Internet, los definiremos y explicaremos; conceptos como señales, satélite, mensaje de datos, electrónico, entre

otros, nos limitaremos a indicar la definición legal que otorga nuestra legislación.

### 5.1. Las telecomunicaciones

En la historia, el ser humano se encuentra en la búsqueda constante de comunicarse con otras personas, en especial, superando las distancias existentes por aspectos territoriales, por lo cual surge un conjunto de procedimientos que tienen por objeto transmitir un mensaje desde un punto de origen hasta un punto de destino (unidireccional), sumándole que este último pueda a su vez emitir su propia comunicación al punto origen (bidireccional) o en su caso a múltiples destinos receptores (multidireccional); a esta técnica se les identifica con el concepto telecomunicación. El significado proviene del griego *tele* que significa distancia y del latín *communicare* que significa comunicación, convergiendo en el significado de comunicación a distancia.

El concepto telecomunicación “cubre todas las formas de comunicación a distancia, incluyendo radio, telegrafía, televisión, telefonía, transmisión de datos e interconexión de ordenadores a nivel de enlace. Telecomunicaciones, es toda transmisión, emisión o recepción de signos, señales, datos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de cables, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos.” ([www.wikipedia.org](http://www.wikipedia.org); 2009).

La entidad nacional encargada de las telecomunicaciones es la Superintendencia de Telecomunicaciones –SIT- la cual se define como un organismo eminentemente técnico del Ministerio de Comunicaciones, Transporte y Obras Públicas, con independencia funcional para el ejercicio de las atribuciones y funciones que la ley establece siendo ellas: administrar y supervisar la explotación del espectro radioeléctrico, administrar el Registro de Telecomunicaciones, dirimir controversias entre los operadores, elaborar y administrar el Plan Nacional de Numeración, entre otras competencias. (Artículo 5 y 7 de la Ley General de Telecomunicaciones<sup>8</sup>, Decreto Número 94-96 del Congreso de la República).

A nivel internacional, la Unión Internacional de Telecomunicaciones -UIT- es el organismo especializado de las Naciones Unidas en el campo de la regulación y administración de las telecomunicaciones.

## 5.2. El ciberespacio

El diccionario de la Real Academia Española define al Ciberespacio como el “Ámbito artificial creado por medios informáticos.” (2009). Este concepto es muy

utilizado en el ambiente de las TIC y tiene por objeto describir los elementos intangibles de comunicación, es decir describe ese espacio de interacción que no es perceptible en forma física, sino a través de dispositivos electrónicos; nos referimos a las señales electrónicas, transmisiones satelitales y comunicaciones inalámbricas.

Un ejemplo de esta idea surge cuando usted envía un correo electrónico de Guatemala a España; este documento electrónico o mensaje de datos se transmite o “viaja” por el Ciberespacio.

## 5.3. La digitalización

En el párrafo anterior, utilizamos el ejemplo de un documento o fotografía impresa que antes enviábamos plasmado en formato de papel y ahora lo almacenamos y reproducimos en un archivo electrónico, es decir, en forma digital; al proceso por medio del cual se convierte un objeto, documento o imagen en un archivo digital se le denomina digitalización o como acostumbra indicar “se transforma del mundo de los átomos al mundo de los bytes.”

---

<sup>8</sup> **Artículo 1. Ámbito de aplicación.** El objeto de esta ley es establecer un marco legal para desarrollar actividades de telecomunicaciones y normar el aprovechamiento y la explotación del espectro radioeléctrico, con la finalidad de apoyar y promover el desarrollo eficiente de las telecomunicaciones, estimular las inversiones en el sector, fomentar la competencia entre los diferentes prestadores de servicios de telecomunicaciones; proteger los derechos de los usuarios y de las empresas proveedoras de servicios de telecomunicaciones, y apoyar el uso racional y eficiente del espectro radioeléctrico. (Ley General de Telecomunicaciones)

<sup>9</sup> “Además, se trata de una expresión que etimológicamente deriva de la cibernetica, esto es, el estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; en particular, de las aplicaciones de los mecanismos de regulación biológica a la tecnología.” (Herrera, 2007)

<sup>10</sup> Digitalización es diferente a digitar o digitación porque este último consiste en introducir a la computadora la información o contenido desde el teclado.

Algunos conceptos relevantes con este tema los define la Ley de Derechos de Autor y Derechos Conexos, en el artículo 4:

**Cable distribución:** la operación por la cual las señales portadoras de signos, sonidos, imágenes o imágenes y sonidos, producidos electrónicamente, o por otra forma, son transmitidos a distancia por hilo, cable, fibra óptica, u otro dispositivo conductor, conocido o por conocerse, a los fines de su recepción por el público.

**Medida tecnológica efectiva:** tecnología, dispositivo o componente que en el giro normal de su funcionamiento, controla el acceso a obras protegidas, interpretaciones o ejecuciones y fonogramas protegidos, o cualquier otro material protegido, o proteja un derecho de autor o un derecho relacionado con el derecho de autor.

**Satélite:** todo dispositivo situado en el espacio extraterrestre, apto para recibir y transmitir o retransmitir señales.

**Señales:** todo vector producido electrónicamente y apto para transportar programas.

**Transmisión:** la comunicación a distancia por medio de la radiodifusión, cable distribución u

otro procedimiento análogo o digital, conocido o por conocerse, de imágenes, sonidos imágenes con sonido, datos o cualquier otro contenido.

Otros conceptos se encuentran definidos en la Ley y el Reglamento para el Reconocimiento de las Comunicaciones y Firmas Electrónicas:

**Artículo 2. Definiciones.** Para los efectos de la presente ley, se entenderá por:

**Comunicación Electrónica:** toda comunicación que las partes hagan por medio de mensajes de datos.

**Intercambio Electrónico de Datos (IED):** la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida.

**Mensaje de Datos:** el documento o información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (IED), el correo electrónico el telegrama, el télex o el telefax.

**Documento Electrónico:** toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

**Electrónico:** característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, **i n a l á m b r i c a s , ó p t i c a s ,** electromagnéticas u otras similares.<sup>11</sup>

Desarrollamos conceptos en los puntos iniciales como informática, computadora u ordenador, información y datos; en el presente punto tratamos conceptos básicos como telecomunicaciones, digitalización, ciberespacio y cerramos con las definiciones legales de conceptos como señales, intercambio de datos, documentos electrónicos, porque si sumamos a todos ellos las relaciones sociales y comerciales que surgen de la integración de todos, sumamos miles de usos y aplicaciones, que integramos en un espacio que se identifica con el concepto de Internet.

## 6. Aspectos básicos sobre la Internet

Pero realmente ¿Qué es la Internet? La respuesta la tiene cada usuario según el uso o aplicaciones que utilice en su vida diaria o trabajo al utilizar la supercarretera de información. Desde un punto de vista general, la Internet es el conjunto de computadoras, redes y dispositivos de telecomunicaciones, conectados por medio de enlaces, que permiten la comunicación, el intercambio de información y servicios,

a través de un protocolo común en un espacio geográfico nacional o internacional.<sup>12</sup>

El término Internet fue identificado en un origen como la contracción de Internetwork System, es decir, un Sistema de Intercomunicación de Redes. Otra forma técnica de describirlo es como una contracción de International Net que describe a la Red Internacional de Computadoras. La vigésima tercera edición del Diccionario de la Real Academia Española incorpora el término Internet y lo define como la “Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación.” (RAE, 2005)

Estamos tan acostumbrados a dar un click para transmitir información por medio de Internet que no podemos imaginarnos qué es lo que pasa en ese proceso; para explicar la estructura y describir cómo funciona la Internet con la data que usted envía o accede, vea el video que encontrará en <http://www.warriorsofthe.net/movie.html>

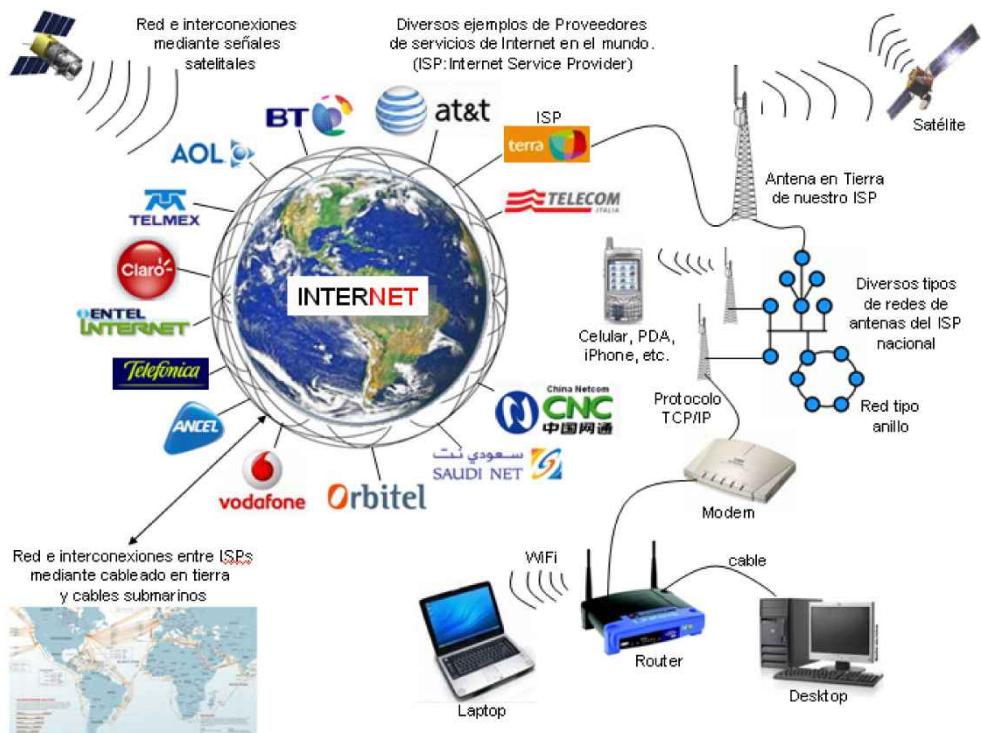
---

<sup>11</sup> La Ley de Garantías Mobiliarias (Decreto No. 51-2007 del Congreso de la República) en el artículo 2 inciso r define: **Electrónico:** se refiere a toda forma de generación, envío, comunicación, procesamiento, recepción, almacenamiento o visualización de datos o información, por medio de tecnologías eléctricas, digitales, magnéticas, ópticas, electromagnéticas, fotónicas. Vía facsímil y cualquier otra tecnología semejante.

<sup>12</sup> “**Internet:** Red mundial de computadoras u ordenadores interconectados mediante un protocolo especial de comunicación. Funciona a modo de nombre propio, por lo que, en el uso mayoritario de todo el ámbito hispánico, se escribe con mayúscula inicial y sin artículo... Si se usa precedido de artículo u otro determinante, es preferible usar las formas femeninas (la, una, etc.), por ser femenino el nombre genérico red, equivalente español del inglés net.” (Diccionario Panhispánico de Dudas, 2005).

### Esquema general de Internet

<http://pringaonomore.files.wordpress.com/2009/02/internet2.jpg>



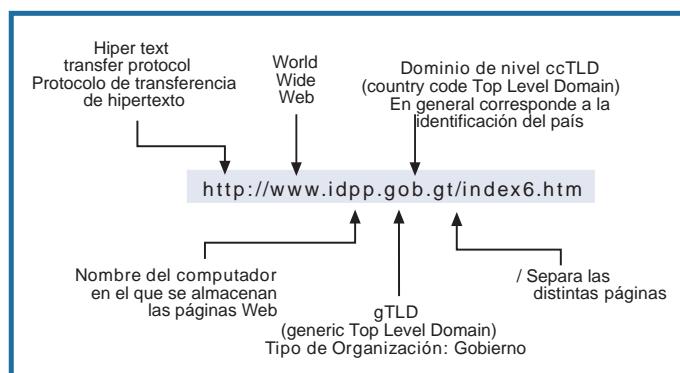
### 7. Aplicaciones y relación de la Internet en el Derecho

Cada día es más complicado describir los usos y aplicaciones que pueden darse utilizando las líneas de comunicación que permite la Internet en virtud de su crecimiento y constante desarrollo. En el ámbito profesional se pueden agrupar en dos, siendo las utilizadas para comunicación y las de acceso a la información. En el primer grupo, encontramos el correo electrónico, el Chat o aplicaciones de charlas en línea, la mensajería instantánea, las listas de interés, el Telnet, la FTP, VoIP, las videoconferencias, los grupos de discusión; en el segundo grupo lideran, la World Wide Web (www) o navegación en

páginas, acceso a sitios web de aplicaciones o servicios, como la banca electrónica, servicios de comercio electrónico e inclusive pueden considerarse las redes sociales. Por la importancia de su uso en el ámbito legal, nos limitaremos a describir las más utilizadas.

La World Wide Web (www) o red mundial de sitios es una de las aplicaciones más utilizadas de la Internet; consiste en un sistema de información en línea, basado en los enlaces de “hipertexto” (las páginas o sitios web, se encuentran entrelazadas entre sí o con otras por medio de palabras

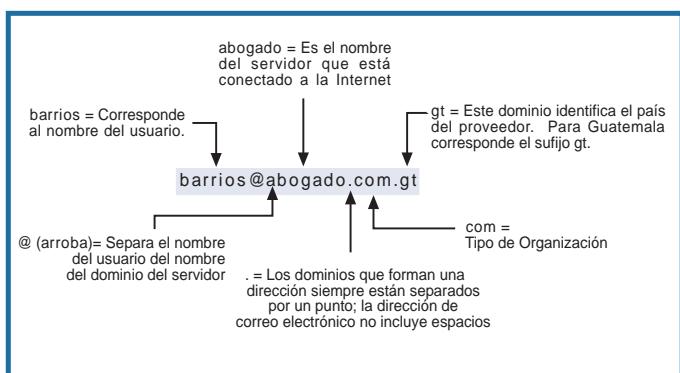
o imágenes que permiten acceder a otros documentos), integran una gama de información de diversa categoría y contienen desde un simple texto hasta imágenes, video, sonidos, etc. Para poder efectuar la comunicación o conexión con un sitio web es necesario ubicar su dirección para lo cual debe contarse con la URL (Uniform Resource Locator) o Localizador Uniforme de Recursos; cada página web queda identificada por una única dirección para su ubicación. La dirección para localizar una página específica se estructura generalmente de la forma siguiente:



El correo electrónico o e-mail es un sistema de mensajería electrónica personal, en donde el envío y despacho se realiza desde un computador a otro en cuestión de segundos, sin importar las distancias y se pueden adjuntar (attachment) archivos de texto, imágenes, sonido, videos, entre otros.<sup>13</sup> Como complemento de servicios por medio de correo-e encontramos las listas de Interés o de correo que consiste

en un sistema que distribuye mensajes electrónicos a un grupo de personas que comparten intereses comunes, que desean intercambiar información o ideas y que pueden ser de un mismo ámbito profesional, o en su caso, no necesitan conocerse; los usuarios se han suscrito en una lista del tema o área de su interés donde realizarán sus comentarios e intercambiarán y discutirán sus puntos de vista sobre algún tema común.

Una dirección de correo o buzón electrónico se integra de la forma siguiente:



Es importante que todos los datos de la dirección electrónica los escriba con minúscula; además no hay que dejar espacios.

Entre otras aplicaciones populares utilizadas, encontramos el servicio de función de charla o chat como se le conoce comúnmente, que permite comunicarse con un grupo de personas a escala nacional o internacional

<sup>13</sup> Un ejemplo de la importancia del correo electrónico en el ámbito legal lo encontramos en el Código Tributario:

“Artículo 98 “A”. Otras atribuciones de la Administración Tributaria. La Administración Tributaria también podrá:

1. Establecer de mutuo acuerdo con el contribuyente, una dirección electrónica en Internet, o buzón electrónico, para cada uno de los contribuyentes y responsables, a efecto de remitirles los acuses de recibo de las declaraciones y pagos efectuados, boletines informativos, citaciones, notificaciones y otras comunicaciones de su interés, cuando correspondan.
2. Establecer procedimientos para la elaboración, transmisión y conservación de facturas, libros, registros y documentos por medios electrónicos, cuya impresión pueda hacer prueba en juicio y los que sean distintos al papel.

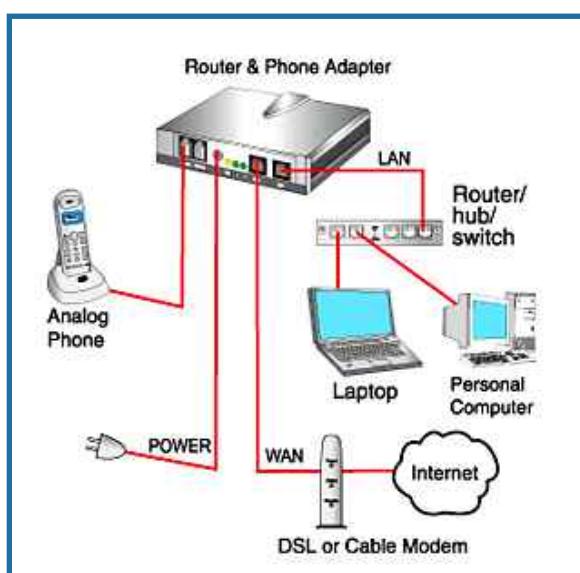
en tiempo real, a través de computadoras interconectadas, mediante el envío de textos, lo cual crea un diálogo para todos los participantes o bien con uno de ellos y esta acción se conoce como chatear. El chat puede ser complementado con imágenes e inclusive video. Actualmente, se utiliza el término mensajería instantánea para describir una forma avanzada del chat y con mejores posibilidades de comunicación en tiempo y recursos.

Entre las aplicaciones utilizadas en Internet encontramos dos que podemos identificar como “comunicaciones personalizadas” por ser una forma de transmitir mensajes entre personas más directos al permitir utilizar la voz y el video, siendo las más comunes VoIP y la videoconferencia. La comunicación oral o por voz utilizando la plataforma de Internet se identifica como VoIP que significa “Voz sobre Protocolo de Internet” (VozIP). “Esto significa que se envía la señal de voz en

forma digital, en paquetes, en lugar de enviarla en forma digital o analógica, a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional o PSTN (sigla de Public Switched Telephone Network, -Red Telefónica Pública Comutada-).”<sup>14</sup> ([www.wikipedia.org](http://www.wikipedia.org); 2009)

La videoconferencia es otro de los servicios que se ha incorporado a la Internet y que consiste en un sistema que permite mantener comunicaciones en tiempo real entre dos o más personas que se encuentran en lugares geográficamente distintos, en la que se establece relación de sonido e imagen en uno o en ambos sentidos de los enlaces e inclusive con múltiples conexiones. En materia penal, encontramos el uso de esta aplicación en el Código Procesal Penal (Decreto Número 51-92 del Congreso de la República) en virtud que fue reformado por el Decreto Número 17-2009 del Congreso de la República de Guatemala (Ley del Fortalecimiento de la Persecución Penal) y se encuentra vigente desde el 16 de mayo de 2009. Los artículos adicionados establecen lo siguiente:

**Artículo 218 Bis. Declaración por medios audiovisuales de comunicación.** Si por circunstancias debidamente fundadas, el testigo, perito o colaborador eficaz no puede concurrir a prestar declaración en forma personal, el tribunal, a pedido de parte o de oficio, podrá ordenar la realización de la declaración testimonial a través de videoconferencia o cualquier otro



Soluciones típicas basadas en VoIP  
[www.wikipedia.org](http://www.wikipedia.org)

<sup>14</sup> Diferente es la denominada Telefonía sobre IP que consiste en el servicio de telefonía que utiliza la tecnología de voz sobre IP, pero sujeto al sistema y normativas de numeración.

medio audiovisual de comunicación similar de la tecnología, de las mismas o mejores características, que resguarden la fidelidad e integralidad de la declaración y garanticen a las partes el adecuado ejercicio de sus derechos procesales...

Artículo 218 TER. Procedimiento en caso de declaración por medio audiovisual. La declaración a través de videoconferencia u otros medios audiovisuales de comunicación, podrá realizarse durante el debate oral y público o en carácter de anticipo de prueba. La diligencia se realizará con base en lo siguiente:

- a) En caso se efectúe la diligencia en anticipo de prueba, el órgano jurisdiccional deberá informar a las partes, con no menos de diez días de anticipación, de la realización de la diligencia, sin perjuicio de lo dispuesto en este Código en dicha materia en relación al peligro de pérdida de elementos de prueba y de actos de extrema urgencia. Durante el debate oral deberá programarse la diligencia al inicio del mismo. En el anticipo de prueba se observarán los artículos 317, 318 y 348 de este Código, recibiendo la declaración testimonial mediante videoconferencia u otro medio electrónico cuando proceda;
- b) El órgano jurisdiccional competente efectuará el trámite respectivo ante las autoridades del país o lugar donde resida la persona; en caso se trate de un testigo protegido o colaborador eficaz, deberá mantener bajo reserva de confidencialidad el

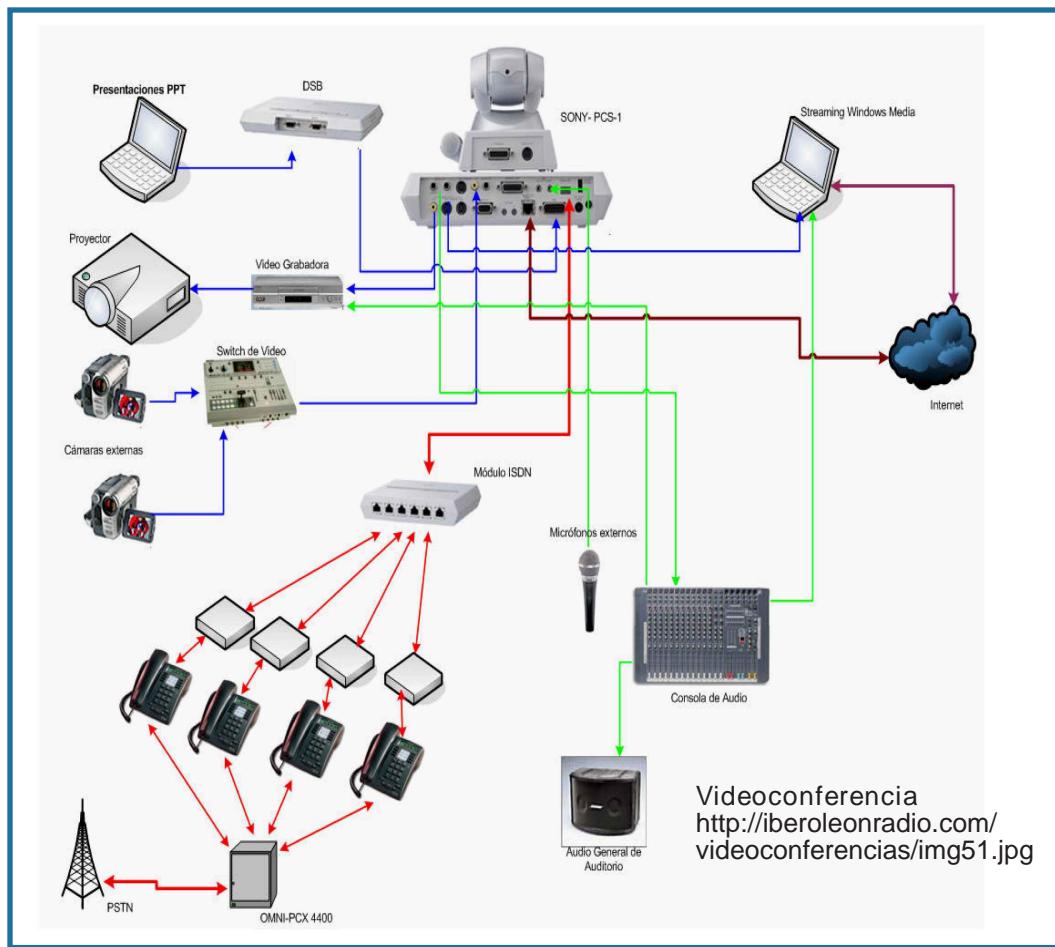
- c) trámite y el lugar donde se encuentra el mismo;
- d) En el lugar donde se encuentre el testigo, perito u otra persona cuya declaración sea relevante en el proceso, debe estar presente una autoridad designada por el órgano jurisdiccional competente, la cual tiene la obligación de verificar la presencia del testigo, perito u otra persona; tomar sus datos de identificación personal, verificar que la persona no está siendo coaccionada al momento de prestar declaración, verificar que las instalaciones reúnan las condiciones adecuadas y que se cuente con los aparatos audiovisuales idóneos y conectados con enlace directo con el tribunal. El órgano jurisdiccional competente a cargo de la diligencia, dejará constancia de haberse cumplido la obligación precedente;
- e) El órgano jurisdiccional competente deberá verificar que las instalaciones y medios audiovisuales permitan que las diferentes partes procesales puedan oír y observar con fidelidad la declaración prestada por un testigo, así como ejercer sus derechos en materia de interrogatorio;
- f) En caso que el testigo goce del beneficio del cambio de identidad o se determine que por razones de seguridad se deba ocultar su rostro, se tomarán todas las precauciones necesarias para evitar que el mismo pueda observarse a través del medio audiovisual que se utilice.

Toda la diligencia deberá ser grabada y debidamente registrada. Una vez concluida la diligencia, el personal autorizado por el órgano jurisdiccional competente que se encuentre en el lugar donde estuviere la persona que tuviera que declarar, accionará acta de la diligencia, misma que deberá ser firmada por todos los presentes y remitida al órgano jurisdiccional que emitió la orden respectiva. Las partes tendrán acceso a los documentos, grabaciones y registros producto de dicha diligencia.

En estas diligencias siempre deberá comparecer el defensor designado por el imputado, en su defecto el defensor público que se designe por el juez, y el fiscal del caso, cuidándose porque se observen debidamente las garantías constitucionales

del derecho de defensa y el debido proceso. En caso de no existir imputado, igualmente se hará comparecer a un defensor público de oficio, para garantizar la legalidad de la declaración testimonial en esta forma; asimismo comparecerán en ese acto probatorio anticipado, el fiscal del caso, el querellante adhesivo si lo hubiere, y dicho acto será presidido personalmente por el juez del proceso.

En la siguiente gráfica, puede observar uno de los múltiples modelos a utilizar en esta aplicación, pero es importante considerar los niveles de seguridad de la plataforma para garantizar la calidad de la comunicación como su integridad.



Otras aplicaciones que hay que considerar por los aspectos legales, protección de datos e inclusive para el procedimiento de investigación en materia penal, son los blog, diarios o agendas personales en línea, así como las redes sociales (Facebook, Hi5, Twitter, MySpace).

## 8. Los nombres de dominio (ND)

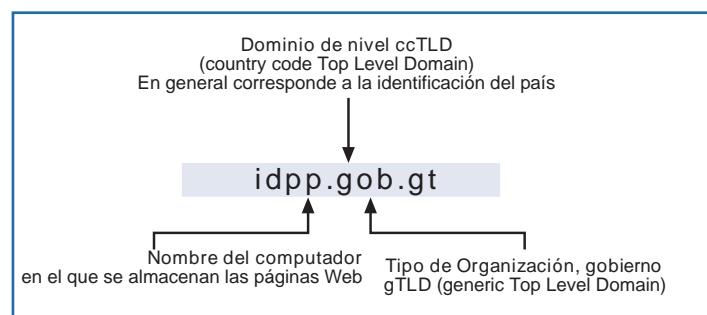
Cuando el usuario “navega” en la Internet o quiere ingresar a un sitio web y realizar el proceso de una forma amigable existen los nombres de dominio (domain name en inglés) el cual se define como “Una dirección asignada a una conexión de red y que identifica al propietario de dicha dirección de una forma jerárquica: servidor.organización.tipo.” (Diccionario de Internet y Redes, 2005). El nombre de dominio es el conjunto de caracteres clasificados por niveles que identifican la dirección o ubicación utilizada en la Internet por una computadora o servidor para su conexión o ubicación.

### 8.1. Estructura de un nombre de dominio

Establecemos en la definición de nombre de dominio que se componen de niveles, siendo los siguientes:

www world wide web  
 SLD Second Level Domain  
 gTLD generic Top Level Domain  
 ccTLD country code Top Level Domain

Cada nivel debe de ir separado con un punto (.). La estructura básica de un nombre de dominio es la siguiente:



El SLD (Second Level Domain) es el segundo nivel de dominio. Representa el nombre del servidor o computadora conectada; se utiliza regularmente el nombre de la empresa o persona, marca, siglas o iniciales, producto distintivo o cualquier otro término de fácil ubicación para el usuario. El gTLD (generic Top Level Domain) es considerado el nivel de primera clase o primer nivel de dominio (junto con ccTLD) y describe de forma genérica (generic) la actividad o sector del servidor o equipo de cómputo conectado a la Internet. Los primeros gTLD creados fueron:

gTLD	Tipo de Organización
com	Empresas comerciales
net	Proveedores de Servicio de Internet o para cualquier tipo de redes
org	Instituciones u organizaciones sin fines de lucro o asociaciones
gov (gov)	Entes de gobierno (government) <sup>15</sup>
Int	Entes u organismos internacionales
mil	Exclusivo para entes militares

<sup>15</sup> Algunos dominios se identifican con gov por el término en inglés Government (gobierno).

En el año 2000, el ICANN introdujo siete nuevos nombres de dominio genéricos de primer nivel, siendo ellos:

gTLD	Tipo de Organización
name	Empresas comerciales
info	Proveedores de Servicio de Internet o para cualquier tipo de redes
pro	Instituciones u organizaciones sin fines de lucro o asociaciones
biz	Entes de gobierno (government) <sup>15</sup>
museum	Entes u organismos internacionales
aero	Para aerolíneas
coop	Cooperativas comerciales

El ccTLD (country code Top Level Domain) es el nivel de primera clase o primer nivel de dominio (junto con gTLD) y describe el código del país (country code), es decir, el Estado donde se encuentra registrado el dominio y que se identifica con dos letras; en el caso de Guatemala, corresponde las letras o siglas gt.

## 8.2. La administración y el registro de un nombre de dominio

La entidad internacional conocida por sus siglas en inglés como ICANN - Internet Corporation for Assigned Names and Numbers Corporación- es el organismo o corporación que se encarga de ejecutar

las tareas fundamentales en el funcionamiento y administración de la Internet; sustituyó en sus funcionales a la IANA -InterNet Assigned Numbers Authority- quien fue el ente que al inicio se encargó de la administración de los nombres de dominio. En cada Estado, al principio la IANA y después el ICANN han facultado a un ente para que administre el ccTLD de su territorio. En Guatemala ejerce esa competencia la Universidad del Valle de Guatemala ([www.gt](http://www.gt)).

El procedimiento para registrar un nombre de dominio para su uso o reserva, conlleva cumplir con un proceso de asignación, el cual puede realizarse desde Internet y en algunos casos, ciertos requisitos de forma presencial ante el Registrador Autorizado.

The screenshot shows the homepage of register.com. At the top, it says "register.com" and "grow your business online. handholding included." Below that is a navigation bar with links for HOME, DOMAINS, EMAIL, WEB SITES, HOSTING, SOLUTIONS, MARKETING, and YOUR BUSINESS. A "Register" button is highlighted. To the right, there's a call to action: "Experience the difference great service can make Call us toll free at 1-888-Register (1-888-734-4783)". Below the navigation, there's a search bar with "Advanced Domain Search" and dropdown menus for "Web Site Transfer", "Domain Renew", and "Email Packages". To the right, there are three boxes: "I have never built a Web Site - BEGINNER -", "I have some basic knowledge - INTERMEDIATE -", and "I'm familiar with building Web sites - ADVANCED -". Further down, there's a section for "Email Packages" and "Web Sites". On the right side, there's a large box for "FREE Web site with every domain name!" featuring a "Go!" button and a "FREE 1-PAGE WEB SITE" offer. At the bottom, there are three more sections: "Multi-User Email", "Web Site Building Made Easy!", and "Web Hosting just got bigger and BETTER!!".

Es importante anotar que el nombre de dominio no se compra, es decir no se encuentra en propiedad, se adquiere el derecho a su asignación (uso) y

administración. Esto hay que tenerlo presente, porque regularmente se otorga el uso por uno o dos años (lo que el titular solicite y pague), complementado con las normas del administrador con el que se registra.

Para adquirir un nombre de dominio se acude, según sea el caso o interés, o puede realizarse con un administrador internacional, o un administrador nacional o local (los que cuentan con ccTLD). Si el nombre de dominio que desea adquirir no usa el dominio de nivel ccTLD<sup>16</sup>, el procedimiento lo puede efectuar vía Internet con distintos administradores. Primero debe verificar que el dominio no esté otorgado a otra persona; el pago se realiza comúnmente en línea con tarjeta de crédito llenando formularios electrónicos con datos generales y técnicos (por ejemplo [www.register.com](http://www.register.com), [www.netronica.net](http://www.netronica.net)).

Si el nombre de dominio que desea adquirir utiliza el dominio de nivel ccTLD<sup>17</sup> (cuando lleva las siglas de los Estados: .ar .es .gt), deberá verificar con el administrador local.

El procedimiento para determinar quién es el administrador es colocar en la barra del navegador las siglas www el signo de punto (.) y las siglas del Estado. El procedimiento para registrar el dominio es similar al explicado para el administrador internacional, pero en algunos casos el administrador local solicita otros requisitos.

### 8.3. Conflictos derivados por el registro o uso de nombres de dominio

Los entes encargados de registrar los nombres de dominio no cuentan con un acuerdo general que permita establecer o realizar un examen previo del interesado en registrar un término como un nombre de dominio. Para otorgar el registro han aplicando el principio que “primero en registro primero en derecho”. Con el crecimiento de Internet y sus aplicaciones, las personas individuales y jurídicas han empezado a utilizar esta vía para dar a conocer su misión, objetivos, servicios, etc. Por ello necesitan que los usuarios los ubiquen en la Internet, siendo el nombre de su empresa, sociedad, marca, productos, la vía para que puedan ser ubicados en la red de redes. El problema surge cuando las personas quieren registrar su nombre de dominio, siendo el .com el más solicitado, y otra persona cuenta con ese registro. Esto ha hecho que surja una gran cantidad de conflictos para determinar quién es el titular del derecho sobre el nombre de dominio. Es importante recordar que los dominios no se equiparan al sistema de marcas (propiedad intelectual) en forma expresa. Un ejemplo podría ser el término “gallo”; el dominio gallo.com.gt podría tener varias personas interesadas en registrarlo, en virtud que en Guatemala identifica a una marca de jabón, a una marca de fósforos y la marca de una cerveza. Si a ello agregamos que queremos adquirir el nombre sin el uso del ccTLD, dominio internacional (gallo.com), los interesados o titulares están a nivel mundial.

---

<sup>16</sup> Conocidos de forma común como: Nombres de dominio internacionales.

<sup>17</sup> Denominados: Nombres de dominio nacionales

Para solucionar las controversias que surgen entre quien tiene registrado el nombre de dominio y quien considera tiene el derecho o un mejor derecho a su uso, existen varias vías para resolverlo: La resolución directa o vía voluntaria, la resolución mediante mecanismos alternativos y la resolución en la vía jurisdiccional (ordinaria).

La vía de resolución de conflictos directa o vía voluntaria se utiliza en especial en los casos de “Ciberocupación” (Cybersquatters), inclusive es la primera opción que tienen los sujetos. Se constituye como un arreglo directo entre la persona que ostenta el registro del nombre de dominio, que en la mayoría de los casos no lo está utilizando, y la persona interesada o con mejor derecho a su uso. La resolución mediante mecanismos alternativos es la utilizada para resolver las controversias derivadas de la administración, registro y utilización de los nombres de dominio cuando no se ha utilizado el arreglo en forma directa, o se agotó sin solución, o la persona que lo tiene registrado si lo utiliza con relación a un servicio o dato que presta. En este caso, el ICANN (Internet Corporation for Assigned Names and Numbers) - Corporación Internet para Nombres y Números Asignados- ha proporcionado la Política Uniforme de Solución de Controversias en materia de Nombres de Dominio (Uniform Disputes Resolution Policy –UDRP-), para resolver los conflictos, aprovechando la tecnología de la Internet, y constituyéndose en un procedimiento en

línea para resolver quién tiene el derecho sobre el nombre de dominio.<sup>18</sup> En el caso de la vía jurisdiccional (ordinaria) para resolver conflictos, dependerá de las reglas establecidas por el Centro de Registro Autorizado para cada Estado, en virtud que se discuten los dominios ccTLD (nacionales), pero se duda de la competencia de los tribunales de justicia en esta materia.

---

<sup>18</sup> **OBJETO DE LA UDRP:** 1. **Objetivo.** La presente Política uniforme de solución de controversias en materia de nombres de dominio (la "Política") ha sido aprobada por la Corporación de Asignación de Nombres y Números de Internet ("ICANN"), se incorpora mediante referencia en su acuerdo de registro y establece las cláusulas y condiciones en relación con una controversia que surja entre usted y cualquier otra parte distinta a la nuestra (el registrador) sobre el registro y utilización de un nombre de dominio de Internet registrado por usted. El procedimiento establecido en virtud del párrafo 4 de la presente Política se llevará a cabo de conformidad con el Reglamento de la Política uniforme de solución de controversias en materia de nombres de dominio (el "Reglamento"), disponible en [www.icann.org/udrp-rules-24oct99.htm](http://www.icann.org/udrp-rules-24oct99.htm), y el Reglamento Adicional del proveedor del servicio de solución de controversias administrativas seleccionado.





## EJERCICIOS DE AUTOAPRENDIZAJE

1. Contar con el conocimiento técnico del funcionamiento básico de Internet es necesario.

Vea el video Warriors of the net y redacte sus aspectos más relevantes.  
Puede acceder a él en:

<http://www.warriorsofthe.net/movie.html>  
(Elam, G; Stephanson, T; Hanberger, N. All Rights Reserved. Copyright 2002.)

2. Despues de ver el video e investigar en Internet, trace un esquema de los puntos por los cuales debe trasladarse un correo electrónico que envía a otro usuario, tanto en una red interna o privada como por medio de Internet.
3. Se presenta el siguiente caso y se le solicita su opinión legal-técnica sobre los aspectos indicados.

### i) Planteamiento del caso:

El sujeto está sindicado de falsificar y alterar facturas con el fin de cometer defraudación tributaria; el ente investigador realiza un allanamiento en el lugar del trabajo del sindicado y secuestra el equipo informático ubicado en su oficina, consistente en la computadora de escritorio, un escáner y una impresora láser, con los cuales se presume que han estado alterando, editando, elaborando e imprimiendo los documentos. En una carpeta del directorio del disco duro, se encuentran las imágenes de los documentos alterados y en un flash disk se encuentran dos archivos encriptados donde se presume que se encuentran imágenes de otros documentos; la lista de archivos contiene información relevante como la fecha y hora de almacenamiento de cada archivo informático; también se puede acceder a la lista de programas de ordenador de edición de documentos; pero esa computadora no se encuentra aislada, es parte integral de un sistema de información contable y se encuentra interconectada con otras computadoras por medio de una red interna y en su servidor se encuentran almacenados datos de otros clientes, así como las constancias electrónicas por efectuar los pagos tributarios vía Internet utilizando el sitio web de la Superintendencia de Administración Tributaria ([www.sat.gob.gt](http://www.sat.gob.gt))

4. Obtenga un acta de secuestro de equipo informático y verifique si se cumplió con todo el procedimiento legal y describa qué aspectos técnicos son relevantes para documentar.
5. Investigue a nombre de quien se encuentra registrado el nombre de dominio que indique el facilitador. Explique el procedimiento utilizado.

## CAPÍTULO

# 2

### INTRODUCCIÓN AL DERECHO INFORMÁTICO Y LA INFORMÁTICA JURÍDICA

El rechazo frontal a la utilización de la informática –las Tecnologías de la Información y Comunicaciones- y de los medios de “razonamiento” que ofrecen los desarrollos tecnológicos, lejos de descalificar a estos avances técnicos descalifica a los que los rechazan, que ellos mismos se discriminan en su actuación profesional. Afortunadamente, este rechazo ha sido superado en gran parte y se abre el camino –reclamado a gritos en todos los ámbitos jurídicos- de la regulación jurídica del fenómeno informático.

No se trata, dice el Profesor Hernández Gil, de que el Derecho va a ordenar nuevas realidades, sino que el Derecho mismo va a experimentar, en cuanto objeto de conocimiento, una mutación, derivada de un modo distinto de ser elaborado, tratado y conocido.

Tengamos en cuenta, sin embargo, que, en palabras de Kennet Laudon, “la Informática parece ser un elemento que facilita las tendencias sociales, políticas y culturales del momento, pero no las crea”.

Miguel Davara



## CONTENIDO DEL CAPÍTULO

La Informática, como la ciencia que estudia el procesamiento automatizado de la información, tiene aplicaciones en todas las áreas del saber humano y en todas las actividades que realizan las personas; el Derecho como ciencia social, y los juristas, no podían quedar alejados de las ventajas que genera el uso de los programas de ordenador, bases de datos, acceso a la información en general y medios de comunicación, pero con el surgimiento de las TIC también se crean nuevos derechos y obligaciones, se transforman los medios de comunicación y se generan nuevos conflictos en la sociedad, por lo cual el Derecho debe investigar y emitir los ordenamientos necesarios para el buen uso social de la tecnología.

Cuando se empiezan a utilizar las ventajas que proporcionan las aplicaciones de la Informática en el procesamiento de los volúmenes de información que produce el Derecho, se le ha denominado Informática Jurídica, y cuando se estudian los efectos que tienen los fenómenos derivados de las tecnologías y regularlos para la correcta convivencia social, se utiliza el concepto Derecho Informático; en virtud de lo anterior, quedan, delimitados ambos campos de estudio. Estos criterios doctrinarios tienen sus detractores, pero por el momento siguen siendo utilizados para delimitar la actividad de cada ámbito; lo que es innegable para todos es que las Tecnologías de la Información y de las Comunicaciones están innovando el conocimiento humano y la sociedad en general, por ello, el Derecho tiene un nuevo reto, el cual describe de manera idónea Cristian Calderón al indicar que el objeto es “flexibilizar sus instituciones e incorporar aquellas normas surgidas dentro del Internet para que todos los actos jurídicos que se den dentro del mundo virtual tengan idénticas consecuencias en el mundo físico, y que además, cualquier relación jurídica que se desplace entre ambos espacios tenga los mismos efectos legales.” (2000)





## Objetivos Específicos

- a) Diferenciar el campo de aplicación de la Informática Jurídica, el Derecho Informático y el Derecho de las Nuevas Tecnologías.
- b) Aplicar los conocimientos adquiridos en el ámbito de la Informática y aplicarlos posteriormente en el campo de estudio, investigación y ejercicio profesional.
- c) Conocer las aplicaciones existentes para desarrollar la actividad del defensor público.



Introducción de las nuevas tecnologías en el derecho  
Instituto de la Defensa Pública Penal

## 1. EL DERECHO INFORMÁTICO

El crecimiento de la Informática y sus aplicaciones, ha generado nuevos derechos y obligaciones que se inician desde su propia creación, se desarrollan con el uso, e inclusive, transforman los existentes. Por eso se define al Derecho Informático o Derecho de la Informática como “una materia inequívocamente jurídica, conformada por el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir de la informática y la telemática.” (Pérez, 2001)

El Profesor Julio Téllez define al Derecho de la Informática “como el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática”. (2004) El Derecho Informático es el conjunto de doctrinas, principios y normas, que regulan los bienes jurídicos que la Informática crea, las acciones y las responsabilidades de las personas derivadas del uso de la tecnología.

### 2. Contenido del Derecho Informático

El contenido del Derecho Informático es amplio y de constante desarrollo. La siguiente enumeración es una recopilación de Rodolfo Herrera Bravo, indicando sobre

su propuesta que no es un orden doctrinal, sino pedagógico. Los temas son:

1. “El valor probatorio de los soportes modernos de información, provocado por la dificultad en la aceptación y apreciación de elementos de prueba derivados de estos soportes entre los órganos jurisdiccionales.
2. La protección de datos personales, ante el manejo inapropiado de informaciones nominativas que atenta contra derechos fundamentales de las personas.
3. Los delitos informáticos, es decir, la comisión de verdaderos actos ilícitos en los que se tenga a los computadores como instrumentos o fines.
4. El flujo de datos transfronterizos, con el favorecimiento o restricción en la circulación de datos a través de las fronteras nacionales.
5. La protección de los programas computacionales, como respuesta a los problemas provocados por la piratería de software que atenta contra la propiedad intelectual.
6. Los contratos informáticos, en función de esta categoría contractual sui generis con evidentes repercusiones fundamentalmente económicas.
7. La regulación de los bienes informacionales, en función del innegable carácter económico de la información como producto informático.

8. La ergonomía informática, como aquellos problemas laborales suscitados por la informatización de actividades." (2000)

Por supuesto que la anterior enumeración no cubre ni describe en su totalidad el contenido del Derecho Informático denominado actualmente como el Derecho de las Tecnologías de la Información y de las Comunicaciones, porque el avance de la tecnología incorpora cada vez más temas o problemas por solucionar, pero los enumerados son los comunes actualmente.

En Guatemala, se cuenta con ordenamientos legales que regulan algunos aspectos o usos del fenómeno tecnológico que deben considerarse para el estudio de la temática, sin excluir otras normas ordinarias y reglamentarias que pueden consultarse en la bibliografía del presente módulo, inclusive los principios constitucionales que consideraron a la tecnologías; los decretos principales a estudiar son los siguientes:

- a) Ley de Comunicaciones y Firmas Electrónicas (Decreto Número 47-2008 del Congreso de la República): regula lo relacionado con las actividades electrónicas como el comercio electrónico, los documentos electrónicos o mensajes de datos, la contratación electrónica y las firmas electrónicas.
- b) Ley de Acceso a la Información Pública (Decreto Número 57-2008 del Congreso de la República): establece la importancia de la

protección de los datos personales y los delitos o infracciones que se pueden cometer en cuanto a violentar el derecho a la intimidad de las personas con relación a los datos personales.

- c) Código Penal ((Decreto Número 17-73 del Congreso de la República): se tipifican los delitos informáticos, adicionados por reformas al Código Penal por el Decreto Número 33-96; además otros delitos que se comenten por medio de tecnologías o utilizándolas como instrumentos del delito.
- d) Código Procesal Penal (Decreto Número 51-92 del Congreso de la República): con las últimas reformas se incorpora el uso de videoconferencias para lo cual se utiliza la plataforma Internet.
- e) Ley de Telecomunicaciones (Decreto Número 94-96 del Congreso de la República): Establece el marco legal de las telecomunicaciones, el uso del espectro radioeléctrico, los derechos de los usuarios, la actividad de los proveedores de servicio de telecomunicaciones y crea la Superintendencia de Telecomunicaciones.<sup>19</sup>
- f) Ley de Derecho de Autor y Derechos Conexos (Decreto Número 33-98 del Congreso de la República y sus reformas): regula lo relacionado con los programas de ordenador y bases de datos.

<sup>19</sup> Considerar además la Ley Reguladora del Uso y Captación de Señales Vía Satélite y su Distribución por Cable (Decreto Número 41-92 del Congreso de la República) y la Ley De Radiocomunicaciones (Decreto Ley 433 del Jefe de Gobierno de la República).

- g) Ley de Promoción del Desarrollo Científico y Tecnológico Nacional: constituye el Consejo Nacional de Ciencia y Tecnología –CONCYT- para impulsar el desarrollo científico y tecnológico de Guatemala.

Otras leyes complementarias en materia de comercio electrónico como el Código de Comercio, la Ley de Protección al Consumidor; se deben considerar, además, los tratados y convenios internacionales en la materia, así como las fuentes legislativas, en especial, las leyes modelo impulsadas por la UNCITRAL.

### 3. La Informática Jurídica

Durante el desarrollo de la Informática se realizaron estudios para utilizar sus aplicaciones en todas las ciencias, pero es cuando se empiezan a utilizar los sistemas informáticos en el campo del Derecho cuando surge el concepto Informática Jurídica la cual puede ser considerada como una rama, subdivisión o aplicación de la Informática que tiene por objeto utilizar los procedimientos, técnicas, herramientas y sus recursos propios, en el campo, materia, contenido o fines del Derecho. Antonio Pérez indica que “la Informática Jurídica estudia el tratamiento automatizado de: las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal (Informática jurídica documental); las fuentes de producción jurídica, a través de la elaboración informática tanto de los factores

lógico-formales que concurren en el proceso legislativo y en la decisión judicial (Informática jurídica decisional); y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho (Informática jurídica de gestión).” (1996)<sup>20</sup>

### 4. Clasificación de la Informática Jurídica

La definición anterior nos permite clasificar la Informática Jurídica en Informática jurídica de gestión, Informática jurídica documental e Informática jurídica decisional. El Doctor Julio Téllez establece en su obra Derecho Informático, una categorización similar indicando que “es posible clasificar dicha interdisciplina de la siguiente manera: a) Informática Jurídica Documentaria (almacenamiento y recuperación de textos jurídicos); b) Informática Jurídica de Control y Gestión (desarrollo de actividades jurídico-adjetivas); y c) Sistemas Expertos Legales o Informática Jurídica Metadocumentaria (apoyo en la decisión, educación, investigación, redacción y previsión del Derecho).” (2004)

En los próximos puntos explicaremos cada una de ellas e indicaremos ejemplos y aplicaciones relevantes para el profesional guatemalteco.

<sup>20</sup> No debe confundirse la Informática Jurídica con los cursos de computación para abogados, que consisten en enseñar al jurista al uso de programas del ordenador en su trabajo diario, como procesador de textos, sistema operativo, hojas electrónicas, navegación y correo electrónico, entre otros.

## 5. La Informática Jurídica de Gestión (Ayuda a la organización)

Los avances más sustanciales en materia de Informática aplicada al Derecho los vemos en la denominada automatización de las actividades y gestiones de carácter jurídico que se realizan en la oficina jurídica, tribunales de justicia, administración pública o en cualquier lugar donde el ordenador o computador realiza de manera más eficiente y óptima todas “aquellas operaciones estandarizadas y que obedecen a pautas regulares y constantes en la escritura, el registro, la trascipción, la contabilidad, la documentación, la comunicación y la certificación.” (Pérez, 2001) Las actividades anteriores también son identificadas como la Ofimática o Burótica.

En el mercado guatemalteco, encontramos una serie de programas para automatizar la actividad del Notario, desde proporcionar una recolección de formato o minutos de escrituras públicas y documentos notariales en general, hasta programas que ofrecen al usuario aplicaciones para un

sistema integral del trabajo de la oficina jurídica, tanto del ámbito notarial como control de procesos judiciales.

El desarrollo de programas de ordenador para facilitar y optimizar el trabajo del jurista alcanza también a la administración pública y en algunos casos se desarrolla una plataforma específica para la administración de los expedientes administrativos o judiciales, así como para documentar cada actuación y efectuar un control sobre el seguimiento de cada trámite como es el caso del Instituto de la Defensa Pública Penal.

La aplicación de la metodología informática a toda actividad de trabajo en la oficina jurídica, no queda solo como medio de optimización del documento jurídico o expedientes legales, sino que además atañe otros procesos como el acceso regstral y el operacional. En Guatemala, encontramos un claro ejemplo en el acceso remoto (en línea) a los registros, el cual proporciona el Registro General de la Propiedad de la Zona Central. Entre las funciones que pueden realizarse y que se identifican en el sitio como “Consulta a Distancia” se encuentran la consulta de propiedades, el seguimiento a documentos presentados y validar razones de testimonio.

En el caso de las consultas en línea, se deberá realizar un prepago presentándose a las oficinas del Registro. En los otros dos servicios

No.	Tp	F-INI	H-INI	F-FIN	H-FIN	REPON(s)	ESTADO	DÍAS
000015	J					SUPERVISOR	FINALIZADA	0
000008	J	15-02-2008	14:22	15-02-2008	14:27	SUPERVISOR	FINALIZADA	0
000011	J							
000003	J							
000004	J							
000005	J							
000016	J							
000014	J							
000010	J							
000007	F							
000009	J							
000001	J							
000012	J							
000006	J							
000002	I							

Programa para Control de Casos

electrónicos no se realiza ningún pago. Puede tener acceso en: [www.rgp.org.gt](http://www.rgp.org.gt).

The screenshot shows the homepage of the Registro General de la Propiedad. At the top, there's a banner with the text "REGISTRO GENERAL DE LA PROPIEDAD" and "Bordando Certeza y Seguridad Jurídica". Below the banner, there's a navigation bar with links for "Inicio", "Historia", "Visión y Misión", and "Autoridades". On the left, there's a sidebar with links for "Consulta a Distancia de Propiedades", "Consulta de Propiedades", "Seguimiento a Documentos", "Validar Razones Registrales", "Reportar Error de Inscripción en Comisión Nacional Registral", "Publicaciones", "Nuevos Servicios y Producto", "Preguntas más Frecuentes", "Arancel y Reglamento", "Legislación Registral", "Procedimientos", "Formularios", and "Ley de Acceso a la Información Pública". In the center, there's a large image of a key and a login form with fields for "Usuario" and "Password", and a button labeled "Ingresar". Below the login form, there's a message about consulting services at the agency. At the bottom, there's a footer with a logo for "cybertrust certified" and a statement: "Registro General de la Propiedad es Número 1 en Latinoamérica y el Caribe, según el Doing Business 2010 Report".

Página principal sitio web Registro General de la Propiedad

Uno de los registros públicos que aprovecha en forma eficiente las distintas aplicaciones informáticas es el Registro Mercantil en el sitio [www.registromercantil.gob.gt](http://www.registromercantil.gob.gt); es importante mencionar que a través del sitio descrito pueden efectuarse procedimientos administrativos en línea, lo cual optimiza el trabajo de la abogacía y el notariado, y lo más importante, que es un impulso a la certeza jurídica, al comercio y a las inversiones.

En cuanto a la que podemos denominar Informática Jurídica de Gestión Operacional, se utiliza en un inicio en el

campo jurídico procesal para controlar la actuación o etapas de un proceso específico, tanto en la vía administrativa como en la judicial. En Guatemala, estos servicios son prestados por la administración pública como en el Centro Administrativo de Gestión Penal y en el Centro de Servicios Auxiliares de Administración de Justicia, cuando se empieza a llevar un control electrónico del trámite de los procesos. En el Ministerio Público, se cuenta con el Sistema Informático del Control de Casos del Ministerio Público –SICOMP-. El Organismo Judicial

implementó el sistema de información para consulta de expedientes judiciales (departamento de Guatemala), lo cual se encuentra disponible en Internet a través del sitio web del Organismo Judicial [www.oj.gob.gt](http://www.oj.gob.gt).

The screenshot shows the homepage of the Organismo Judicial. At the top, there's a banner with the text "ORGANISMO JUDICIAL REPÚBLICA DE GUATEMALA" and "PBX: 1549". Below the banner, there's a navigation bar with links for "Inicio", "Menú Principal", "Inicio", "Organismo Judicial", "Corte Suprema de Justicia", "Organización", "Información Judicial", "Información Administrativa", "Mensaje del Presidente", "Memoria de Labores", and "Periodos de Vacaciones para Funcionarios y Personal del Organismo Judicial". There are also links for "Leyes y Resoluciones", "Directorio Telefónico", "Mapa del Sitio", and "Buscar". In the center, there's a news article titled "OJ Y GOBERNACIÓN SE REÚNEN PARA HACER FRENTE A LA DELINCUENCIA" dated Wednesday, December 09, 2009, 15:37. The article features a photo of several men in suits sitting around a conference table. To the right, there's another news article titled "DÍA DE LA TRANSPARENCIA" dated Wednesday, December 09, 2009, 15:32. The right sidebar contains links for "Servicios al Público", "CENADOJ", "Antecedentes Penales", "Juzgados Móviles", "Unidad de...", "Consulta de Expedientes Judiciales", "Archivo General de Protocolos", "Requisitos de Inscripción ABOGADOS Y NOTARIOS", "Otras Publicaciones", and "Denuncias y Quejas".

Página principal Sitio web Organismo Judicial

Un ejemplo legal del uso de TIC en la administración pública lo encontramos en la Ley de Acceso a la Información Pública cuando, establece:

**Artículo 38. Procedimiento de acceso a la información pública.** El procedimiento para el acceso a la información pública se inicia mediante solicitud verbal, escrita o vía electrónica que deberá formular el interesado al sujeto obligado, a través de la Unidad de Información.

Lo anterior obliga a la administración pública a considerar la optimización de los servicios públicos al utilizar los sistemas informáticos como vía; además, la ley indica que:

**Artículo 39. Sistemas de información electrónicos.** Los sujetos obligados establecerán como vía de acceso a la información pública, entre otros, sistemas de información electrónicos.

Bajo responsabilidad de la autoridad máxima garantizará que la información publicada sea fidedigna y legítima.

La información publicada en los sistemas de información electrónicos, entre otros, deberá coincidir exactamente con los sistemas de administración financiera, contable y de auditoría y deberá ser actualizada en los plazos establecidos en esta ley.

**Artículo 40. Respuesta en sistemas de información electrónicos.** Los sujetos obligados adoptarán las medidas de seguridad que permitan dotar de certeza a los informes enviados por mensajes de datos. En cualquier caso conservarán constancia de las resoluciones originales.

Otros ejemplos importantes los encontramos en la Superintendencia de Administración Tributaria -SAT-, la cual ha logrado digitalizar procedimientos como el cumplimiento de obligaciones tributarias o servicios en materia aduanera. El sitio [www.sat.gob.gt](http://www.sat.gob.gt) brinda más información. El portal del Sistema de Información de Contrataciones y Adquisiciones del Estado –Guatecompras- cual cuenta con un sistema electrónico que se administra a través de Internet para que el Estado de Guatemala pueda cumplir con varias de las etapas en el sistema de contrataciones; el sitio web es [www.guatecompras.gt](http://www.guatecompras.gt). Las últimas reformas a la Ley de Contrataciones del Estado establecieron:

**Artículo 35. Notificación electrónica e inconformidades.** Las notificaciones que provengan de actos en los que se aplique la presente Ley, serán efectuadas por vía electrónica a través de GUATECOMPRAS, y surtirán sus efectos al día siguiente de su publicación en dicho sistema.

Lo anterior es otro ejemplo de la informatización o automatización de los procedimientos de la administración pública.

## 6. La Informática Jurídica Documental

Esta clase de Informática Jurídica consiste en el tratamiento automatizado de las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal. La información a la que se acceda vía electrónica puede encontrarse de una forma simple o de una forma automatizada para su búsqueda. Las clases de documentación que procesa la Informática Documental se clasifican en documentación legislativa, documentación jurisprudencial y documentación doctrinal.

El volumen de los ordenamientos legales se encuentra en un crecimiento constante al generarse nuevas acciones o hechos en la sociedad que el legislador debe normar, reformar o en algunos casos, derogar, e inclusive, dejar sin vigencia; contar con acceso constante a esa actualización de carácter legislativo se queda limitada solo con la publicación del Diario Oficial en formato papel, porque este último únicamente permite contar con el documento normativo, pero no con una base de datos que permita consultar de manera automatizada la normativa específica para el caso concreto y su relación con otras leyes. En el caso de la documentación legislativa, dependerá del ente competente que emite la norma, siendo el caso del Congreso de la República muy particular porque tiene por disposición legal, la obligación de proporcionar el acceso a los Decretos emitidos en línea; al respecto, la

Ley Orgánica del Organismo Legislativo en el Artículo 152 ter<sup>21</sup> establece:

Artículo 152 ter. Disponibilidad de información en Internet. Toda iniciativa de ley presentada al Congreso de la República, los decretos, acuerdos, puntos resolutivos y resoluciones, serán dados a conocer a la población por los medios electrónicos correspondientes. La Dirección Legislativa es la responsable de que tales instrumentos legales estén disponibles para las consultas que la población requiera en dichos medios electrónicos.

Además, se pueden obtener los proyectos de ley (iniciativas) recientes en el sitio web [www.congreso.gob.gt](http://www.congreso.gob.gt). Es importante hacer mención que el sitio del Congreso de la República ha logrado un buen desarrollo en la incorporación digitalizada de las publicaciones del Diario Oficial de los Decretos en formato PDF y hace mención en la introducción a cada Decreto de las reformas, inconstitucionalidades y otros aspectos de interés para cada Decreto; además, en el sitio se encuentran otros ordenamientos legales que no han sido emitidos por el Congreso de la República, como Acuerdos Gubernativos, Acuerdos de entidades descentralizadas y autónomas, Acuerdos de la Corte Suprema de Justicia, entre otros, convirtiéndolo en una valiosa fuente de información

---

<sup>21</sup> Adicionado por el Decreto No. 37-04 del Congreso de la República, artículo 22.

PDF	De Fecha	Decreto No.	Nombre o Descripción de la Ley
	27/Oct/2009	<a href="#">37-2009</a>	Aprueba el tratado de libre comercio entre Centroamérica y Chile y el Protocolo Bilateral entre ...
	22/Oct/2009	<a href="#">36-2009</a>	Ratifica el Decreto Gubernativo 10-2009 de fecha 8 de septiembre de 2009.
	03/Dic/2009	<a href="#">35-2009</a>	Reforma al decreto 21-2009 del Congreso de la República, Ley de Competencia Penal en Procesos e ...
	23/Sep/2009	<a href="#">33-2009</a>	Aproueba el convenio de Rotterdam, para la aplicación del procedimiento de consentimiento fundam ...
	23/Sep/2009	<a href="#">32-2009</a>	Modifica el decreto número 10-2009 del Congreso de la República, por medio del cual se aprueba e ...
	22/Sep/2009	<a href="#">31-2009</a>	Aproueba el a) el acuerdo de alcance parcial entre el gobierno de la República de Guatemala y el ...
	20/Ago/2009	<a href="#">30-2009</a>	Exonera el pago del Impuesto al Valor Agregado -IVA- y demás derechos arancelarios a la importa ...

Sitio web del Congreso de la República

Otros órganos que colocan su normativa en línea, así como ordenamientos legales relacionados, son la Superintendencia de Administración Tributaria ([www.sat.gob.gt](http://www.sat.gob.gt)), el Banco de Guatemala ([www.banguat.gob.gt](http://www.banguat.gob.gt)), y la Municipalidad de Guatemala ([muniguate.com](http://muniguate.com)), entre otros.

Las fuentes de información también son proporcionadas por entes de carácter privado, aunque la información que brinden sea de naturaleza pública. Estas empresas cuentan con amplias bases de datos de sumo interés para los juristas e investigadores, las cuales mantienen un ambiente "amigable" para el usuario. El costo del servicio varía en la forma de pago desde cancelar por cada una de las consultas, o una cuota mensual, semestral o anual por el servicio, en la mayoría de los casos, previo contrato de acceso.

Una de las ventajas que proporcionan algunos sitios privados es la compilación de la información normativa en base de datos, lo que permite consultas por casos o temáticas, lo cual no tiene disponible los sitios de la administración pública. La digitalización de las leyes y reglamentos han cambiado las tradicionales "Biblia Jurídicas" de papel a las compilaciones digitales, pudiendo contar actualmente con bases de datos legislativas completas instaladas en nuestras

computadoras personales de escritorio, o portátiles, e inclusive, almacenarlas en nuestras agendas de mano o teléfonos móviles. Algunos sitios web para servicios en línea son [www.infile.com](http://www.infile.com), [www.leyesdeguate.com](http://www.leyesdeguate.com), [www.lexdelta.com](http://www.lexdelta.com).

En el ejercicio profesional, la investigación y la procuraduría, entre otras funciones, se hace necesario tener acceso a los fallos en materia de jurisprudencia, o en su caso, a la doctrina legal. El usuario puede adquirir las gacetas en formato papel, pero resultan onerosas, ocupan mucho espacio y no son automatizadas. También puede consultar las bibliotecas, pero no todos los diarios oficiales se encuentran en buen estado.

Para optimizar esto, las bases de datos jurídicos que contienen jurisprudencia se han almacenado en dispositivos ópticos o electromagnéticos que permiten al usuario,

entre otros beneficios, transportarlos cómodamente, y sobre todo, la automatización para realizar búsquedas específicas.

En cuanto a materia jurisprudencial de amparo, inconstitucionalidad y otros fallos, la Corte de Constitucionalidad y el Organismo Judicial han emitido una serie de CD-ROM, lo cual permiten las consultas fuera de línea, pero sigue siendo una de las mejores opciones acceder al sistema vía la Internet (en línea). En Guatemala, existen empresas privadas y organizaciones no gubernamentales (ONG) que proporcionan un acceso de carácter automatizado a consultas generales y específicas, pero son los sitios de la Corte de Constitucionalidad [www.cc.gob.gt](http://www.cc.gob.gt) y el del Organismo Judicial [www.oj.gob.gt](http://www.oj.gob.gt) quienes proporcionan una opción gratuita a la información jurisprudencial, con una base de datos accesible, aunque con limitaciones.

En el sitio web de la Corte de Constitucionalidad, se permite el acceso a la base de datos identificada como “Gacetas Jurisprudenciales (MLex) Para acceso a usuarios externos”

Inicio | Gaceta y Jurisprudencia  
Enlaces a bases de datos documentales

Gacetas Jurisprudenciales (MLex)  
Para acceso a usuarios externos

Gacetas Jurisprudenciales Corte (MLex)  
Para acceso a usuarios internos de la Corte de Constitucionalidad

Base de datos externa Corte de Constitucionalidad

2818-2005 - Windows Internet Explorer  
<http://200.35.179.201/masterlex/default.asp>

**MasterLex**

Palabras Similares Buscar  
En Documentos De Todas las bases de datos

Vistas del Árbol Normal Cambiar

Exportar <->Regresar

Corte de Constitucionalidad  
Inconstitucionalidades de Caráct  
2006  
Gaceta Jurisprudencial N.75  
1011-2005  
1122-2005  
1173-2003  
1206-2005  
1243-2005  
1319-2003  
1331-2005  
1421-2004  
1581-2004, 2156-2004 Y  
1584-2004

LEYES APLICABLES  
Artículos citados, 267, 268 y 272, inciso a), de la Constitución Política de la República de Guatemala; 114, 133, 134, 143, 144, 145, 149, 163 inciso a), 183 y 185 de la Ley de Amparo. Exhibición Personal y de Constitucionalidad; y 31 del Acuerdo 4-89 de la Corte de Constitucionalidad.

PODER JUDICIAL  
JUAN FRANCISCO FLORES JUÁREZ  
PRESIDENTE  
RODOLFO ROHRMOSER VALDEAVELLANO  
MAGISTRADO  
MARIO GUILLERMO RUIZ WONG  
MAGISTRADO  
CARLOS ENRIQUE LUNA VILLACORTA  
MAGISTRADO  
LUIS DE JESÚS HERNÁNDEZ TORRES  
SECRETARIO GENERAL

SAÚL DIGHERO HERRERA  
MAGISTRADO  
CIPRIANO HUERTAS SOTO TOBAR  
MAGISTRADO  
GLORIA MELGAR DE AGUILAR  
MAGISTRADA

POR TANTO  
Corte La de Constitucionalidad, con base en lo considerado y leyes citadas, resuelve: I. Con lugar la acción de inconstitucionalidad de ley general, de carácter parcial, promovida por el Procurador de los Derechos Humanos, que impugnó el artículo 200 del Código Penal. Como consecuencia de este pronunciamiento, se expulsa del ordenamiento jurídico el artículo impugnado. Los efectos del presente fallo se retrotraigan a la fecha en la que se publicó la suspensión provisional decretada en el Diario Oficial. II. Publíquese. III. Notifíquese.

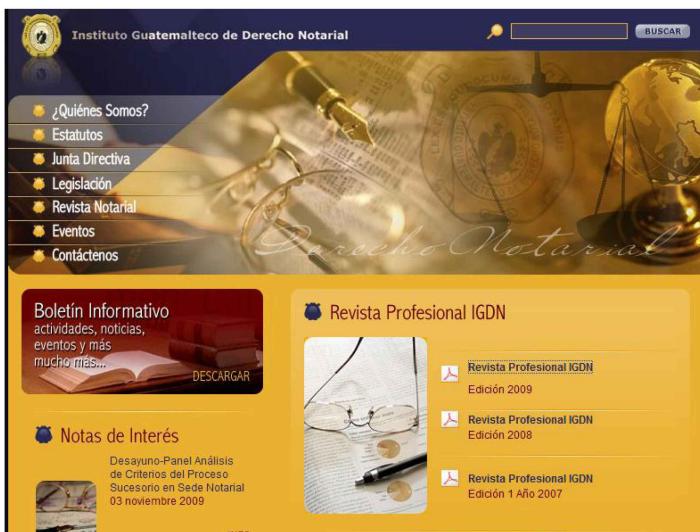
Página principal sitio web Corte de Constitucionalidad

Encontramos sitios importantes que contienen legislación de carácter internacional para el estudio y aplicación del Derecho, entre los que tenemos: Corte Interamericana de Derechos Humanos [www.corteidh.or.cr](http://www.corteidh.or.cr), Corte Centroamericana de Justicia [www.ccj.org.ni](http://www.ccj.org.ni), Organización Internacional de Trabajo [www.ilo.org](http://www.ilo.org), Corte Penal Internacional [www.un.org/icc](http://www.un.org/icc), Organización de las Naciones Unidas (ONU) [www.un.org/spanish](http://www.un.org/spanish), Organización Mundial de la Propiedad Intelectual [wwwOMPI.org](http://wwwOMPI.org), entre otros.

En cuanto a la Informática Jurídica Documental en lo relativo a doctrina, encontramos un listado enorme de sitios en materia de temas extranjeros. Basta con ingresar a uno de los buscadores más conocidos y colocar el término a investigar para que cientos, y en algunos casos, miles de páginas de información puedan ser accedidas por el usuario. En la mayoría de los sitios, el acceso es gratuito, pero en

otros sí es necesario hacer un pago para proporcionar la información o suscribirse al servicio. Como ejemplo en materia de Informática Jurídica y Derecho Informático encontramos los sitios: [www.alfa-redi.org](http://www.alfa-redi.org), [www.derecho.com](http://www.derecho.com), [www.delitosinformaticos.com](http://www.delitosinformaticos.com), [www.vlex.com](http://www.vlex.com) entre otros.

En materia de doctrina guatemalteca relativa al Derecho y las ciencias con las que se relaciona, la información se encuentra muy limitada en Internet. La mayoría de publicaciones y artículos escritos por autores guatemaltecos en materia de Derecho, se encuentra en formato papel como la Revista del Colegio de Abogados y Notarios de Guatemala [www.colegioabogadosynotarios.org.gt](http://www.colegioabogadosynotarios.org.gt) y no se publica en formato digital, contrario a la Revista del Instituto Guatemalteco de Derecho Notarial que publica su revista en formato digital [www.igdnotarial.org.gt](http://www.igdnotarial.org.gt).



Sitio web del Instituto Guatemalteco de Derecho Notarial

El sitio web del Instituto de la Defensa Pública penal [www.idpp.gob.gt](http://www.idpp.gob.gt) cuenta con distintas publicaciones en línea entre los que se encuentran los módulos instructoriales en versión digital (PDF), revistas del defensor y folletos de apoyo a la labor del abogado defensor.



Sitio web del Instituto de la Defensa Pública Penal / Publicaciones / doctrina

Otro sitio es la página web del Centro de Estudios de Derecho –CEDE- que proporciona información para estudiantes de Derecho, estudiantes pendientes de examen técnico profesional y abogados y notarios en [www.cede.com.gt](http://www.cede.com.gt). En el caso de investigación nacional el sitio web del Instituto Nacional de Estadística proporciona datos fundamentales [www.ine.gob.gt](http://www.ine.gob.gt). En el caso de doctrina a nivel internacional, encontramos en América Latina sitios recomendados como:

<http://www.legislaw.com.ar/doctri/filo.htm>  
<http://www.bibliojuridica.org/>  
<http://www.juridicas.unam.mx/publica/>

## 7. La Informática Jurídica Decisional (Ayuda a la Decisión)

La Informática Jurídica Decisional también denominada Metadocumental, consiste en el empleo de ordenadores como ayuda para la toma de decisiones de carácter jurídico. Ello va a depender de muchos factores, desde la evolución de la inteligencia artificial y los denominados sistemas expertos, hasta crear una cultura informática que permita la integración de los procedimientos informáticos a los procedimientos jurídicos. Es importante recalcar que no se pretende que el ordenador resuelva la decisión que le corresponde al juzgador, el fin es contar con un apoyo en la toma de decisiones.

## 8. El uso de Internet para el profesional del Derecho

Desde que empecé a utilizar la Internet pude percibirme que su alcance en la ciencia del Derecho dependerá de muchos factores, pero son dos los principales: el primero es el factor técnico, de simple solución por la facilidad que representa su uso y la reducción en sus costos; el segundo factor, complicado en algunos casos, superar la actitud, la "mentalidad" o el interés que se tenga en su incorporación y uso en las actividades a realizar, la disponibilidad del sujeto para su autoaprendizaje; este segundo factor es precisamente el problema que ha tenido en el Derecho, por lo que es importante indicar que no tenemos una cultura informática en el área jurídica. Es necesario desarrollar estudios y proyectos encaminados a superar esa situación incómoda, ese desinterés por su estudio e incorporación en las actividades

del jurista y que tiene como efecto limitarnos en el acceso a las herramientas TIC que se pueden aprovechar en el ejercicio profesional del jurista.

Una de las preguntas de partida es ¿Para qué sirve la Internet en el Derecho?, lo cual generaría una respuesta extensa, pero que Víctor Rojas (2000) resume en cuatro áreas: La Internet como medio de comunicación, el acceso a fuentes de información, la comercialización de los servicios profesionales y la Internet como objeto de estudio del Derecho. A lo anterior me permito agregar la posibilidad de realizar estudios e investigación on line (en línea).

### 8.1. La Internet como medio de comunicación

El utilizar la Internet como medio de comunicación sigue siendo una de las mayores ventajas para los abogados y notarios y que mayor utilización tiene actualmente en Guatemala, siendo la principal el uso del correo electrónico, que representa una forma de comunicación en la cual el contenido de lo transmitido puede ser procesado, con la ventaja que factores como la distancia o el tiempo son superados fácilmente, porque colegas o clientes pueden estar en otro ámbito territorial, inclusive en otro Estado con diferente uso horario, que en cuestión de segundos o minutos estarán recibiendo la información necesaria.

## 8.2. El acceso a fuentes de información

La información es parte importante del trabajo legal y el acceso a las fuentes que la contienen es sumamente necesario, en especial, por uno de los factores más importantes en el trabajo jurídico, el factor tiempo. Las bases de datos jurídicas en Guatemala como la accesible de forma gratuita en [www.congreso.gob.gt](http://www.congreso.gob.gt), o que por medio de pago como [www.infile.com](http://www.infile.com) o [www.accionciudadanaciel.org](http://www.accionciudadanaciel.org), así como la de otros Estados, facilitan la investigación y el trabajo<sup>22</sup>, en especial en las ramas del Derecho Internacional<sup>23</sup>; además, para ampliar el conocimiento jurídico existen fuentes de información doctrinarias, a las que se puede tener acceso de manera fácil y rápida, que son las aplicaciones fundamentales de la Informática Jurídica Documental expuesta en punto anterior.

## 8 . 3 . La comercialización de los servicios profesionales

Los abogados y notarios brindan servicios profesionales por lo que el campo profesional que ejercen debe ser conocido por el público en general como posibles clientes o usuarios de sus servicios.

Una persona que esté al día en materia de procesos informáticos e interesada en contar con los servicios de un profesional del Derecho, espera como mínimo que el profesional se encuentre en una situación similar, para poder realizar los actos previos o posteriores en que no se necesite la presencia de las partes o la inmediación del asesor jurídico, facilitar las consultas, envío y recepción de datos y documentos, ahorro de tiempo y recursos, entre otros aspectos. Cabe mencionar que contar con un sitio web es cada día más accesible y registrar el nombre de dominio del bufete u oficina profesional se realiza en línea, incluso, existen directorios electrónicos para abogados y notarios.

The screenshot shows the homepage of ABOGADOS-Guatemala.com. At the top, there is a navigation bar with links for 'Inicio', 'Quienes Somos', 'Como elegir a su abogado', and 'Contáctenos'. Below the navigation is a large search bar labeled 'Buscar en este sitio' with a magnifying glass icon. To its right is a yellow button labeled 'Inscriba su despacho'. The main content area features a large image of a magnifying glass focusing on a map of Central America, specifically highlighting Guatemala, with labels for Mexico, Belice, Ocean Atlántico, Honduras, and El Salvador. To the right of the map, there is a section titled '¡Optimice su Despacho!' with text about improving contacts, tools, and opportunities, and a call to action to try the map and search engines. Further down, there are sections for 'RECURSOS' (Periodicals and Revistas, SITIOS GUBERNAMENTALES) and 'ARTICULOS' (with a preview of an article by Steve Jobs). On the right side, there is a sidebar for 'Publicidad' featuring the 'Portal Jurídico' at [www.leyesyopiniones.com](http://www.leyesyopiniones.com), a poll asking '¿Quién es el legítimo presidente de Honduras?', and a section for 'Ultimos agregados' with a link to David Alberto Juarez Aldana's profile.

Directorio electrónico

<sup>22</sup> Estar actualizado de la emisión, reformas o derogación de normas jurídicas, es parte relevante del trabajo jurídico. Una forma práctica y gratuita es suscribirse al sumario que envía el CENADOJ lo cual se realiza enviando un correo-e a [cenadoj@oj.gob.gt](mailto:cenadoj@oj.gob.gt)

<sup>23</sup> El acceso a Tratados Internacionales es otro ejemplo, en especial aquellos que tienen efectos en nuestro ordenamiento jurídico. En materia laboral [www.oit.org](http://www.oit.org); en materia de propiedad intelectual [wwwOMPI.org](http://wwwOMPI.org).

#### 8.4. La Internet como objeto de estudio del Derecho

La incorporación de la Internet en las actividades personales produce una serie de efectos en la sociedad, por lo cual se convierte en un objeto de estudio e investigación, en especial porque por medio del ciberespacio podemos adquirir derechos y obligaciones. Ese conjunto de acciones o hechos que se realizan en las plataformas electrónicas son innumerables, de constante cambio y desarrollo. En este punto, encontramos el tema principal a ser tratado por la ciencia del Derecho, la cual debe realizar profundos estudios de la Internet y sus efectos, estudios que deben evolucionar constantemente.

#### 8.5. Estudios e investigación jurídicos on line (en línea)

La capacitación, aprendizaje o educación, utilizando la plataforma de comunicación de la Internet se denomina comúnmente e-learning y está siendo aprovechada para estudiar y capacitarse, por lo que deben evaluarse aspectos como adaptabilidad de los horarios laborales a los de estudio, ausentarse largos períodos de tiempo, costo, distancia entre el centro de estudio y el hogar o trabajo, calidad y acreditación del docente, temas especializados, y un sin fin de factores que inciden en la decisión. El factor tiempo, distancia y estudios especializados, han sido superados a través de los estudios por la Internet, brindándose a los profesionales una serie de posibilidades académicas, incluso de áreas jurídicas y no jurídicas que no se cuentan en Guatemala. Para aprovechar este sistema, se crean salones

virtuales cuando se quiere trabajar en grupo, o bien desde su ordenador en forma individual. Un ejemplo en Guatemala es la capacitación que realiza la Escuela de Estudios Judiciales con los Jueces de Paz ([www.oj.gob.gt](http://www.oj.gob.gt)). Deben considerarse, además las opciones de becas por vía electrónica tanto en información como en su otorgamiento ([www.fundacioncarolina.es](http://www.fundacioncarolina.es)).





## EJERCICIOS DE AUTOAPRENDIZAJE

1. El abogado defensor de oficio es notificado que se le asigna un caso por abandono de la defensa privada; faltan diez días para que el Ministerio Público formule la solicitud de apertura a juicio y presente la acusación. En la tesis de defensa es necesario verificar: a) la propiedad de dos bienes inmuebles; b) si el delito por el que se encuentra sindicado no ha sufrido reformas; y, c) analizar la jurisprudencia existente. ¿De qué manera y en donde consultaría para ahorrar tiempo y tener la información veraz?
2. Consulte el estado de un expediente o el nombre de una de las personas que representa vía electrónica.
3. Le notifican que el imputado desea participar como colaborador eficaz para obtener los beneficios que establece la ley en un caso de narcotráfico. El hecho ilícito se cometió el 3 de julio de 2009 y solicita hoy, participar colaborando. Verifique vía Internet en algunos de los sitios disponibles, la fecha de la Reforma de la Ley Contra la Delincuencia Organizada para establecer si es posible gozar del beneficio por el ámbito temporal de la ley.
4. Verifique en la jurisprudencia guatemalteca cuales fueron las últimas declaratorias de inconstitucionalidad de carácter general de la Ley en Materia de Antejuicio.



## CAPÍTULO 3

### LOS PROGRAMAS DEL ORDENADOR Y LOS DATOS PERSONALES

La protección por el régimen de derecho de autor de los programas informáticos existe en la mayoría de los países y ha quedado armonizada en diversos tratados internacionales a tal efecto.

Este régimen permite al autor de un programa de computación determinado licenciarlo bajo los términos y condiciones que estime convenientes conforme su modelo de negocios. En tal sentido, se advierte la existencia de infinidad de licencias, que van desde las más restrictivas hasta las más permisivas.

Dentro de este último grupo se encuentran las denominadas licencias libres, existiendo algunas que procuran perpetuar la libertad y evitar que se añadan nuevas restricciones, para lo cual insertan la cláusula copyleft, concepto que en modo alguno se opone al copyright, sino que se apoya en él y le imprime un nuevo sentido, preservando la libertad en el uso del software.

Fernando Maresca



## CONTENIDO DEL CAPÍTULO

Los programas de ordenador constituyen creaciones del intelecto humano, por ello, el Derecho los reviste de una protección que garantiza a sus titulares, los derechos morales y patrimoniales de su producción. Uno de los programas de ordenador más populares en el trabajo jurídico es el denominado procesador de texto; al redactar un documento como una demanda o una escritura pública, el contenido queda almacenado como un archivo; cuando el usuario, utilizando los programas de ordenador, ingresa datos a una computadora a través de un procedimiento técnico, por medio del cual se organiza y clasifica en forma lógica e interrelacionada la información para que pueda ser consultada posteriormente a través de instrucciones preestablecidas, se crea una base de datos o banco de datos. Por lo anterior, es necesario distinguir qué es lo que está almacenado en los dispositivos electromagnéticos de una computadora (disco duro); existen tres elementos o en su caso bienes jurídicos grabados en forma de archivo que hay que distinguir: Los programas de ordenador (software), con lo que se realiza el vínculo entre el usuario y la computadora y sus dispositivos de almacenamiento, así como la generación de archivos informáticos; los datos o en su caso la información, que cuando atienden a identificadores de las personas deben ser regulados y protegidos por medio de normas legales.

Estos datos de las personas son parte de sus derechos humanos (inherentes a la persona), por lo que están sujetos a la protección, al igual que las bases de datos, que es el conjunto ordenado sistemáticamente de identificadores de conocimiento.

Determinar los aspectos legales fundamentales para los programas de ordenador, las bases de datos y los datos personales, es el objetivo de este capítulo.





## Objetivos Específicos

- a) Fundamentar las normas jurídicas que regulan los aspectos generales y específicos de los derechos de autor en materia de programas de ordenador.
- b) Ampliar el conocimiento en materia de los derechos humanos de las personas en relación con sus datos personales contenidos en bases de datos públicas.
- c) Analizar los aspectos informáticos contenidos en la Ley de Acceso a la Información Pública.



## LOS PROGRAMAS DEL ORDENADOR Y LOS DATOS PERSONALES

### 1. Los Programas de Ordenador (Software)

Es uno de los elementos en un sistema informático y se conoce comúnmente con el término software al programa o conjunto de programas que se utilizan en la computadora para ingresar, almacenar y procesar los datos (sistemas operativos, paquetes, utilitarios, etc.); el concepto adecuado para este tema es programas de ordenador, aunque el Código Penal guatemalteco lo denomina programas de computación.

La Ley de Derechos de Autor y Derechos Conexos -LDADC- (Decreto Número 33-98 del Congreso de la República y sus reformas) establece la definición legal del concepto programa de ordenador en el artículo 4 como “La obra constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma, que al ser incorporadas a un soporte legible por máquina, es capaz de hacer que un ordenador ejecute determinada tarea u obtenga determinado resultado.” Se define en doctrina como “un conjunto de órdenes o instrucciones que, siguiendo una lógica determinada, guían o dirigen las actividades del sistema (ordenador), indicándole las acciones u

operaciones a realizar para lograr el fin deseado.” (Davara, 2006)

### 2. Aspectos legales de los programas de ordenador

Los programas de ordenador, como creaciones intelectuales del ser humano, se encuentran establecidos en la categoría de derechos de autor, por lo tanto, se regulan y protegen por la Ley de Derechos de Autor y Derechos Conexos, en especial, convenios internacionales en la materia; además, se debe verificar lo establecido entre dos o más partes en acuerdos y contratos.

Por ser un bien creado por el intelecto humano de reciente existencia, ha pasado por diversas etapas, iniciándose en los años sesenta, cuando se consideraba que no existía distinción entre el hardware y el software y que eran parte intrínseca uno del otro. Conforme se desarrollan los avances en computación, los creadores de estos bienes se ven obligados a que un grupo de personas desarrolle el hardware y otro grupo el software. Ello tiene como incidencia que cada grupo de trabajo tenga derecho sobre lo que ha creado. El ejemplo claro lo tenemos con el surgimiento de la computadora personal, cuando un grupo de personas crea el hardware (IBM) y otro grupo el software (Microsoft). Se inicia entonces la distinción para poder proteger los derechos de sus creadores, empezando con la intención de protegerlo en el ámbito de la propiedad industrial, es decir, los programas de ordenador se registraban conforme al procedimiento de un invento, por lo que estaba sujeto al trámite de una patente. Posteriormente, se considera más conveniente y de facilidad para su incorporación, proteger a los programas de

ordenador con los mismos principios que los de las creaciones de la mente como obras literarias, poemas, canciones.<sup>24 -25</sup>

El Tratado sobre Derechos de Autor de la Organización Mundial de Propiedad Intelectual adoptado el 20 de diciembre de 1996 establece que:

**Artículo 4. Programas de Ordenador.** Los programas de ordenador están protegidos como obras literarias en el marco de lo dispuesto en el Artículo 2 del Convenio de Berna del Convenio de Berna. Dicha protección se aplica a los programas de ordenador, cualquiera que sea su modo o forma de expresión.

En virtud del tratado indicado y por las características y particularidades que representan los programas de ordenador, se hace necesario tener consideraciones especiales, corriente que sigue la Ley de Derechos de Autor y Derechos Conexos, en el Título II Derecho de Autor, Capítulo IV Disposiciones Especiales para Ciertas Categorías de Obras, Sección Segunda Programas de Ordenador y Bases de Datos,

como se encuentra regulado actualmente; la norma específica establece:

**Artículo 30.- Los programas de ordenador** se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o código objeto y cualquiera que sea su forma o modo de expresión. La documentación técnica y los manuales de uso de un programa gozan de la misma protección prevista para los programas de ordenador.

Los autores de las obras protegidas por el derecho de autor y en su caso los herederos, gozan de ciertos derechos básicos (morales y patrimoniales<sup>26</sup>) y derechos conexos.<sup>27</sup>

Uno de ellos es el derecho exclusivo a utilizar la obra de conformidad con la ley, o autorizar a terceros a aprovecharla en los términos que convienen de común acuerdo.

---

<sup>24</sup> Al proteger a los programas de ordenador con los derechos de autor se determina que “no están supeditados a la formalidad de registro y cualquier otra y son independiente y compatibles entre si, así como en relación con la propiedad y otros derechos que tengan por objeto el soporte material a la que esté incorporada la obra...” (Artículo 3, Ley de Derechos de Autor y Derechos Conexos).

<sup>25</sup> El Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio de la Organización Mundial de Comercio establece:

Artículo 10. Programas de ordenador y compilaciones de datos.

1. Los programas de ordenador, sean programas fuente o programas objeto, serán protegidos como obras literarias en virtud del Convenio de Berna (1971).
2. Las compilaciones de datos o de otros materiales, en forma legible por máquina o en otra forma, que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, serán protegidas como tales. Esa protección, que no abarcará los datos o materiales en sí mismos, se entenderá sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales en sí mismos.

<sup>26</sup> Ver: Artículos 18 al 25, Ley de Derechos de Autor y Derecho Conexos.

<sup>27</sup> Ver: Artículos 50 al 62, Ley de Derechos de Autor y Derecho Conexos.

El creador de una obra puede prohibir o autorizar<sup>28</sup> la reproducción bajo distintas formas de la obra, la publicación impresa o el grabado de sonidos, la ejecución o interpretación pública, las grabaciones de la obra bajo la forma de discos compactos, cassetes, videocasetes, su traducción en otros idiomas, entre otros derechos. El sujeto titular de los derechos de los programas de ordenador se identifica en la LDADC como el productor; al respecto, establece la normativa citada:

**Artículo 11.-** En los programas de ordenador se presume, salvo pacto en contrario, que el o los autores de la obra han cedido sus derechos patrimoniales al productor, en forma ilimitada y exclusiva, lo que implica la autorización para divulgar la obra y ejercer la defensa de los derechos morales en la medida en que ello sea necesario para la explotación del programa de ordenador.

Se presume, salvo prueba en contrario, que es productor del programa de ordenador la persona natural o jurídica que aparezca indicada como tal en el mismo.

Uno de los derechos más importante a considerar es el plazo de protección que gozará el titular del programa de ordenador; el artículo 44 de la LDADC establece:

**Artículo 44.-** En el caso de los programas de ordenador y de las obras colectivas, el plazo de protección será de setenta y cinco años contados a partir de la primera publicación o, en su defecto, de la realización de la obra.

Por “primera publicación” se entiende la producción de ejemplares puestos al alcance del público, disponibles en cantidad tal que pueda satisfacer sus necesidades razonables, tomando en cuenta la naturaleza de la obra.

### 3. Clasificación de los Programas de Ordenador

Existen varias formas de clasificar el software siendo la que más identifican los usuarios por la finalidad o funciones de los programas; los más comunes son sistemas operativos (Windows, OS, Linux), programas de uso general como los procesadores de texto, hojas electrónicas, edición de

---

<sup>28</sup> Artículo 21. El derecho pecuniar o patrimonial confiere al titular del derecho de autor, las facultades de utilizar directa y personalmente la obra, de ceder total o parcialmente sus derechos sobre la misma, y de autorizar o prohibir su utilización y explotación por terceros.

Sólo los titulares del derecho de autor y quienes estén expresamente autorizados por ellos, tendrán derecho de utilizar la obra de cualquier manera, forma o por medio de cualquier proceso y por consiguiente les corresponde autorizar o prohibir cualquiera de los siguientes actos:

- a) La reproducción y la fijación total o parcial de la obra en cualquier tipo de apoyo material, formato o medio, temporal o permanentemente, por medio de cualquier procedimiento conocido o por conocerse;
- d) La comunicación al público, directa o indirecta, por cualquier procedimiento o medio, conocido o por conocerse, en particular los siguientes actos:
  - 7) Acceso público a bases de datos y ordenadores por medio de las telecomunicaciones; y...
  - f) La importación y exportación de copias de sus obras o de fonogramas legalmente fabricadas y la importación y exportación de copias fabricadas sin su consentimiento.

\* Reformado por el artículo 85 de la Ley de Implementación del RD-CAFTA. (Transcripción parcial)

presentaciones, bases de datos (llamados también paquetes) y que actualmente se distribuyen como suites ofimáticas, es decir, la recopilación de varios programas destinados a la administración y edición de documentos (Office de Microsoft, OfficeOpen de Sun MicroSystem), programas de aplicaciones específicas denominados como “diseñados a la medida”, los programas utilitarios y de protección como los antivirus y antispyware, los lenguajes de programación o de desarrollo (como C++, Java, SQL, Visual Basic), programas para administración de redes, programas para el uso de aplicaciones en Internet como navegadores web, correo electrónico, entre otros. Por la relación del tema con el Derecho nos limitaremos a explicar la clasificación establecida en la ley o clasificación legal, y la clasificación por su forma de distribución al usuario.

El artículo 30 de la Ley de Derechos de Autor y Derechos Conexos clasifica los programas de ordenador de forma básica (clasificación legal) en programas operativos y programas aplicativos.<sup>29</sup>

Los primeros se definen como los programas que permiten la comunicación entre el computador y el usuario ejecutando las tareas esenciales del ordenador; los programas aplicativos son los que realizan los procedimientos de almacenar, procesar y acceder a la información.

La ley de la materia también hace referencia al código fuente y al código objeto;

el “código fuente de un programa informático es un conjunto de líneas de texto que son las instrucciones que debe seguir la computadora para ejecutar dicho programa.

Por tanto, en el código fuente de un programa está descrito por completo su funcionamiento. El código fuente de un programa está escrito por un programador en algún lenguaje de programación, pero en este primer estado no es directamente ejecutable por la computadora, sino que debe ser traducido a otro lenguaje (el lenguaje máquina o código objeto) que sí pueda ser ejecutado por el hardware de la computadora. Para esta traducción se usan los llamados compiladores, ensambladores, intérpretes y otros sistemas de traducción.” (Wikipedia, 2009) El código objeto es el resultado de compilar<sup>30</sup> las instrucciones del programa convirtiéndolo en el programa final o de disposición al usuario. Es importante tener presente que para cualquier modificación posterior al software se necesita contar con el programa o código fuente.

La clasificación por la forma de distribución de los programas lleva por objetivo determinar y delimitar los usos que el titular de la creación autoriza al usuario que lo adquiere y no solamente el costo del programa; se puede iniciar por clasificarlos en software propietario y software libre, aunque existen diversas modalidades para ambos, lo cual permite otras subcategorías, pero que van a estar relacionadas con aspectos como disponibilidad o no del

---

<sup>29</sup> Se protege además el quinto elemento de los sistemas de información como los son la documentación técnica y los manuales.

<sup>30</sup> Se conoce con el término compiladores a los programas o el procedimiento de convertir el código fuente en código objeto; esta acción también se identifica como “cerrar” el programa.

código fuente, contraprestación por el uso o adquisición del programa y cantidad de equipos al que se autoriza su instalación.<sup>31</sup>

Es importante diferenciar entre comprar el programa que es adquirirlo en propiedad, o la modalidad más común actualmente que es adquirir una licencia de usuario o el derecho de uso, para lo cual el usuario del software acepta las condiciones establecidas por el autor por medio del denominado Contrato de Licencia de Usuario Final, conocido como CLUF, en el cual cada distribuidor establece sus condiciones y términos, no limitándose a la obra y a su uso, sino que incorpora cláusulas relativas a exclusión de responsabilidades, competencia en caso de conflicto legal, entre otras.

Los programas en los que el autor se reserva todos los derechos que otorga la ley, en especial los patrimoniales (identificando por ello el costo del programa) y solo pone a disposición del usuario el código objeto se conoce como software propietario<sup>32</sup> o proprietary software; además, en la mayoría de casos se limita la instalación del programa a una sola computadora.<sup>33</sup>

Los ejemplos más comunes de estos programas son los distribuidos por Microsoft, Adobe, Macintosh, entre otros, y se encuentran instalados en más del 90% de computadoras en Guatemala en virtud que la mayoría de usuarios utilizan programas de este tipo conocidos en la jerga informática como “programas enlatados”. Para el uso de los programas el usuario realiza un pago que le permite utilizarlos en una computadora y los puede adquirir en el momento de la compra del ordenador, o posteriormente. Establece la LDADC lo siguiente:

#### Artículo 32.

La reproducción de un programa de ordenador, incluso para uso personal, exigirá la autorización del titular de los derechos, con excepción de la copia que se haga con el fin exclusivo de sustituir la copia legítimamente adquirida, cuando ésta ya no pueda utilizarse por daño o pérdida. Sin embargo, ambas copias no podrán utilizarse simultáneamente.

---

<sup>31</sup> La LDADC establece al respecto:

Artículo 33. Es lícita la introducción de un programa en la memoria interna del ordenador que sirva únicamente para efectos de la utilización del programa por parte del usuario. No es lícito el aprovechamiento del programa por varias personas mediante la instalación de redes, estaciones de trabajo y otro procedimiento análogo, sin el consentimiento del titular de los derechos.

<sup>32</sup> “Suele significar que algún individuo o compañía retiene el derecho de autor exclusivo sobre una pieza de programación y niega a otras personas el acceso al código fuente del programa y el derecho a copiarlo, modificarlo o estudiarlo.” (Maresca, 2007)

<sup>33</sup> Artículo 31.

El derecho de arrendamiento incluido en la literal e) del artículo 21 de la presente ley, no es aplicable a los arrendamientos cuyo objeto esencial no sea el del programa de ordenador en sí.

La colocación en el mercado del original o copias autorizadas de un programa de ordenador, con el consentimiento del titular de los derechos, no extingue el derecho de autorizar el arrendamiento o préstamo de dichos ejemplares, ni cualesquiera otros establecidos en el artículo 21 de esta ley.

Estos programas se protegen y regulan por lo establecido en los tratados internacionales, la LDADC y en los contratos o convenios específicos; inclusive se establece en la legislación nacional obligaciones al Estado como la indicada en el Decreto Número 11-2006 del Congreso de la República (Ley de Implementación del RD-CAFTA), la cual en el artículo 122 establece lo siguiente:

**Artículo 122. Utilización por parte del Estado de programas de Informática y similares.**

Para asegurar que los programas de informática que se empleen con autorización del autor o titular del derecho de autor, los organismos del Estado, así como las entidades descentralizadas y autónomas deberán, en un plazo no mayor de un año a la entrada en vigencia del Tratado de Libre Comercio entre la República Dominicana, Centroamérica, Estados Unidos de América:

- a) Programar en sus proyectos de presupuesto de ingresos y egresos, las partidas que sean necesarias para regularizar el uso lícito de programas de informática y similares, según sea el caso; y
- b) Aprobar, ejecutar y aplicar sus correspondientes disposiciones normativas, que además de establecer los

procedimientos o mecanismos de adquisición licita de dichos programas de informática y similares, regulen las condiciones y políticas de su administración de conformidad con los <sup>(sic)</sup> establecido en la Ley de Derecho de Autor y Derechos Conexos, incluyendo la obligación de contar con un registro o inventario actualizado de los ordenadores y programas utilizados y de las correspondientes licencias, así como de toda medida tendiente a evitar la utilización no autorizada de dichos programas de ordenadores.

Por lo anterior, el Estado y sus órganos deberán realizar y practicar auditorias informáticas en los sistemas informatizados que utilizan para cumplir con lo establecido.

En el caso de los programas de ordenador que no utilizan el sistema propietario clásico utilizaremos como punto de partida el concepto software libre y que ha evolucionado en dos corrientes el free software y el open source software, siendo sus exponentes principales la Free Software Foundation –FSF- <sup>34</sup> (1985) y la Open Source Initiative<sup>35</sup> (1998). En el caso del free software indica la FSF se fundamenta en el trabajo del Proyecto GNU que tenía por objetivo desarrollar un sistema operativo “de modo que nadie tuviera que pagar por

---

<sup>34</sup> La Free Software Foundation (FSF) es una organización con una misión mundial para promover la libertad de usuario de la computadora y para defender los derechos de todos los usuarios de software libre. [www.fsf.org](http://www.fsf.org) En América Latina: [www.fsfla.org](http://www.fsfla.org)

<sup>35</sup> La Open Source Initiative (OSI) es una corporación sin ánimo de lucro creada para educar y abogar por los beneficios del código abierto y construir puentes entre los distintos grupos en la comunidad de código abierto. [www.opensource.org](http://www.opensource.org)

el software y generar una comunidad a partir de él" (Carranza, 2004) considerando que "el código fuente es fundamental para fomentar la informática y que la libre disponibilidad del código fuente es verdaderamente necesaria para que la innovación continúe", (Di Bona, citado por Carranza, 2007) es decir, se busca una libre reproducción, modificación y distribución del programa. La filosofía de la FSF se fundamenta en el principio que el usuario de los programas tiene las libertades siguientes:

"0. la libertad de usar el programa, con cualquier propósito.

1. la libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a tus necesidades.
2. la libertad de distribuir copias del programa, con lo cual puedes ayudar a tu próximo.
3. la libertad de mejorar el programa y hacer públicas esas mejoras a los demás, de modo que toda la comunidad se beneficie." (www.fsfla.org, 2009)

Se conoce a las licencias de esta corriente como licencias públicas de uso general o GNU o GPL General Public License. Posteriormente, surge la corriente open source software (programas de código o fuente abierta) el cual se fundamenta en la accesibilidad al programa o código fuente, así como sus posteriores mejoras y limita las libertades enarboladas por la FSF. Ejemplos de estos tipos de software son Linux, Ubuntu, Fedora, OfficeOpen.

Es importante aclarar que aunque existen programadores que pueden proporcionar el código fuente de su creación se reservan la titularidad de los derechos patrimoniales y limitan su distribución, cambios o mejoras, así como cualquier otra condición en la licencia de uso. Utilizando los principios de la FSF podemos indicar que la libertad 0 está inmersa en la mayoría de tipos de licencia; son las libertades 1, 2 y 3 las que se contraponen al sistema de licenciamiento cerrado o propietario y para que puedan disfrutarse esas libertades es necesario contar con el código fuente y cumplir con las condiciones establecidas por el desarrollador o titular del programa.

Al respecto la LDADC establece:

Artículo 34. Los autores o titulares de un programa de ordenador podrán autorizar las modificaciones necesarias para la correcta utilización de los programas. No constituye modificación la adaptación de un programa realizada por el usuario, para su uso exclusivo, cuando la modificación sea necesaria para la utilización de ese programa o para un mejor aprovechamiento de éste.

Es importante acotar que free software y el open source no debe confundirse con el software gratis porque este último no necesariamente debe ser libre o de código abierto.

Cuando el usuario, utilizando los programas de ordenador, ingresa datos a una computadora a través de un procedimiento técnico por medio de la cual

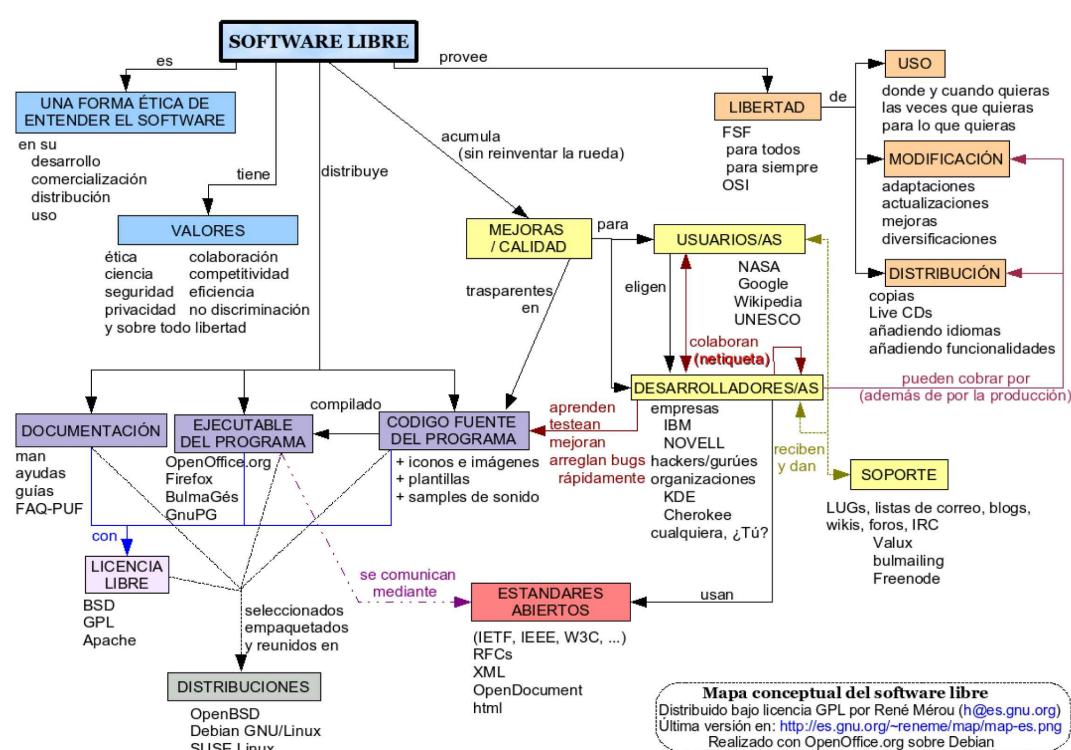
se organizan y clasifican en forma lógica e interrelacionada para que puedan ser consultados posteriormente a través de instrucciones preestablecidas, se crea una base de datos o banco de datos.

Los programas de ordenador que se utilizan en forma común para el desarrollo de los bancos de datos se conocen como Sistemas de Gestión de Bases de Datos, o SGBD (DMS Database Management System por su concepto en inglés). Las bases de datos constituyen un bien distinto al programa de ordenador que la genera; la LDADC establece:

**Artículo 35. Las compilaciones o bases de datos sean que fueren legibles en máquina o cualquier otra**

forma, se consideran como colecciones de obras para efectos de su protección de conformidad con esta ley. Esta protección no se extenderá a los datos o material contenido en las compilaciones ni prejuzgará sobre el derecho de autor existente sobre los mismos.

No debe de confundirse la titularidad sobre las bases de datos con el derecho sobre los propios datos. Un ejemplo lo encontramos en la Ley del Registro Nacional de las Personas, que establece en el artículo 98, “Además, la base de datos que contenga toda la información de las personas naturales, será propiedad exclusiva del RENAP.”



Esquema: Mapa conceptual de software libre ([www.wikipedia.org](http://www.wikipedia.org))

#### 4. Procedimientos para solucionar controversias derivadas de los derechos sobre los programas de ordenador.

Los titulares de los programas de ordenador pueden hacer valer los derechos que emanan de sus creaciones por medio de diferentes procedimientos: en forma directa, procedimientos tecnológicos o ante órganos jurisdiccionales. Los primeros consisten en que los autores, o sus representantes, se pueden comunicar con los sujetos que estén utilizando los programas de ordenador en forma anómala, es decir, sin las autorizaciones legales emitidas por el titular; esa comunicación se realiza por medio de cartas de invitación, circulares, requerimientos directos, todo ello con documentos enviados en formato papel o por correo electrónico. En caso de controversia en los derechos y obligaciones, pueden optar por un procedimiento conciliador, o en su caso, a través del arbitraje. La LDADC en el artículo 133 segundo párrafo establece “No obstante lo dispuesto en este artículo y cualquier otra disposición contenida en la presente ley que dé lugar a acciones civiles o mercantiles, los interesados también podrán utilizar métodos alternativos de resolución de controversias, tales como la conciliación y el arbitraje.”

La segunda forma es una de las más utilizada actualmente por los creadores de los programas de ordenador y consiste en uno o varios procedimientos tecnológicos que tienen por objeto implementar archivos de seguridad de acceso, instalación, validación, entre otros, en el uso del programa; cabe agregar que el proceso de activación en línea del software instalado es uno de ellos, además, actualmente,

cuando se utilizan los programas y se tiene acceso a Internet, se realizan conexiones con la entidad distribuidora del programa la cual envía notificaciones electrónicas al usuario y puede inclusive inactivar el software en forma remota (en línea). El artículo 4 de la LDADC establece la definición de los mecanismos tecnológicos que protegen las creaciones:

**Medida tecnológica efectiva:** Tecnología, dispositivo o componente que en el giro normal de su funcionamiento, controla el acceso a obras protegidas, interpretaciones o ejecuciones y fonogramas protegidos o cualquier otro material protegido; o proteja un derecho de autor o un derecho relacionado con el derecho de autor.

La vía jurisdiccional, es decir, acudir a los tribunales de justicia permite dos opciones: el juicio oral de naturaleza civil, o el proceso penal común. En cuanto la opción que goza el productor de acudir a los juzgados de competencia civil la LDADC establece en el artículo 133 primer párrafo que “Los procesos civiles que se promuevan para hacer valer derechos reconocidos en esta ley se tramitarán de acuerdo con el procedimiento del juicio oral, establecido en el Libro Segundo, Título II, Capítulos I y II del Código Procesal Civil y Mercantil.”

Los conflictos que surgen en el uso de los programas de ordenador pueden llegar a constituir delito como lo establece el Código Penal, en el Artículo 274 “C” que indica “al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación.”; en este caso se podrá acudir

a la vía penal en el proceso penal común y en este caso el ejercicio de la acción penal es de oficio, lo cual establece la LDADC:

**Artículo 127.** Corresponde al Ministerio Público el ejercicio de la acción penal en contra de los responsables de los delitos y faltas tipificados en materia de Derecho de Autor y Derechos Conexos en el Código Penal y otras leyes. El titular o licenciatario de los derechos infringidos podrá provocar la persecución penal denunciando la violación de tales derechos o adherirse a la ya iniciada por el Ministerio Público, entidad que estará obligada a actuar directa e inmediatamente en contra de los responsables. Podrá también instar la persecución penal cualquier asociación u organización representativa de algún sector de la producción o de los consumidores.

**Artículo 128.** El Ministerio Público, de oficio o a solicitud del titular del derecho o el agraviado, al tener conocimiento de un acto ilícito, dentro de los plazos que correspondan según las disposiciones del Código Procesal Penal, deberá requerir al Juez competente que autorice cualesquiera de las providencias cautelares establecidas en esta ley o en el citado Código, que resulten necesarias para salvaguardar los derechos reconocidos y protegidos por esta ley y en los tratados internacionales sobre la materia de los que la República de Guatemala sea parte, y que se estén resultando infringiendo, o cuando su violación

sea inminente. Con este fin, el Ministerio Público juzgará que la solicitud de medidas cautelares será procedente cuando las circunstancias del caso y la evidencia disponible den lugar a la suposición de que se ha producido la infracción o de que existe riesgo de que se produzca.

Presentada la solicitud ante el Juez competente, éste estará obligado a ordenar las medidas cautelares con carácter de urgente de conformidad con las disposiciones procesales aplicables, autorizando al Ministerio Público para que proceda a su ejecución con el auxilio de la autoridad policiaca necesaria.

Es importante establecer que la LDADC establece la oportunidad de poder celebrar un acuerdo entre el agraviado (el productor) y los sujetos sindicados del hecho ilícito cuando se han “resarcido satisfactoriamente del daño ocasionado y se ha pagado, o se ha garantizado debidamente los perjuicios producidos por la comisión del delito, podrá darse por terminado el procedimiento legal iniciado, en cualquier estado del proceso.” (Artículo 128 ter.)

En este punto desarrollamos aspectos específicos para los programas de ordenador, pero con el uso de las TIC se pueden violentar otras creaciones del intelecto humano como música, canciones, poemas, libros, fotografías, entre otros, pero especialmente los datos personales.

## 5. Los datos personales

Establecemos que los datos representan un hecho o significado, pero carecen de algún valor si no se encuentran relacionados con otros, o con una persona. Existen varias clases de datos, pero son los datos personales los que se revisten de una protección jurídica especial derivada del desarrollo de los derechos sobre aspectos inherentes a la persona, como lo son su identidad y su intimidad, y que con el surgimiento de las tecnologías de la información y comunicaciones están cobrando importancia y relevancia para el Derecho, por la facilidad de poder afectar a cualquier sujeto en estos derechos. “El incremento en el uso de las TICs entraña desafíos para la protección de los datos personales. Las redes tecnológicas de entidades públicas y privadas así como la Internet tienen, entre otras, las siguientes características: a) se nutren de datos personales; b) ofrecen innumerables posibilidades para tratar dicha información en poco tiempo y de manera imperceptible a las personas a que se refieren los datos; c) no son tecnologías absolutamente seguras que impidan el acceso a datos personales por parte de personas no autorizadas; d) rompen las fronteras físicas facilitando el flujo internacional de datos personales.” (Remolina, 2007)

Por lo anterior y para limitar el abuso que el Estado puede cometer con las bases de datos de los ciudadanos y personas en general, reviste gran importancia contar con legislación clara y actualizada para la protección de los datos personales, en especial los cometidos por particulares, así como los derivados en la administración de las TIC. Me limitaré a señalar uno de los pronunciamientos más relevantes, contenido

en la Declaración de Principios sobre Libertad de Expresión, de la Comisión Interamericana de Derechos Humanos de la Organización de Estados Americanos que establece que “Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla.” ([www.cidh.oas.org](http://www.cidh.oas.org), 2009) Existen regulaciones de carácter internacional (Comunidad Europea) como el Convenio para la Protección de las Personas en relación con el Tratamiento Automatizado de Datos de Carácter Personal, conocido como Convenio de Estrasburgo (del 28 de enero de 1981) y en especial para el ámbito del presente estudio la Directiva 2002/58/CE del Parlamento Europeo y del Consejo (12 de julio de 2002) relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), las cuales son fuentes de Derecho fundamentales para regular el derecho a la protección de datos personales en la utilización de TIC en Europa, pero proporcionan un antecedente de Derecho comparado para las legislaciones en otras regiones.

En virtud de lo expuesto, es necesario definir los datos personales, la clasificación de los datos así como una breve explicación de los derechos que surgen y la jurisprudencia extranjera y nacional, en especial, porque gran parte del trabajo que realizan los defensores públicos radica en el acceso a los datos personales del imputado al que representan.

### 5.1. Definición de datos personales

Los datos personales son el conjunto de descriptores, hechos o circunstancias que tienen relación con una persona y que proporcionan una idea o representación de ellas; como ejemplo, el nombre, fecha de nacimiento, record crediticio, profesión, religión, afiliación política, entre una amplia variedad de datos. La Ley de Acceso a la Información Pública –LAIP- (Decreto Número 57-2008 del Congreso de la República) define los datos personales en el artículo 9 como “Los relativos a cualquier información concerniente a personas naturales identificadas o identificables.”

Los datos se almacenan en distintos medios físicos, siendo la forma principal las bases de datos electrónicas;<sup>36</sup> los sujetos que almacenan esos datos pueden ser entes públicos o privados. Determinar qué datos pueden estar contenidos en los distintos sistemas hace necesario clasificarlos en datos personales públicos y datos personales privados.

### 5.2. Los datos personales públicos

La información de las personas que se clasifican como datos personales públicos son todos los descriptores que figuran dentro de los registros de carácter público, que no excluyen poder estar en registros privados, que tienen la característica esencial de estar al alcance de todas o la mayoría de personas que deseen consultarlos. Estos datos se encuentran regulados en su recopilación como el caso del Registro

Nacional de las Personas –RENAP- que en la ley de la materia regula que “es la entidad encargada de organizar y mantener el registro único de identificación de las personas naturales, inscribir los hechos y actos relativos a su estado civil, capacidad civil y demás datos de identificación desde su nacimiento hasta la muerte, así como la emisión del Documento Personal de Identificación...” (Artículo 2). Además los entes públicos deberán garantizar la integridad y seguridad de esos datos; el artículo 42 de la Ley del Registro Nacional de las Personales designa esa responsabilidad a la Dirección de Informática y Estadística de proteger la base de datos y “tendrá a su cargo la custodia y elaboración de los respaldos electrónicos, vigilando porque de los mismos se efectúe también un respaldo en un sitio remoto y éste sea realizado en forma simultánea con el ingreso de los datos y su procesamiento en el sitio central del RENAP, velando porque se cumplan las normas y mejores prácticas en materia tecnológica que garanticen su absoluta seguridad (...).”

Ejemplos de datos personales públicos los encontramos en el artículo 56 de la última ley citada que establece entre otros el código único de identificación que se le ha asignado al titular, los nombres y apellidos, el sexo, el lugar y fecha de nacimiento, estado civil, la vecindad y residencia del titular. Además poder indicar los datos de las personas contenidos en otros registros como el Registro General de la Propiedad, el Registro Mercantil, el Sistema de Contrataciones y Adquisiciones

---

<sup>36</sup> La base de datos más importante de Guatemala se encuentra en el Registro Nacional de las Personas. Al respecto establece el Reglamento de Inscripciones del Registro Civil de las Personas:  
Artículo 13. Todos los libros que se lleven en los Registros Civiles, serán electrónicos, los cuales deberán cumplir con los requisitos de uniformidad, inalterabilidad, seguridad, certeza jurídica y de publicidad.

de Guatemala, e inclusive otros de origen privado como las guías telefónicas y comerciales, el directorio de profesionales, siempre y cuando se limiten a publicar los datos de naturaleza pública y no aquellos que puedan afectar la intimidad y privacidad de las personas.

### 5.3. Los datos personales privados

Existen otra clase de hechos o descriptores de las personas que se denominan datos privados y se definen como los “datos personales que tienen reguladas y tasadas las situaciones o circunstancias en que la persona se ve obligada a proporcionarlos, o ponerlos en conocimiento de terceros, siendo la conciencia social favorable a impedir su difusión y respetar la voluntad de secreto sobre ellos de su titular.” (Davara, 2006) Estos datos se subclasifican en datos personales no sensibles y datos personales sensibles.

Los datos personales privados no sensibles son los “que se refieren a un sujeto individualizado y son relativos a su fuero interno o íntimo sin llegar a ser información puramente sensible. Identifican su personalidad, sus creencias e ideologías, sus pensamientos, sentimientos y salud, entre otras cosas. En definitiva, son los relacionados al orden privado de los individuos que los hacen merecedores de una protección más profundizada y específica que los demás tipos de datos generales, debido a que se revelan exclusivamente de forma particular e individual, y rara vez son objeto de tratamiento público.” (Elías, 2001) En el extremo de la privacidad e intimidad de una

persona encontramos los datos personales sensibles los cuales define nuestra legislación como “Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, de origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza.” (Artículo 9, Ley de Acceso a la Información Pública)

Es importante establecer que el almacenamiento de datos públicos y privados conlleva una responsabilidad para el sujeto asignado de su administración y los usuarios con acceso a la información, por ello se deberá contar con todas las medidas protectoras tecnológicas y legales.

Cabe agregar que la naturaleza de los datos personales puede ir variando según cada legislación, estatus de la persona (ejemplo: Personas Políticamente Expuestas), o inclusive, por la tecnología; un ejemplo pueden ser el Sistema Automatizado de Identificación de Huellas Dactilares –SAGEM- (AFIS por sus siglas en inglés Automated Fingerprint Identification System); otros son los datos de localización que se define como “cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;” (Artículo 5, Directiva 2002/58/CE del Parlamento Europeo y del Consejo; 2002) como podría ser una dirección IP o inclusive el Sistema de Posicionamiento

Global (GPS por sus siglas en inglés Global Positioning System) que consiste en un sistema global que permite establecer la ubicación de una persona, vehículo, nave o aeronave, inclusive su transito o ruta, mediante el uso de tecnología satelital con un margen de error de metros hasta centímetros.<sup>37</sup>

## 6. La protección de datos personales; especial referencia a la protección por el uso de TIC

En la doctrina de la materia, en derecho comparado, en la legislación nacional y en la jurisprudencia nacional, encontramos los derechos fundamentales relacionados con la protección de los datos personales, los cuales pueden resumirse en dos: el derecho a la protección de datos o intimidad de las personas, conocido en el derecho anglosajón como "Privacy" (privacidad de los datos); el segundo, el derecho de acceso a los datos personales o habeas data. Estos derechos pueden ser protegidos, y en contrario, vulnerados de múltiples formas, pero por la temática del presente capítulo, nos referiremos solo al uso de las tecnologías.

### 6.1. El derecho a la protección de los datos personales

El derecho fundamental de la protección de los datos personales es un derecho que se encuentra en constante

desarrollo derivado del auge de las bases de datos y de su informatización, incrementado con el uso de las TIC. Se define el derecho fundamental a la protección de datos como el reconocimiento a la facultad de una persona de ejercer control sobre sus datos personales y "la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos." (apde.org; 2009) Se define en doctrina además como el derecho a la intimidad entendido como "la autorrealización del individuo. Es el derecho que toda persona tiene a que permanezcan desconocidos determinados ámbitos de su vida, así como a controlar el conocimiento que terceros tienen de él." (Rebollo, 2008)

Antes de la emisión de la LAIP se emitió jurisprudencia sobre este derecho manifestando la Corte de Constitucionalidad al respecto:

"Los avances de la tecnología informática generan a su vez una dificultad en cuanto a proteger adecuadamente el derecho a la intimidad y a la privacidad de una persona individual. Una solución a esa problemática ha sido la de reconocer el derecho a la autodeterminación informativa del individuo, cuyo goce posibilita a éste un derecho de control sobre todos aquellos datos referidos a su persona y, a su vez, le garantiza la tutela debida ante un uso indebido (es decir, sin su autorización) y con fines de

<sup>37</sup>"El GPS funciona mediante una red de 27 satélites (24 operativos y 3 de respaldo) en órbita sobre el globo, a 20.200 km, con trayectorias sincronizadas para cubrir toda la superficie de la Tierra. Cuando se desea determinar la posición, el receptor que se utiliza para ello localiza automáticamente como mínimo tres satélites de la red, de los que recibe unas señales indicando la posición y el reloj de cada uno de ellos. Con base en estas señales, el aparato sincroniza el reloj del GPS y calcula el retraso de las señales; es decir, la distancia al satélite. Por "triangulación" calcula la posición en que éste se encuentra. La triangulación en el caso del GPS, a diferencia del caso 2-D que consiste en averiguar el ángulo respecto de puntos conocidos, se basa en determinar la distancia de cada satélite respecto al punto de medición. Conocidas las distancias, se determina fácilmente la propia posición relativa respecto a los tres satélites. Conociendo además las coordenadas o posición de cada uno de ellos por la señal que emiten, se obtiene la posición absoluta o coordenadas reales del punto de medición." (Wikipedia.org, 2009)

lucro, por parte de un tercero, de todos aquellos datos personales susceptibles de tratamiento automatizado, con los cuales se integra una información identificable de una persona; información que cuando es transmitida a terceras personas sin los pertinentes controles que permiten determinar su veracidad o actualización, puedan causar afectación del entorno personal, social o profesional de esa persona, causando con ello agravio de sus derechos a la intimidad y al honor.” Expediente Número 1356-2006, sentencia de fecha 11 de octubre de 2006.

En virtud de lo expuesto, el Estado y sobretodo los funcionarios y empleados públicos, deberán establecer los mecanismos técnicos y legales para la protección de los datos de las personas en las bases de datos que administren, lo relativo al consentimiento de los sujetos en proporcionar la información<sup>38</sup> y en especial, el derecho de acceso, siendo conocido como habeas data.

## 6.2. El Habeas Data

La autodeterminación informativa no solo consiste en la manifestación del consentimiento para proporcionar los datos, se complementa con el derecho de conocer la información propia en poder de entes estatales (e inclusive privados), información de uno mismo, es decir la existencia de los datos personales en las bases de datos o ficheros, pero además, cobra relevancia establecer el origen de esa data y sobretodo, la finalidad por la cual se conserva. El derecho de acceso a los datos personales es fundamental para poder hacer valer otros derivados de él como el derecho de rectificación, el derecho de cancelación y el derecho de oposición. La LAIP en el artículo 9 define este derecho así:

4. Habeas data: Es la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación

<sup>38</sup> La LAIP estable en el Título Primero, Capítulo Sexto lo siguiente:

Artículo 31. Consentimiento expreso. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciere referencia la información. El Estado vigilará que en caso de que se otorgue el consentimiento expreso, no se incurra en ningún momento en vicio de la voluntad en perjuicio del gobernado, explicándole claramente las consecuencias de sus actos.

Queda expresamente prohibida la comercialización por cualquier medio de datos sensibles o datos personales sensibles.

Artículo 32. Excepción del consentimiento. No se requerirá el consentimiento del titular de la información para proporcionar los datos personales en los siguientes casos:

1. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
2. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades del Estado, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
3. Cuando exista una orden judicial;
4. Los establecidos en esta ley;
5. Los contenidos en los registros públicos;
6. En los demás casos que establezcan las leyes.

En ningún caso se podrán crear bancos de datos o archivos con datos sensibles o datos personales sensibles, salvo que sean utilizados para el servicio y atención propia de la institución.

o actualización. Los datos impersonales no identificables, como aquellos de carácter demográfico recolectados para mantener estadísticas, no se sujetan al régimen de hábeas data o protección de datos personales de la presente ley.

Es importante establecer que sola la persona titular de los datos o en su caso su representante, puede tener acceso a los ellos; la LAIP define como sujeto activo “a toda persona individual o jurídica, pública o privada, que tiene derecho a solicitar, tener acceso y obtener la información pública que hubiere solicitado conforme lo establecido en esta ley. (Artículo 5); la limitación establecida al inicio de este párrafo se establece en el Artículo 33 de la ley al indicar que “Sin perjuicio de lo que dispongan otras leyes, sólo los titulares de la información o sus representantes legales podrán solicitarla, previa acreditación, que se les proporcione los datos personales que estén contenidos en sus archivos o sistema de información...” (Acceso a los datos personales). Además el último párrafo del artículo 30 establece una obligación para los sujetos activos al indicar que “no podrán usar la información obtenida para fines comerciales, salvo autorización expresa del titular de la información.”

En cuanto a las personas que administran las bases de datos denominados como sujetos obligados, como responsables de la data de las personas deberán cumplir con: 1. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos que sean presentados por los titulares de los mismos o sus representantes legales, así como capacitar a los servidores públicos y dar a conocer

información sobre sus políticas en relación con la protección de tales datos; 2. Administrar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido; 3. Poner a disposición de la persona individual, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento; 4. Procurar que los datos personales sean exactos y actualizados; 5. Adoptar las medidas necesarias que garanticen la seguridad, y en su caso confidencia o reserva de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado. (LAIP, Artículo 30)

### 6.3. Riesgos tecnológicos para la protección de los datos personales

Existe un sinfín de riesgos para los datos de las personas, que van desde el desconocimiento de las garantías y derechos, hasta una deficiente administración de las bases de datos; pero el riesgo es mayor con el uso de las tecnologías de la información y comunicaciones, en especial la accesibilidad a insumos de almacenamiento y captación de datos. Los empleadores, desde el Estado hasta la iniciativa privada, realizan compilaciones de datos de las personas desde formularios de solicitud de empleos, administración de la planilla laboral con los descuentos correspondientes, como las cuotas de seguridad social o la cuota sindical, declaraciones de seguros, plan de prestaciones, nombres de beneficiarios y condiciones de los mismos, expediente médico o historiales clínicos de los trabajadores, controles laborales mediante

el uso de tecnología, información de los trabajadores en circulares o memorándum, hasta administración de cuentas de correo electrónico y navegadores, información en el sitio web de la empresa, desplegado de mensajes de texto y grabación de llamadas telefónicas. Haremos especial referencia en este punto a la tecnovigilancia y el uso de los correos electrónicos.

### 6.3.1. La tecnovigilancia

Cobra relevancia en los datos indicados anteriormente la denominada tecnovigilancia entendida “no solo desde el plano físico de observación y control directo de los movimientos de la persona, lugar o cosa objeto de control de sus actividades, sino que la entendemos abarcando todo tipo de control telemático de la actividad personal del individuo o de cuanto sucede en un espacio, lugar u objeto, referido siempre a un momento determinado y sirviéndose para ello de algún instrumento de base científica.” (Llamas y Gordillo, 2007)

Cada día vemos que los entes públicos, empresas y personas individuales invierten en sistemas electrónicos de seguridad que incluyen controles de ingreso en locales, residenciales, edificios privados y públicos, en especial cámaras de seguridad que fotografían, o en su caso, filman (video y en algunos casos audio) el ingreso del sujeto, registro del documento de identificación desde un apunte en hojas de control, hasta escanear el documento y almacenarlo en orden de ingreso, y otros, como la asignación de una tarjeta electrónica de ingreso; es importante recordar que todos estos sistemas guardan desde datos personales de los sujetos hasta los registros de fecha y hora de ingreso y egreso, y que esa base de datos no se encuentra protegida o con normas de seguridad que garanticen

al usuario la confidencialidad, convirtiéndose, aunque ese no sea su fin, en violaciones a la protección de datos personales y por supuesto, riesgos para las personas. No existe en Guatemala regulación específica para estas situaciones, caso contrario de la Comunidad Europea que cuenta con la Instrucción Número 1/1996, de 1 de marzo de 1996, de la agencia de protección de datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios, que establece:

#### Ámbito de aplicación

1. La presente Instrucción regula los datos de carácter personal tratados de forma automatizada que son recabados por los servicios de seguridad con la finalidad de controlar el acceso a los edificios públicos y privados, así como a establecimientos, espectáculos, certámenes y convenciones.
2. A tales efectos, tendrá la consideración de dato personal cualquier información concerniente a personas físicas identificadas o identificables, debiendo entenderse comprendidos dentro de la misma el sonido y la imagen. (2009)

Las situaciones anteriores se dan además, en los sistemas informáticos disponibles para las personas en sus centros de trabajo, recreación, e inclusive domiciliarios. La Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas DSPCE) Número 2002/58/CE del Parlamento Europeo y del Consejo, nos da un ejemplo de la importancia de esta data estableciendo que:

### 6.3.2. Los correos electrónicos y su responsabilidad

Caso muy particular lo constituyen el uso y la administración de los correos electrónicos; partiremos de explicar esta aplicación utilizando la definición legal que proporciona la DSPCE en el artículo 2, al indicar que correo electrónico es “todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo.” La Constitución Política de la República de Guatemala (1986) había considerado la necesidad de proteger las comunicaciones de las personas así como su intimidad, por lo cual en el Artículo 24 hace referencia a “otros productos de la tecnología moderna”; el artículo referido establece:

**ARTICULO 24.** Inviolabilidad de correspondencia, documentos y libros. La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.

Por lo anterior, podemos establecer que para poder acceder a la cuenta personal de correo electrónico de un sujeto, se debe contar con la autorización del titular, o en su caso, una orden judicial. Es importante recordar que los correos electrónicos no se

almacenan solo en la cuenta del destinatario, sino en el servidor del proveedor del servicio, e inclusive, en la cuenta del propio remitente; además la mayoría de servidores cuentan con copia de seguridad (backup) de la información almacenada. Caso aparte lo constituyen las cuentas de correo electrónico asignadas por el patrono para uso de los trabajadores cuando se establezcan por un procedimiento legal como una herramienta de trabajo. Al respecto trasladamos fallos de derecho extranjero como un ejemplo:

“La posibilidad de efectuar registros en las terminales del ordenador de los trabajadores no es un derecho absoluto e incondicionado de la empresa, pues el art. 18 ET 1995 lo condiciona a que ello sea necesario para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, cosa que la demanda ni siquiera adujo causa o motivo alguno para la realización del registro en cuestión. Por ello, dicho registro violó el derecho a la intimidad del trabajador, garantizada en el plano estrictamente laboral por el art. 4.2 e) ET 1995 y con carácter general en el art. 10 CE.” (Tribunal Superior de Justicia de Andalucía, Sala de lo Social de Málaga; S 25/02/2000)

Cabe agregar que los trabajadores también están en la obligación de utilizar el correo electrónico de la empresa, así como los demás servicios tecnológicos, para el destino correcto o servicios que está obligado a prestar; en ese aspecto, encontramos algunos fallos que se han dado en el extranjero:

“Por lo tanto, el envío de mensajes por parte del trabajador, en horario laboral a través del correo electrónico que tiene asignado en la empresa, ajenos a las prestación de servicios supone una clara transgresión de la buena fe contractual y deber de lealtad laboral que justifica el despido en base a lo dispuesto en el art. 54.2. d) ET. (Tribunal Superior de Justicia de Cataluña, Sala de lo Social; S 14/11/2000)

La cuenta de correo electrónico de los usuarios se ve afectada también por terceros, siendo el caso más común el denominado spam o correo no deseado que puede definirse en forma básica como el mensaje o conjunto de mensajes recibidos por el destinatario, que no fueron solicitados y que se han enviado en forma masiva afectando su privacidad. Es complejo poder definir qué es spam y cuando no se considera como tal; al respecto el Dr. Daniel Oliver explica que “cabe diferenciar cuatro tipos básicos de envíos electrónicos masivos y no solicitados. En primer lugar, los mensajes que remite una empresa identificada para promocionar sus productos o servicios. A ellos me referiré con la expresión neutral de correo comercial no solicitado (UCE: unsolicited commercial e-mail). El segundo y el tercer grupo lo integran, respectivamente, los mensajes comerciales que podríamos calificar de sospechosos, por cuanto el remitente del envío publicitario camufla de alguna manera su identidad, y los mensajes estériles, que a priori no tienen una finalidad comercial, como las cadenas de mensajes sobre la fortuna y la felicidad personal, así como otras burlas o engaños (hoax). Reservaré para estos dos grupos la calificación de

correo basura (junk mail). Finalmente, existe variedad y diferencia de mensajes maliciosos, como aquellos que solicitan al destinatario datos personales o bancarios suplantando la identidad de empresas conocidas (phising), los dirigidos a colapsar un servidor (mail bombing) o inclusive los que generan los virus informáticos para reproducirse.” (2007)

En el caso de la primera clase de correos electrónicos, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas en el último párrafo del artículo 51 establece que “Las empresas deben desarrollar e implementar procedimientos efectivos y fáciles de usar, que permitan a los consumidores manifestar su decisión de recibir o rehusar mensajes comerciales no solicitados por medio del correo electrónico. Cuando los consumidores manifiesten que no desean recibir mensajes comerciales por correo electrónico, tal decisión debe ser respetada.” Para la segunda y tercera clase de correos electrónicos denominados correos basura existen herramientas informáticas que los bloquean o los dirigen a la carpeta de “correos no deseados”. Son los correos de la cuarta clasificación los que los usuarios deben tratar con más cuidado, así como las empresas afectadas; un ejemplo de ello ha sucedido en los bancos nacionales cuando los usuarios han recibido mensajes solicitando actualizar sus datos ingresando su usuario y password, lo que tiene consecuencias en la privacidad de la persona, y por supuesto, en su patrimonio.

Algunos aspectos a considerar en el ejercicio profesional es el procedimiento de ofrecimiento, proposición y diligenciamiento de los correos electrónicos como medios

de prueba, diferenciando presentar el contenido del correo electrónico, o en su caso, los archivos que se adjuntan; no existe duda del medio de prueba correspondiente para presentar los correos electrónicos en virtud que son “Documentos Admisibles” según el artículo 178 del Código Procesal Civil y Mercantil para las materias en que se aplica esta normativa procesal, , pero es importante señalar que la norma citada anteriormente indica en el segundo párrafo que “No serán admitidas como medio de prueba las cartas dirigidas a terceros, salvo en materia relativa al estado civil de las personas, ejecución colectiva y en procesos de o contra el Estado, las municipalidades o entidades autónomas o descentralizadas.”

En materia penal, deben considerarse varios aspectos, pero fundamentalmente dos situaciones; que el agraviado posea el correo electrónico que le fue remitido por el imputado, o que sea necesario sujetar a secuestro ese correo. Al respecto, el Código Procesal Penal establece en el artículo 203 que “Cuando sea de utilidad para la averiguación, se podrá ordenar la interceptación y el secuestro de la correspondencia postal, telegráfica o teletipográfica y los envíos dirigidos al imputado o remitidos por él, aunque sea bajo un nombre supuesto, o de los que se sospeche que proceden del imputado o son destinados a él.

La orden será expedida por el juez ante quien penda el procedimiento o por el presidente, si se tratare de un tribunal

colegiado. La decisión será fundada y firme.”<sup>39</sup>

Es importante considerar que puede llegar a existir responsabilidad en el reenvío de los correos electrónicos al poder incurrir en faltas administrativas, laborales o hasta de índole penal, cuando su contenido está sujeto a reserva del usuario del sistema informático, o en su caso, en los abogados y abogadas de faltas a la confianza y sigilo profesional con el cliente o usuario.

En casos penales, encontramos como ejemplo, el delito de pánico financiero contenido en el artículo 342 “B” del Código Penal que establece “quien elabora, divulgue o reproduzca por cualquier medio o sistema de comunicación, información falsa o inexacta que menoscabe la confianza de los clientes, usuarios, depositantes o inversionistas de una institución sujeta a la vigilancia e inspección de la Superintendencia de Bancos...” En el caso de los envíos masivos de correos electrónicos conocidos como Spam nuestra legislación nacional no lo contempla como delito, pero existen iniciativas de ley al respecto.

Por medio de las actuales tecnologías también se vulneran los derechos de los usuarios y consumidores mediante otros procedimientos informáticos como los virus, las cookies, el spyware, malware, pop-ups, inclusive se están dando estos tipos de afectaciones en los teléfonos móviles o celulares de las personas; el

<sup>39</sup> Es importante tener presente que cuando se ofrecen medios de investigación o de prueba debe cumplirse con el principio de legalidad en la obtención de los mismos; el Código Procesal Penal establece que “Un medio de prueba, para ser admitido, debe referirse directa o indirectamente, al objeto de la averiguación y ser útil para el descubrimiento de la verdad... Son inadmisibles, en especial, los elementos de prueba obtenidos por un medio prohibido, tales como la tortura, la indebida intrusión en la intimidad del domicilio o residencia, la correspondencia, las comunicaciones, los papeles y los archivos privados.” (Artículo 183)

desconocimiento técnico sobre cómo prevenir o contrarrestar estas situaciones, así como la falta de una regulación legal al respecto, permiten que se sigan afectando los derechos de los usuarios informáticos.

## 7. Aplicación de la Ley de Acceso a la Información Pública en el ámbito informático

Una de las iniciativas o proyecto de ley que dieron base a la vigente Ley de Acceso a la Información Pública establecía, que “El presente proyecto regula tres aspectos: el derecho de acceso a la información pública, el derecho de acceso a datos personales obrantes en archivos estatales y el derecho de acceso de datos personales obrantes en archivos privados” (Iniciativa No. 3165, de fecha 3 de noviembre de 2004 y presentada al Congreso de la República el 11 de noviembre de 2004). En el caso de Guatemala, se dio una situación especial al regular en un solo decreto lo que en otros países son dos leyes independientes; por una lado, las leyes de acceso a la información pública que tienen por objeto la transparencia y publicidad de los actos administrativos y de gobierno como el caso de Colombia, Chile, Panamá, Ecuador, entre otros, y por el otro, las leyes de protección de datos personales que en esencia protegen el derecho a la intimidad, privacidad o autodeterminación de los datos, como es el caso de Chile, Argentina, España. Considero que regular dos ámbitos en una sola ley creó confusión en las personas y quedó muy limitado el derecho de acceso en archivos privados, quedando prácticamente la ley nacional para el acceso a información pública y el derecho de acceso a datos personales, pero en archivos públicos.

Una de las diferencias fundamentales de estos dos derechos es en cuanto a la propia información, en virtud que en el derecho de acceso a la información pública se accede a actos administrativos y de gobierno, mientras en el derecho de acceso a datos personales, solo se puede acceder a los datos con relación al solicitante (titular de los datos). La LAIP define en el artículo 9 el Derecho de acceso a la información pública como el “El derecho que tiene toda persona para tener acceso a la información generada, administrada o en poder de los sujetos obligados descritos en la presente ley, en los términos y condiciones de la misma.”; el principio constitucional establece:

Artículo 30.- Publicidad de los actos administrativos. Todos los actos de la administración son públicos. Los interesados tienen derecho a obtener, en cualquier tiempo, informes, copias, reproducciones y certificaciones que soliciten y la exhibición de los expedientes que deseen consultar, salvo que se trate de asuntos militares o diplomáticos de seguridad nacional, o de datos suministrados por particulares bajo garantía de confidencialidad. (Constitución Política de la República de Guatemala)

A diferencia del acceso a la información pública, el Habeas Data se constituye como “la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización.”

(LAIP, Artículo 9). El principio constitucional indica:

Artículo 31.- Acceso a archivos y registros estatales. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos. (Constitución Política de la República de Guatemala)

La Corte de Constitucionalidad había establecido la diferencia entre los dos derechos, al manifestarse en el Expediente Número 684-2006, sentencia de fecha veintinueve de noviembre de dos mil seis:

“Las nuevas tendencias doctrinarias hacen una distinción entre dos elementos o conceptos que integran el derecho a la información, siendo éstos, la “libertad informática” y la “auto determinación informativa”. La libertad informática consiste, básicamente, en la posibilidad de acceder a las fuentes de información, a los registros y archivos de dominio público y en fin a cualquier otro banco de datos; por otro lado, la auto determinación informativa hace alusión al derecho de toda persona de acceder, rectificar y complementar la información que de ella conste en los distintos archivos existentes, a la confidencialidad y exclusión de la misma.”

En el expediente relacionado, el Tribunal Constitucional de Guatemala estableció el ámbito de los actos administrativos y de gobierno indicando:

“De conformidad con el artículo 30 precitado, todos los actos de la administración son públicos y los interesados tienen derecho, entre otras cosas, a que se les exhiban los expedientes que deseen consultar. No obstante lo anterior, dicha norma no determina puntualmente qué se debe entender por actos de administración, qué implica el principio de publicidad de los mismos, ni quiénes son o deben ser considerados como interesados en los expedientes relacionados, de ahí que para determinar la posible violación de dicha norma resulte imperioso, como cuestión preliminar, determinar dichas circunstancias. En términos generales, se ha considerado como actos propios de la administración aquellos realizados por autoridades de naturaleza administrativa, es decir, autoridades o funcionarios del gobierno central, del Organismo Ejecutivo. Dicha afirmación no encuentra un sustento debido en la norma indicada, ya que la acepción “actos de la administración” se refiere tanto a la administración de la cosa pública como a la administración de justicia, de ahí que en un sentido netamente garantista y acorde al espíritu de la norma, debe considerarse que el principio de publicidad y el derecho de acceso a la información, establecidos en el precepto objeto de estudio, abarcan la totalidad de

las actuaciones del aparato estatal, con excepción, claro esta, de los asuntos militares o diplomáticos de seguridad nacional y de aquellos datos suministrados bajo garantía de confidencialidad.

Respecto al principio de publicidad, el Tribunal Constitucional Español ha indicado que el mismo tiene una doble finalidad: por un lado, proteger a las partes de una justicia sustraída al control público, y por otro, mantener la confianza de la comunidad en los Tribunales, constituyendo en ambos sentidos tal principio una de las bases del debido proceso y una de los pilares del Estado de Derecho. De conformidad con dicho Tribunal, el referido principio exige que las actuaciones judiciales puedan llegar a ser presenciadas por cualquier ciudadano mientras se disponga de espacio, por lo que será necesario en todo caso habilitar un espacio razonable; en segundo lugar, implica que los procesos sean conocidos más allá del círculo de los presentes en los mismos.” Expediente Número 684-2006, sentencia de fecha veintinueve de noviembre de dos mil seis.

Como establecimos, el derecho de habeas data se encuentra limitado en los archivos que administran entes privados en virtud que la Ley de Acceso a la Información Pública estableció que constará “en archivos, fichas, registros o cualquier otra forma de registros públicos”, siendo el debate si “públicos” deviene de ser un ente estatal o

que es de acceso libre a las personas aún estando administrado por un sujeto no estatal. La Constitución Política de la República de Guatemala establece como principio en el primer y segundo párrafo del artículo 44:

**ARTICULO 44. Derechos inherentes a la persona humana.**  
Los derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana.

El interés social prevalece sobre el interés particular.

Se establece en La Declaración Universal de Derechos Humanos en el Artículo 12 que “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.” Además debe de considerarse lo indicado en el Artículo 11 de la Convención Americana sobre Derechos Humanos, en el Pacto Internacional de Derechos Civiles y Políticos artículo 17, en la Declaración Americana de los Derechos y Deberes del Hombre artículo V, en especial el artículo 3 de la Declaración de Principios sobre Libertad de Expresión de la Comisión Interamericana de Derechos Humanos relacionado en esta unidad. Una de las iniciativas de ley base para la LAIP indica que “Dada su naturaleza y en armonía con la norma del artículo 31 de la Constitución Política de la República, el proyecto establece que no hay excepciones al derecho de las personas a acceder a sus datos personales propios obrantes en

archivos estatales y privados.” (Exposición de motivos, Ley de Acceso a la Información Pública)

En el caso del ejercicio profesional de los abogados, nuestra experiencia establece que muchas veces la administración pública nos limita la información relativa a nuestros defendidos; por lo anterior es necesario estudiar la jurisprudencia contenida en los fallos de la Corte de Constitucionalidad acerca de la actividad legal:

“Con relación a la determinación de quienes pueden ser consideradas como personas con interés en las actuaciones públicas, debido a lo amplio y complejo del tema no puede hacerse una argumentación generalizada que permita determinar, con certeza en cada caso en particular, quienes pueden tener interés o no en los actos de la administración pública, debido a lo riesgoso que resultaría emitir un pronunciamiento tan temerario sin poder contar con todos los elementos que permitan tener un panorama más amplio de cada una de las circunstancias que podrían suscitarse. En el caso objeto de estudio, es necesario determinar si el accionante, en su calidad de abogado litigante, posee los elementos necesarios para ser considerado como “una persona con interés”.

Los profesionales del Derecho, concretamente los abogados, tienen encomendada la importante misión de asesorar legalmente a las

personas, de defender los intereses y las posturas de aquellas que se ven involucradas en procesos legales; en cumplimiento y ejercicio de tal función, los abogados participan y se involucran en los distintos procesos legales, no motivados por un interés personal, sino atendiendo el requerimiento de su cliente. Por ello, para garantizar su adecuada actuación, es indispensable indicar que cuando tales profesionales requieran la exhibición de actos propios de la administración pública, o la consulta de actuaciones dentro de los distintos procesos jurisdiccionales, se presumirá que dicha actitud se verifica como parte de su labor profesional, a requerimiento de alguna persona que tiene algún interés en el asunto y que, eventualmente, puede llegar a ser auxiliado por el referido letrado; de ahí que en atención a dicha presunción, no puede ni debe restringirse de forma alguna el acceso de los abogados a los procesos judiciales, pues de lo contrario se estaría ante una eventual vulneración del derecho de libre acceso a los tribunales de justicia. Dicha tesis se ve reforzada con el contenido del artículo 198 de la Ley del Organismo Judicial, el cual dispone, con relación a los derechos de tales profesionales, que: “...ni se coartará directa ni indirectamente el libre desempeño de su alta investidura e igual trato deberán darles las autoridades, funcionarios y empleados de la Administración Pública de cualquier jerarquía. Los

tribunales darán a los abogados el trato respetuoso inherente a su investidura.” Expediente Número 684-2006, sentencia de fecha veintinueve de noviembre de dos mil seis.

Es importante resaltar que cuando la Corte de Constitucional se pronuncia por medio del fallo relacionado no se había emitido la vigente LAIP, pero la jurisprudencia establecida no es contradicha en ninguna norma de la ley indicada.





## EJERCICIOS DE AUTOAPRENDIZAJE

1. Analice los aspectos legales del siguiente párrafo:

La persona se sienta en su escritorio y se volteá hacia su computadora personal; pulsando el botón de encendido empieza el “arranque” del computador y una versión de Windows, sistema operativo de Microsoft, inicia su aparición; posteriormente da un click y se muestra un procesador de texto, Word de Microsoft, el cual utiliza para realizar una investigación de sus estudios universitarios; activa su navegador e ingresa a un sitio web, donde encuentra un artículo de su interés además de fotografías por lo cual en el menú edición selecciona copiar y posteriormente en su documento pulsa pegar (“copy-paste”); visita otro sitio y encuentra varias de sus canciones favoritas y las “descarga” en su computadora para poderlas grabarlas en un CD y entregárselas a su pareja como regalo de cumpleaños.

2. Elabore un pequeño documento en un procesador de texto de un programa propietario y en un procesador de texto en un programa libre. Indique sus observaciones, diferencias, similitudes y sobretodo realice un análisis de costo y legal.
3. Elabore un listado de datos personales que le proporciona el imputado a usted en su calidad de abogado defensor. A la par de esa columna de datos, establezca si son datos públicos, privados no sensibles, o privados sensibles; en la siguiente columna establezca en qué registros pueden encontrarse esos datos; en la cuarta columna indique en qué clase de documento o certificación se pueden obtener de forma legal esos datos. Un ejemplo del listado de datos personales lo puede encontrar en el artículo 82 del Código Procesal Penal, pero existen otra serie de datos personales a los cuales usted tiene acceso que pueden ir desde el monto del salario de su representado hasta el expediente clínico del mismo.
4. El imputado cuenta con un correo electrónico que recibió del querellante adhesivo, el cual contiene información que sirve de descargo en su defensa. ¿Cuál es el procedimiento para incorporarlo a la investigación, o en su caso, cómo ofrecerlo como medio de prueba?

5. Establezca los aspectos técnicos y legales que deben verificarse en el momento de incorporar como medio de investigación y en su caso de prueba, una videograbación de un sistema de cámaras de seguridad.
6. Verifique en el sitio web del Congreso de la República las iniciativas de ley existentes en materia de Protección de Datos y realice un breve análisis de derecho comparado con algunas de las leyes vigentes en América o España.

## CAPÍTULO

# 4

### LOS DOCUMENTOS Y LAS FIRMAS ELECTRÓNICAS

El documento electrónico ha sido admitido por la sociedad, desde hace tiempo, como un medio por el que comunicarse, guardar información o realizar y confirmar transacciones, entre otros. Sin embargo, toda la confianza depositada en el documento electrónico, fundamental para la realización del comercio “on line”, podría tambalearse si dichos documentos electrónicos carecieran de valor probatorio ante los tribunales o ante cualquier otro organismo que resuelva conflictos extrajudicialmente.

Tengamos en cuenta, por ejemplo, la importancia del reconocimiento de un contrato o de la entrega de una factura facilitada “on line” y por medios electrónicos. Será, por tanto, la eficacia probatoria de los documentos electrónicos la piedra angular sobre la que descance la implantación del comercio electrónico, para el que es vital que las transacciones económicas realizadas “on line” tengan un reconocimiento judicial, sin perjuicio de que también tenga una gran relevancia en otros ámbitos distintos de este tipo de comercio.

José Cervelló



## CONTENIDO DEL CAPÍTULO

Las actividades que realizan las personas se benefician del crecimiento de aplicaciones informáticas, y los actos o comunicaciones que realizan antes en documentos en soporte papel, los realizan ahora en soporte electrónico.

La administración pública también se ha dado a la tarea de aprovechar las nuevas tecnologías para desarrollar procesos de automatización e informatización de sus procedimientos, logrando mejor desempeño en sus objetivos o finalidades. Desde una circular de convocatoria a una reunión de trabajo hasta discutir o celebrar pequeños o grandes negocios, los usuarios de las tecnologías de la información y comunicaciones necesitan dejar plasmados los actos lo cual realizarán en documentos de fácil acceso en cuanto a tiempo, lugar, distancia, idiomas, etcétera.

Los negocios electrónicos o los procedimientos administrativos en su caso, necesitan por la índole del medio donde se celebran de documentos electrónicos y cuando éstos incluyan características muy especiales como la aceptación de obligaciones o manifestación de voluntad llenar y cumplir con requisitos establecidos por la legislación, se convertirán en contratos electrónicos o actos administrativos. Pero, ¿Cómo manifestamos la voluntad en el ciberespacio? ¿Qué validez tendrán esos hechos digitales en un proceso? Existen respuestas otorgadas por la doctrina y la ley pero aún tenemos duda de los criterios jurisdiccionales que se emitirán oportunamente, por ello los defensores públicos deben de llevar un paso adelante, para poder orientar a los sujetos procesales en la legalidad y legitimidad de las acciones, pero en especial deben guiar al órgano jurisdiccional.





## Objetivos Específicos

- a) Distinguir los elementos tecnológicos y legales para la documentación electrónica.
- b) Proporcionar la base legal y técnica para la manifestación de voluntad por medios informáticos.
- c) Definirá que es un documento electrónico.
- d) Destacar los aspectos relevantes de la Ley del Reconocimiento de Comunicaciones y Firmas Electrónicas.



## LOS DOCUMENTOS Y LAS FIRMAS ELECTRÓNICAS

### 1. El comercio electrónico y el gobierno electrónico

Las actividades que realizan las personas utilizando las plataformas electrónicas pueden consistir en operaciones administrativas y contables de carácter interno (usuario-usuario), de relación entre empresas o con proveedores, crediticias o financieras (usuario-banco), e inclusive, con órganos administrativos del Estado (Contribuyentes-Superintendencia de Administración Tributaria). Todos estos actos han pasado de un procedimiento manual a un procedimiento informatizado; al acto de digitalizar los procedimientos y su incorporación a plataformas de comunicación electrónicas se les denomina comúnmente e-business (negocios electrónicos); cuando esa comunicación digital es entre personas se utiliza el concepto comercio electrónico y cuando participa brindando el servicio público un ente estatal se utiliza el concepto gobierno electrónico.

#### 1.1. El comercio electrónico

La Asociación de Usuarios de Internet de España define al Comercio Electrónico como “Cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación.” (2000) La Ley de Reconocimiento de Comunicaciones y

Firmas Electrónicas de Guatemala establece que se entenderá por Comercio Electrónico “las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de una o más comunicaciones electrónicas o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, incluyendo el factoraje y arrendamiento de bienes de equipo con opción a compra; de construcción de obras: de consultoría: de ingeniería: de concesión de licencias: de inversión: de financiación; de banca; de seguros; de todo acuerdo de concesión o explotación de un servicio público: de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.” (Artículo 2)

Se utilizan distintos términos para identificar las actividades como e-commerce, electronic commerce, comercio digital, e-commerce o CE. Cuando una persona adquiere un bien o servicio por medio de la plataforma web que brinda Internet está utilizando tan solo uno de los más visibles ejemplos del comercio electrónico ([www.cemaco.com](http://www.cemaco.com)), pero las subastas ([www.mercadolibre.com](http://www.mercadolibre.com)), la publicidad (Google AdWords), los catálogos y clasificados electrónicos ([www.prensalibre.com.gt](http://www.prensalibre.com.gt), [www.mundoanuncio.com.gt](http://www.mundoanuncio.com.gt)), son una muestra más de las actividades comerciales vía Internet, e inclusive, fases necesarias para la denominada compra electrónica.

Las actividades descritas son conocidas como B2B (Business to Consumer) que significa “Negocio a Consumidor”, aunque actualmente también se describen otras formas como B2B (Business to Business) negocio a negocio, C2C (Consumer to Consumer) consumidor a consumidor o comercio entre particulares y G2C (Government to Consumer) gobierno a consumidor.

En materia de comercio electrónico, las empresas deberán cumplir con las normativas nacionales y en su caso internacionales, así como con la Ley de Protección al Consumidor (Decreto Número 6-2003 del Congreso de la República); es importante resaltar regulaciones para la prestación de servicios por medio de Internet, las cuales establece la Ley para el Reconocimiento de Comunicaciones y Firmas Electrónicas en el artículo 51, al indicar la “Prevalencia de las leyes de protección al consumidor. La presente Ley se aplicará sin perjuicio de las normas vigentes en materia de protección al consumidor. Las entidades o empresas involucradas en el comercio electrónico deben respetar los intereses de los consumidores y actuar de acuerdo a prácticas equitativas en el ejercicio de sus actividades empresariales, publicitarias y de mercadotecnia. Así mismo, las entidades o empresas no deben realizar ninguna declaración, incurrir en alguna omisión, o comprometerse en alguna práctica que resulte falsa, engañosa, fraudulenta o desleal.” Cabe agregar que los entes que ofrecen sus servicios o mercancías por medio de Internet deberán cumplir con lo establecido en la ley citada, la cual indica en otra de sus normas:

**Artículo 52. Información el Línea.**  
Sin perjuicio de cumplir con la legislación vigente para comerciantes y empresas mercantiles, las empresas que realicen comercio electrónico deberán proveer la siguiente información:

- a) información sobre la empresa:  
Las empresas que realicen transacciones con los consumidores por medio del comercio electrónico deben proporcionar de manera precisa, clara y fácilmente accesible, información suficiente sobre ellas mismas, que permita al menos:
  1. La identificación de la empresa – incluyendo la denominación legal y el nombre o marca de comercialización; el principal domicilio geográfico de la empresa; correo electrónico u otros medios electrónicos de contacto, o el número telefónico; y, cuando sea aplicable, una dirección para propósitos de registro, y cualquier número relevante de licencia o registro gubernamental;
  2. Una comunicación rápida, fácil y efectiva con la empresa;
  3. Apropriados y efectivos mecanismos de solución de disputas;
  4. Servicios de atención a procedimientos legales; y,
  5. Ubicación del domicilio legal de la empresa y de sus directivos, para uso de las autoridades encargadas de la reglamentación y de la aplicación de la ley.

Cuando una empresa de a conocer su membresía o afiliación en algún esquema relevante de autorregulación, asociación empresarial, organización para resolución de disputas u otro organismo de certificación, debe proporcionar a los consumidores un método sencillo para verificar dicha información, así como detalles apropiados para contactar con dichos organismos, y en su caso, tener acceso a los códigos y prácticas relevantes aplicados por el organismo de certificación.

- b) Información sobre los bienes o servicios: Las empresas que realicen transacciones con consumidores por medio del comercio electrónico deben proporcionar información precisa y fácilmente accesible que describa los bienes o servicios ofrecidos, de manera que permita a los consumidores tomar una decisión informada antes de participar en la transacción y en términos que les permita mantener un adecuado registro de dicha información.

## 1.2. El gobierno electrónico

El G2C, gobierno electrónico o e-government por su término en inglés, se define como el conjunto de actividades y servicios públicos que prestan los entes del Estado a través del uso de Tecnologías de la Información y Comunicaciones con el objeto de optimizar los servicios o

procedimientos por medios digitales. En algunos países, se han constituido órganos administrativos especializados para desarrollar esta relación tecnológica con las actividades estatales, como es el caso de la Oficina Nacional de Gobierno Electrónico e Informática del Perú (); en Guatemala, no se cuenta con un órgano especializado para la materia, aunque existió un ente temporal denominado la Comisión Presidencial para la Reforma, Modernización y Fortalecimiento del Estado y de sus Entidades Descentralizadas –COPRE-, la cual fue inicialmente constituida mediante el Acuerdo Gubernativo Número 24-2002 y fue reformada para el ámbito TIC con fecha 4 de noviembre de 2004 mediante Acuerdo Gubernativo Número 346-2004, el cual en el artículo 1 establecía entre sus funciones: “La formulación de políticas y estrategias, así como la ejecución de los planes, programas y acciones necesarios para la implementación del Gobierno Electrónico en el Estado, la promoción del consenso y la coordinación de dichas acciones con todas las Instituciones del Organismo Ejecutivo; entiéndase por Gobierno Electrónico la aplicación de las tecnologías de la información y las comunicaciones, con el propósito de lograr eficacia y transparencia en la gestión del gobierno.” La comisión fue suprimida mediante el Acuerdo Gubernativo Número 21-2008 de fecha 22 de abril de 2008.

En Guatemala, no existe actualmente una entidad especializada que pueda impulsar el desarrollo de las funciones administrativas mediante las TIC, por lo cual cada ente ha realizado su desarrollo en forma individual, o mediante convenios con otras entidades u organismos

internacionales logrando brindar a los usuarios aplicaciones en línea para su servicio. Ejemplos encontramos con los tres organismos de Estado [www.congreso.gob.gt](http://www.congreso.gob.gt) (Organismo Legislativo), [www.oj.gob.gt](http://www.oj.gob.gt) (Organismo Judicial) y [www.guatemala.gob.gt](http://www.guatemala.gob.gt) (Organismo Ejecutivo). Cabe destacar en materia de uso de TIC en las actividades que desarrollan, a la Superintendencia de Administración Tributaria ([www.sat.gob.gt](http://www.sat.gob.gt)), la Corte de Constitucionalidad ([www.cc.gob.gt](http://www.cc.gob.gt)) y el portal de Guatecompras ([wwwguatecompras.gob.gt](http://wwwguatecompras.gob.gt)). Además, otras entidades que se encuentran en un aceptable desarrollo web, en su fase inicial, son:

[www.muniguate.com](http://www.muniguate.com)

Municipalidad de Guatemala

[www.igssgt.org](http://www.igssgt.org)

Instituto Guatemalteco de Seguridad Social

[www.contraloria.gob.gt](http://www.contraloria.gob.gt)

Contraloría General de Cuentas

[www.idpp.gob.gt](http://www.idpp.gob.gt)

Instituto de la Defensa Pública Penal

[www.mp.gob.gt](http://www.mp.gob.gt)

Ministerio Público

[www.diaco.gob.gt](http://www.diaco.gob.gt)

Dirección de Atención y Asistencia al Consumidor

[www.banguat.gob.gt](http://www.banguat.gob.gt)

Banco de Guatemala

[www.mineduc.gob.gt](http://www.mineduc.gob.gt)

Ministerio de Educación

[www.mintrabajo.gob.gt](http://www.mintrabajo.gob.gt)

Ministerio de Trabajo y Previsión Social

La administración pública ha construido portales web destinados en forma exclusiva a la realización de procedimientos administrativos, o parte de ellos, vía Internet o en línea. El portal de Guatecompras es uno de los ejemplos en constante desarrollo y utilización de parte de los órganos administrativos. El Reglamento de la Ley de Contrataciones del Estado y sus reformas establece:

**Artículo 4 Bis. Sistema de Información de Contrataciones y Adquisiciones del Estado.** El Sistema de Información de Contrataciones y Adquisiciones del Estado, adscrito al Ministerio de Finanzas Públicas, deberá ser utilizado para la publicación de todo proceso de compra, venta y contratación de bienes suministros, obras y servicios que requieran las entidades reguladas en el artículo 1 de la Ley, desde la convocatoria, resolución de impugnaciones si las hubiere, hasta la adjudicación, incluyendo las compras por excepción y todos los procedimientos establecidos en la Ley y en el presente Reglamento.

Los interesados que deseen solicitar aclaraciones sobre los documentos de licitación, cotización, contrato abierto, incluidas las compras por excepción deberán hacerlo a través del Sistema de Contrataciones y Adquisiciones del Estado, denominado GUATECOMPRAS. Las respuestas aclaratorias también deberán ser publicadas en el mencionado sistema.

La Superintendencia de Administración Tributaria, por medio de su portal electrónico, es uno de los mejores ejemplos del uso de las TIC en las actividades de los órganos administrativos.

El Código Tributario nos da uno de muchos ejemplos en el artículo 98 incisos 1, 2 y 6:

**ARTICULO 98 “A”.** Otras atribuciones de la Administración Tributaria. La Administración Tributaria también podrá:

1. Establecer de mutuo acuerdo con el contribuyente, una dirección electrónica en Internet, o buzón electrónico, para cada uno de los contribuyentes y responsables, a efecto de remitirles los acuses de recibo de las declaraciones y pagos efectuados, boletines informativos, citaciones, notificaciones y otras comunicaciones de su interés, cuando correspondan.
2. Establecer procedimientos para la elaboración, transmisión y conservación de facturas, libros, registros y documentos por medios electrónicos, cuya impresión pueda hacer prueba en juicio y los que sean distintos al papel.
6. Requerir a los contribuyentes que presenten el pago de los tributos por medios electrónicos teniendo en cuenta la capacidad económica, el monto de ventas y el acceso a redes informáticas de los mismos.<sup>40</sup>

En otros Estados, se han emitido ordenamientos específicos para fomentar y regular el uso de TIC en las relaciones entre la administración pública y las

personas; en España, la Ley 11/2007 establece que: “La presente Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.” (Artículo 1. Objeto de la Ley). En Guatemala, al no existir una política integral, cada ente público desarrolla las aplicaciones y procedimientos que diseñen.

Actualmente, las pólizas electrónicas en materia aduanera, el uso incipiente de la factura electrónica, los registros civiles y mercantiles con libros electrónicos, son ejemplos del uso cada vez mayor de los documentos electrónicos o mensajes de datos que se incorporan cada día a un mayor porcentaje de las actividades que realizan la administración pública y privada. “El poder público no puede estar a la zaga de los particulares en la utilización de la informática y las telecomunicaciones. Por ello, se hace necesario desarrollar políticas públicas dirigidas a promocionar la investigación tecnológica, capacitar a profesionales y técnicos del Estado y a los particulares en el conocimiento de las nuevas tecnologías, incentivar el uso de las tecnologías en la actividad intergubernamental y en las relaciones que se instauren entre los órganos del poder público y los particulares.” (Hernández, 2002)

---

<sup>40</sup> El subrayado es de referencia, no es parte de la publicación oficial.

Es importante resaltar que las personas y funcionarios públicos responsables de los sistemas de información en las plataformas de comercio electrónico y de gobierno electrónico, deberán contar con medidas de seguridad tecnológicas y legales para el diseño, implementación, uso y desarrollo de los servicios privados o públicos que se presten, así como auditorías periódicas para poder garantizar las actividades en línea, pero en especial para obtener la confianza de los usuarios y asegurar el bien jurídico más importante dentro del sistema: la información y los derechos y obligaciones intrínsecos a la misma.<sup>41</sup>

## 2. Los documentos electrónicos, mensajes de datos y/o comunicaciones electrónicas

Los documentos electrónicos surgen por el uso de las computadoras y tienen su mayor expresión en la comunicación por medio de redes y la Internet, es decir, la necesidad de digitalizar el contenido de lo redactado o escrito en formato papel, por varias razones, siendo una de las principales, el poder procesar esa información y acceder a ella en cualquier

momento y desde cualquier lugar, menor espacio físico para almacenar, entre otras circunstancias que han vuelto de su uso algo común; pero al principio también existen desventajas en estos documentos, como la incompatibilidad de algunos sistemas, la necesidad de medios electrónicos para su visualización y por supuesto, limitaciones de aspectos legales, pero los aspectos anteriores se han superado por medio de la propia tecnología, y en algunos casos, de la ley.

Podemos partir de indicar que “Al hablarse de documentos electrónicos se alude a casos en que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales, y en que la actividad de un computador o de una red sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque sólo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales.” (Jijena, 2000)

---

<sup>41</sup> Existen definiciones fundamentales en materia de seguridad por lo cual indicamos las principales contenidas en el Glosario del Real Decreto 3/2010 Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (España. 2010):

Auditoría de la seguridad. Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

Gestión de incidentes. Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Política de seguridad. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Requisitos mínimos de seguridad. Exigencias necesarias para asegurar la información y los servicios.

Sistema de gestión de la seguridad de la información (SGSI). Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

## 2.1. Los documentos electrónicos

En doctrina, se le denomina indistintamente documento electrónico, documento digital, documento informático; en la legislación nacional y en algunos casos la internacional, se conceptualiza como mensaje de datos, además de considerar la definición de comunicaciones; todos los conceptos se utilizan de una manera uniforme, aunque algunos autores han encontrado diferencias, pero sigue siendo el concepto documento electrónico el más utilizado.

Para poder definir estos conceptos debemos partir de que la doctrina tecnológica y en especial la jurídica, han querido otorgarle al documento electrónico los mismos efectos que produce el documento escrito en soporte papel. El concepto documento del latín *documentum* es definido por la Real Academia Española como “1. m. Diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos. 2. m. Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.” () Francesco Carnelutti define documento como “Cualquier cosa idónea para la representación de un hecho”. (2000). En cuanto al ámbito legal el Código Procesal Civil y Mercantil establece en el artículo 178 los documentos admisibles los cuales “Podrán presentarse toda clase de documentos, así como fotografías, fotostáticas, fotocopias, radiografías, mapas, diagramas, calcos y otros similares.” (el subrayado es de referencia no es parte de

la publicación oficial). El Código Procesal Penal establece el principio de libertad de prueba indicando que “Se podrán probar todos los hechos y circunstancias de interés para la correcta solución del caso por cualquier medio de prueba permitido. Regirán, en especial, las limitaciones de la ley relativas al estado civil de las personas.” (Artículo 182)

Exponemos lo anterior para confirmar que las definiciones de la Real Academia Española<sup>42</sup> y la definición doctrinaria, e inclusive, la propia legislación, no establecen que en la definición de documento se haga referencia a que su soporte sea en papel, la importancia y esencia de un documento sigue siendo el contenido que es algo escrito, aunque existen problemas en la práctica nacional, porque algunos juristas aún sujetan la única posibilidad documental al soporte papel.

Por lo anterior, al referirnos al documento en forma general, entenderemos un objeto que contiene la representación de un hecho y al establecer el adjetivo electrónico, hacemos referencia al soporte donde se almacena esa representación, o al sistema como se almacena el contenido, aunque, algunos autores refieren al concepto digital; al respecto, hay que recordar que “electrónico” hace referencia a la ciencia Electrónica, es decir, a la forma de crear las señales digitales y el concepto “digital” refiere a la forma de representar los objetos o información a través de valores numéricos, lo cual regularmente se realiza con programas de ordenador. El uso del

<sup>42</sup> Utilizamos la definición de documento que indica la Real Academia Española en virtud que nuestra legislación no cuenta con una definición exacta; lo anterior en virtud de que la Ley del Organismo Judicial establece en el artículo 11 que “Las palabras de la ley se entenderán de acuerdo con el Diccionario de la Real Academia Española, en la acepción correspondiente, salvo que el legislador las haya definido expresamente.”

concepto electrónico tiene como objeto fundamental cumplir con el principio de neutralidad tecnológica, para poder cubrir, por así decirlo, con cualquier tecnología que se utilice para crear, almacenar y procesar el documento en ese formato. Por otra parte, quienes aducen el uso del término digital establecen que “el término “electrónico” hace referencia al dispositivo en el que está almacenado el instrumento o por medio del cual fue confeccionado.”<sup>43</sup>

El vocablo “digital”, en cambio, además de su definición estrictamente tecnológica, tiene una connotación diferente a la que aquí apelamos, puesto que implica “ausencia de tangibilidad”. En suma, si al término “documento” se le agrega la palabra “electrónico” se sigue manteniendo la dependencia del instrumento con su soporte, impidiendo de este modo el desprendimiento conceptual de ambos.” (Sarra, 2001)<sup>44</sup>

## 2.2. Definición de documentos electrónicos y mensaje de datos

La Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto Número 47-2008 del Congreso de la República de Guatemala, en el artículo 2 define mensaje de datos como “El documento o información generada,

enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (IED), el correo electrónico el telegrama, el télex o el telefax.” En el reglamento de la ley en cambio se define el concepto documento electrónico como “toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.” (Artículo 2)

El documento electrónico o mensajes de datos es toda forma de representación de hechos o acciones que contienen datos o información creados por una persona a quien se le atribuye, quien lo genera y almacena a través del uso de equipo electrónico, es decir puede visualizarse solamente por medio de ordenadores<sup>45</sup>, esto es, que “los documentos que se encuentran en un soporte informático necesitan, para poder ser visualizados e interpretados en lenguaje natural, de un proceso mediante un programa, con un procedimiento lógico, que convierta la expresión, en codificación informática, a la misma expresión, en lenguaje natural, y la represente en un equipo que pueda ser visualizado directamente por el hombre.” (Davara, 2006)

---

<sup>43</sup> En el Reglamento de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, artículo 2, define: Electrónico: característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares.

<sup>44</sup> Algunos autores como Andrea Sarra le denominan Instrumento Digital en virtud de “que no es más que una nueva forma de instrumentar los actos jurídicos, mediante la utilización de medios digitales. Así, un instrumento de este tipo es aquel que ha sido confeccionado con tecnología digital, al cual se le considera intangible por el hecho de no haber sido plasmado en soporte tangible. Esta característica de intangibilidad permite que pueda fluir por las redes y quedar almacenado en la memoria de una computadora o en cualquier otro dispositivo de almacenamiento (sea éste un soporte magnético, un soporte óptico, un soporte electrónico, etcétera).” (Sarra, 2001)

<sup>45</sup> Al referirnos a ordenadores debemos de considerar otros dispositivos electrónicos que cuentan con funciones similares en la administración de documentos como una agenda electrónica, teléfono móvil o ebook.

### 2.3. Situaciones distintas entre documentos creados mediante ordenadores

Es importante aclarar cuatro situaciones distintas entre los documentos en soporte papel y en soporte electrónico cuando son creados, generados o incorporados por medio de una computadora, así como en su caso, la conservación del primero por medios digitales o la impresión de los segundos, en especial cuando serán utilizados como medios de prueba. La primera situación surge cuando se utiliza un programa como el procesador de textos instalado en una computadora para elaborar o redactar (teclar o digitar) un documento y después imprimirllo, porque el soporte es en sí el papel como lo podría ser un contrato privado, una acta de legalización de firmas o un memorial a presentar en un juzgado; para este caso no utilizamos el concepto de documento electrónico o digital, porque el equipo informático ha sido una herramienta para su edición e impresión, pero la validez jurídica la tiene el documento en soporte papel, convirtiéndose el archivo informático en un simple respaldo<sup>46</sup>. La segunda situación surge cuando los documentos en formato papel deben ser conservados para su ulterior consulta en una forma rápida y ordenada, para lo cual se realiza la

digitalización del documento, conocida comúnmente como “escanear” que es el acto de realizar una copia del documento original plasmado en formato papel y archivarlo en forma electrónica por medio de un dispositivo periférico, comúnmente un escáner; en este caso, el original sigue siendo el formato papel, pero se cuenta con un respaldo electrónico.<sup>47</sup>

La tercera forma de generar documentos es cuando la información o los contenidos se ingresa, digitando los datos en forma directa a un sistema informático, por ejemplo los archivos informáticos del Registro General de la Propiedad, o del Registro Civil de las Personas, en donde el documento original es de naturaleza electrónica y la versión que se da a los usuarios es una versión impresa en papel, o en su caso, una certificación de ese archivo digital; en este caso, el documento original es el electrónico (magnético u óptico) y se encuentra en poder (disponibilidad) solo de su titular o responsable, y lo que se entrega a los usuarios en formato papel es una reproducción; nótese que aquí el original es electrónico.<sup>48</sup>

La cuarta situación de documentos generados por TIC representan para el presente tema, los de mayor importancia, es decir, los denominados documentos

---

<sup>46</sup> Dos observaciones: es similar a utilizar una máquina de escribir mecánica o eléctrica; si debe de manifestarse voluntad por parte de la persona deberá realizarse por medio de la firma manuscrita u autografa de la misma.

<sup>47</sup> Un ejemplo lo constituye el Reglamento de Inscripciones del Registro Civil de las Personas que indica para estos casos: Artículo 15. Conservación de Documentos. Los documentos que motiven un asiento en los Registros Civiles, se conservarán mediante el sistema de escáner, en un archivo digital, con control de índices que permitan su pronta localización y consulta.

<sup>48</sup> El Reglamento de Inscripciones del Registro Civil de las Personas establece: Artículo 13. Todos los libros que se lleven en los Registros Civiles, serán electrónicos, los cuales deberán cumplir con los requisitos de uniformidad, inalterabilidad, seguridad, certeza jurídica y de publicidad.

electrónicos, o en su caso, mensajes de datos, los cuales se forman en el ordenador, se archivan en un dispositivo electromagnético, se transmiten por medio de redes y se reciben en otro ordenador o servidor y su destino es mantenerse en formato electrónico; documentos como los correos electrónicos, los formularios de declaración tributaria, las notificaciones electrónicas, certificaciones electrónicas, entre otros, pero limitándonos, por el momento, a los documentos generados, almacenados o transmitidos por medio de equipos informáticos (hardware y software).<sup>49</sup>

Insistimos en que estos documentos se generan, transmiten y/o almacenan en soportes electrónicos y no están destinados a reproducirse por medio de una impresora (periférico de salida), es decir, no se van a imprimir en formato papel, salvo casos extremadamente necesarios, pero en esta última situación el original es el documento electrónico y cualquier reproducción en formato papel es el equivalente a una fotocopia simple.<sup>50</sup>

#### 2.4. Los documentos electrónicos privados y públicos

Existe variedad de documentos electrónicos, pero para aspectos legales, cobran relevancia los documentos-e en los cuales se exige la firma de la persona emisora o funcionario responsable, como es el caso de los entes estatales que podrán emitir certificaciones de los documentos electrónicos en formato papel o en formato

electrónico cuando la ley así lo exija, por ejemplo, lo establecido por el Reglamento de la Ley de Garantías Mobiliarias:

**Artículo 13. Certificaciones.** Las solicitudes de certificaciones que se presenten al Registro de Garantías Mobiliarias, podrán hacerse a través del SRGM y serán emitidas por el Registro en forma física o electrónica. Las certificaciones que se emitan en forma física deberán ir firmadas por el Registrador y selladas con el sello del Registro de Garantías Mobiliarias. Las que se emitan en forma electrónica deberán contener firma electrónica.

Otro ejemplo de la emisión de las certificaciones la establece el Código Civil al indicar al respecto:

**Artículo 1183.** Las certificaciones se extenderán por medio de fotocopias, fotostáticas, trascipción mecánica o por cualquier medio de reproducción físico informático, magnético o electrónico y llevarán la firma y sello del registrador que la extiende y sello del Registro, salvo lo dispuesto en el párrafo siguiente. La firma deberá constar por cualquiera de los medios y con los efectos jurídicos que establece el numeral 8º del artículo 1131.

Las certificaciones pueden ser sustituidas por copias fotográficas, legalizadas por el registrador.

---

<sup>49</sup> Otros autores como Miguel Temboury indica que “si nos atendemos a la estricta realidad, resulta que lo que denominamos documento electrónico, quedaría mejor definido por la expresión instrumentos ópticos, magnéticos o de otro tipo generados por fenómenos electrónicos, y capaces de reproducir esos mismos fenómenos, los cuales a su vez pueden reproducir una realidad directamente entendible por el ser humano.” (2000)

<sup>50</sup> Salvo que una norma o procedimiento les de un valor diferente.

Encontramos que en los artículos citados anteriormente se exige en las certificaciones electrónicas la firma y/o firma electrónica, tema que se analiza en un punto posterior, pero que para el caso de los documentos electrónicos la firma electrónica de una persona lo convierte en un documento privado<sup>51</sup> (en soporte electrónico) y la firma electrónica de un funcionario público investido de fe pública lo convierte en un documento electrónico público.<sup>52 - 53</sup>

Cuando ese documento se genera y se almacena en una computadora, nos referimos en forma técnica como un archivo informático, y claro que puede ser utilizado como prueba en un proceso, inclusive, si se tratara de un correo electrónico, sigue siendo un documento electrónico; el determinar la autoría<sup>54</sup> de los documentos creados mediante el uso de programas de ordenador, su originalidad y otros aspectos como la validez legal, hacen que se deba revestir de otros mecanismos tecnológicos para poder garantizar los efectos legales que pueda conllevar, en especial, cuando ese documento se convierte en un contrato electrónico para lo cual la manifestación de

voluntad y la identificación de la persona en el ambiente tecnológico se convierte en un nuevo campo para el Derecho.

### 3. Las formas de manifestar la voluntad en el ámbito electrónico

Cada día vemos en nuestras actividades diarias y laborales el uso más frecuente de documentos electrónicos los cuales en determinados casos se convierten en declaraciones de voluntad, contratos o en su caso actos administrativos; por lo anterior es necesario identificar al autor de esa declaración o comunicación electrónica, por ello en el ambiente de los bytes veremos formas diferentes de manifestar la voluntad a la que estamos acostumbrados y que son propias del ámbito digital y que a la vez identifiquen a las personas. Los medios más comunes para manifestar la voluntad en el ambiente electrónico son los denominados contrato "click", el contrato Browse y la firma electrónica.

---

<sup>51</sup> Documento privado: "1. m. Der. El que, autorizado por las partes interesadas, pero no por funcionario competente, prueba contra quien lo escribe o sus herederos." (RAE, 2009)

<sup>52</sup> Documento público: "1. m. Der. El que, autorizado por funcionario para ello competente, acredita los hechos que refiere y su fecha." (RAE, 2009)

<sup>53</sup> Al respecto la Ley de Firma Electrónica de España (59/2003) establece que el documento electrónico será soporte de:  
a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.  
b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.  
c) Documentos privados. (Artículo 3. Firma electrónica, y documentos firmados electrónicamente)

<sup>54</sup> Es importante diferenciar entre determinar la autoría del mensaje de datos y establecer de que computadora fue enviado el archivo; para esta segunda situación existen peritos informáticos que pueden determinar la dirección IP y en su caso la dirección MAC. La dirección IP consiste en un conjunto de números que identifican a una computadora, red de ordenadores o cualquier dispositivo de comunicación que se encuentre conectado a la Internet. La dirección MAC (Media Access Control) o control de acceso al medio, es un número único de identificación asignado por el fabricante de la tarjeta de red de un computador y este dispositivo es necesario para que pueda conectarse a la red interna o Internet.

La forma más común de manifestar la voluntad en Internet se conoce como contrato click y hace posible que cuando la persona quiera obligarse a lo acordado con un proveedor, las condiciones quedarán aceptadas en el momento en que se seleccione la opción ACEPTAR<sup>55</sup>, lo cual se realiza a través de un periférico de entrada como un mouse, cuando coloca el apuntador en la selección aceptar y pulsa el botón del mouse (regularmente el botón izquierdo) y a esa acción se le denomina click<sup>56</sup>. En doctrina, se le conoce a estos contratos con el término click-wrap contract.<sup>57</sup>

Esta modalidad surge por la gran cantidad de contratos, la distancia entre las partes contratantes, el agilizar los procedimientos de acordar voluntades, la economía en el comercio electrónico y un sin fin de razones.

La forma de manifestar la voluntad conocida como contrato Browne surge en las plataformas electrónicas, especialmente en la navegación por la Internet; en ella se adquieren derechos y obligaciones por la simple acción de acceder a ciertas páginas o sitios web, lo que representa que el usuario se ha vinculado a las condiciones, que regularmente aparecen en la parte inferior central del sitio, por estar conectado a ese espacio electrónico.

La diferencia entre los contratos click y los contratos browse radica en que “el usuario no requiere manifestar su voluntad o siquiera disponer de la oportunidad de revisar los términos y condiciones del contrato –de licencia, por ejemplo- para quedar vinculado por este. El vínculo se presume por el solo hecho de utilizar el bien o servicio regulado contractualmente.” (Iñigo y Cruz, 2004)

En el ambiente electrónico, el usuario podrá seguir utilizando en diversas acciones las manifestaciones click y Browne; cuando la aceptación de derechos y obligaciones lleve inmerso un verdadero acuerdo de voluntades (y no una simple adhesión) y la identificación de las partes se realiza en línea, se hace necesario utilizar otra forma de manifestar la voluntad; en este caso, se utiliza la denominada firma electrónica, la cual según la tecnología utilizada, o la regulación de cada Estado, recibe denominaciones como firma digital o firma electrónica.

#### 4. Aspectos esenciales de la firma electrónica

Empezamos recordando que los documentos siguen siendo un medio de prueba eficiente en el ámbito contractual y que en su contenido, se identifica a la

<sup>55</sup> Agrega Andrea Sarra que “Puede afirmarse que se trata de un verdadero contrato entre ausentes. Sin embargo, por las características de las redes abiertas (fundamentalmente por su inseguridad), la práctica en este tipo de comercio ha impuesto que para confirmar la recepción de la aceptación, una vez conocido el contenido de la aceptación, el oferente envíe por correo electrónico su confirmación al aceptante. Esta práctica corresponde a la teoría de la reconocición y de acuerdo con algunas opiniones podría ser la mejor tutela a los intereses de las partes.” (2001)

<sup>56</sup> Se considera en doctrina que estos son contratos de adhesión solo que celebrados en plataformas electrónicas.

<sup>57</sup> “La expresión click-wrap contract deriva de shrink wrap contract (contratos envueltos). El nombre de estos últimos proviene originariamente del mecanismo de distribución de los contratos de software, los que se encontraban al interior de las cajas, envueltas en celofán, que contenían el soporte físico del software. La naturaleza contractual de la licencia contenida en la caja suele ir avisada en forma impresa a través de un aviso en la caja. De esta manera, el consumidor puede saber que, una vez que ha abierto el celofán queda vinculado por los términos del contrato que esta contiene.” (Madison; citado por Iñigo de la Maza y Sergio Cruz, 2002)

persona contratante, quien manifiesta su voluntad por medio de su firma autógrafo; en la administración pública, en una resolución, se identifica al funcionario competente al inicio y manifiesta la voluntad de la dependencia administrativa por medio de su firma, e inclusive, en algunos casos, el sello.

Lo anterior, es una explicación básica para poder describir qué pasa si el contrato es electrónico y si el acto de la administración pública es por medios digitales, en especial, por la certeza que nos otorga documentar los actos.<sup>58</sup>

Determinamos la existencia y validez del documento electrónico por lo cual ahora indicaremos los aspectos técnicos y legales de la firma electrónica, partiendo de recordar que el uso de la tecnología con la cual se genera la firma electrónica no se realizó en un inicio con el objetivo de poder cumplir con el marco legal de los países, porque este último no existía; su origen fue la seguridad informática y posteriormente, el Derecho estableció una regulación al respecto. Señalo lo anterior porque debemos dejar establecido que las comunicaciones electrónicas debían contar con procedimientos que pudieran identificar a la persona emisora en el ámbito electrónico y que la información que viaja entre un punto y otro en una red abierta pudiera realizarlo,

en forma segura (encriptada).<sup>59</sup> Fue así como se desarrollaron programas de seguridad informática para poder cumplir con esas condiciones, en especial con la manifestación de voluntad del sujeto y posteriormente se aplicó la seguridad jurídica a estos sistemas para cumplir con el ámbito legal, denominándole como un equivalente funcional a la firma autógrafo o manuscrita con el término firma electrónica.

#### 4.1. La firma en el contexto actual

Establecimos que existe una acción denominada digitalización y que consiste en trasladar objetos, actos y procedimientos, del mundo de los átomos al mundo de los bytes; uno de esos objetos o actos que se han trasladado son las firmas. Para comprender mejor lo que es la firma electrónica y sus efectos legales en el ambiente electrónico, explicaremos brevemente acerca de la firma en general, y en especial, de la firma autógrafo y sus finalidades para aplicar el principio de equivalencia funcional al trasladarla al ambiente electrónico a la comunicación en las redes.

#### 4.2. Definición de firma

No existe una ley que defina el concepto o que establezca sus efectos legales, requisitos o condiciones; el concepto

<sup>58</sup> Documentar (Del lat. document•re). Probar, justificar la verdad de algo con documentos. Instruir o informar a alguien acerca de las noticias y pruebas que atañen a un asunto. (RAE; 2009)

<sup>59</sup> “Como respuesta a esta necesidad de conferir seguridad a las comunicaciones por internet surge, entre otros, la firma electrónica. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados prestadores de servicios de certificación. Para ello expedirán certificados electrónicos, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.” (Exposición de Motivos, Ley 59/2003, España).

de firma ha evolucionado durante la historia. La definición que proporcionaremos tiene por objeto no ubicar una clase de firma en especial; en forma general, firma es un signo creado por una persona que plasma en un soporte y que representa al signatario o emisor, y que puede llevar inmersa la aceptación de su contenido en el formato donde fue colocada.

#### 4.3. La firma autógrafa

Por ser la firma autógrafa la más identificada en la sociedad y la que en algunas condiciones se trata de equiparar a la firma electrónica, empezamos por determinar su significado; el término firma proviene del latín firmare que significa afirmar o dar fuerza; el término autógrafa equivale a grabar o escribir por sí mismo. Lo anterior significa que es la persona con su propia mano la que con el trazo de los signos que realiza y que ha determinado, afirma lo que está establecido en donde la plasma. La Real Academia Española define la firma como “Nombre y apellido o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en él se dice.” (RAE; 2009)

En doctrina, se define la firma autógrafa como “la que suscribe la persona física con su propia mano y consiste en un conjunto de letras o bien algún componente de su nombre y a veces el nombre y apellido, aunado a una serie de trazos que pueden abarcar toda gama de evoluciones del instrumento de escritura, que señalan e identifican al sujeto y lo separan de otros, en los documentos que suscribe y es un elemento que refleja permanentemente su

voluntad de expresar lo que firma, o de obligarse al tenor del texto que suscribe.” (Acosta; 2003)

#### 4.4. Objeto y características de la firma autógrafa

La forma de determinar que una persona estaba de acuerdo, o aceptaba el contenido de documentos o actos, ha evolucionado en la historia desde el manufirmatio, el uso de sellos reales o signos de identificación, hasta llegar a lo que conocemos actualmente como la firma autógrafa, forma que hasta ahora han utilizado las personas para manifestar su voluntad; por eso es importante establecer su objeto para poder compararla con la firma electrónica. Se consideran varias razones de la existencia de la firma, pero fundamentalmente son dos: identificar a la persona y determinar la voluntad de la obligación, o su aceptación.

#### 4.5. Clasificación de las firmas

En virtud de que existen en la ley distintas situaciones para el acto de firmar y la doctrina no tiene una posición concertada al respecto, proponemos la siguiente clasificación: firma en cuanto a la forma o procedimiento de creación (manuscrita, mecánica y electrónica); firma en cuanto al formato donde se plasma (papel, objetos materiales y electrónico); en cuanto a la naturaleza de la persona que identifica (persona individual y persona jurídica -privada o pública); la más relevante para el Derecho, firma en cuanto a los efectos legales (con efectos jurídicos o sin efectos jurídicos).

#### 4.6. La seguridad y la firma electrónica

Al utilizar redes abiertas existen riesgos importantes que se derivan del intercambio de información, en especial en el uso de documentos electrónicos,<sup>60</sup> entre las que tenemos “que el autor y fuente del mensaje sea suplantado; que el mensaje sea alterado, de forma accidental o de forma maliciosa, durante la transmisión; que el emisor del mensaje niegue haberlo transmitido o el destinatario haberlo recibido; y que el contenido del mensaje sea leído por una persona no autorizada.” (Martínez; 2000)

Como es necesario cubrir todos estos riesgos, el Derecho debe trabajar con la Informática y aprovechar toda la tecnología existente para que esas necesidades tengan cobertura y aseguramiento legal. Esto se puede realizar a través de los siguientes servicios de seguridad: “a) La autenticación, que asegura la identidad del remitente del mensaje y permite asegurar que un mensaje procede de quien dice que lo envía; b) La integridad, que garantiza que el mensaje no ha sido alterado en el tránsito; c) El no rechazo o no repudio en origen y en destino, que garantiza que una parte interviniente en una transacción no pueda negar su

actuación; y d) La confidencialidad, que protege los datos de revelaciones o accesos de terceros no autorizados.” (Proyecto de guía para la incorporación al derecho interno del Régimen Uniforme de la UNCITRAL para las Firmas Electrónicas).

Por lo anterior, es necesario utilizar la tecnología para identificar y manifestar la voluntad de las personas, lo cual se conoce como firma electrónica, desarrollados por medio de programas informáticos con niveles altos de seguridad, uso de la criptografía<sup>61</sup> y procedimientos de certificación.<sup>62</sup>

Existen esencialmente dos tipos de Criptografía: Encriptación Simétrica o de Clave Privada, y Encriptación Asimétrica o de Clave Pública

#### 4.6. Definición de la firma electrónica

La firma electrónica se define como “un bloque de caracteres que acompaña a un documento (o fichero) acreditando quien es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad). Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema criptográfico

<sup>60</sup> “En un entorno electrónico, el original de un mensaje no se puede distinguir de una copia, no lleva una firma manuscrita y no figura en papel. Las posibilidades de fraude son considerables debido a la facilidad con que se pueden interceptar y alterar datos en forma electrónica sin posibilidad de detección y a la velocidad con que se procesan transacciones múltiples. La finalidad de las diversas técnicas que ya están disponibles en el mercado o que se están desarrollando es ofrecer medios técnicos para que algunas o todas las funciones identificadas como características de las firmas manuscritas se puedan cumplir en un entorno electrónico. Estas técnicas se pueden denominar, en general, firmas electrónicas”. (Régimen Uniforme FE -UNCITRAL-)

Proyecto de guía para la incorporación al derecho interno del Régimen Uniforme de la CNUDMI (UNCITRAL) para las Firmas Electrónicas

<sup>61</sup> El término Criptografía proviene del griego Kryptos que significa oculto y de Graphos significado de escritura. Básicamente criptografía es “Una técnica basada en un algoritmo matemático que transforma un mensaje legible a su equivalente en un formato ilegible para cualquier usuario que no cuente con la clave secreta para desencriptarlo.” (Hance; 1996) La encriptación está basada en dos elementos: Un Algoritmo y una Clave. El algoritmo es el conjunto de caracteres en que viaja la información y la clave es la combinación para resolver el algoritmo y poder interpretarlo. Si alguien intercepta el mensaje, el cual irá en forma de algoritmo (conjunto de carácter sin sentido), no podrá descifrarlo sin la clave. (Barrios; 2006) Existen esencialmente dos tipos de Criptografía: Encriptación Simétrica o de Clave Privada y Encriptación Asimétrica o de Clave Pública

<sup>62</sup> Se define Certificación como la actividad que consiste en que una persona facultada legítimamente acredite que un acto o hecho se ajusta a determinados requisitos o especificaciones de carácter técnico o inclusive jurídico caso.

asimétrico), a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no revocación o no repudio). De esta forma, el autor queda vinculado al documento de la firma. Por último la validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor". (Ramos, 2000)

El artículo 2 de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas –LRCFE-, Decreto Número 47-2008 del Congreso de la República de Guatemala define a la firma electrónica como "Los datos en forma electrónica consignados en una comunicación electrónica, o adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para identificar al firmante con relación a la comunicación electrónica e indicar que el firmante aprueba la información recogida en la comunicación electrónica."

#### 4.7. Sujetos que participan en la firma electrónica

Los sujetos que participan en la creación y uso de una firma electrónica son el emisor o suscriptor, el receptor o destinatario, la autoridad de certificación, o proveedor de servicios de certificación y el organismo licenciatario; para definirlos, utilizaremos la legislación nacional en la materia. En la LRCFE, el emisor es definido como iniciador siendo "toda parte que haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar una comunicación electrónica antes de ser archivada, si ese es el caso, pero que no haya actuado a título de intermediario con respecto a esa comunicación electrónica." (Artículo 2). El receptor o destinatario es "la parte designada por el iniciador para recibir

la comunicación electrónica, pero que no está actuando a título de intermediario con respecto a esa comunicación electrónica."

El proveedor de servicios de certificación –PSC- es la persona jurídica, pública o privada, de origen nacional o extranjero, que previa solicitud al Registro de Prestadores de Servicios de Certificación del Ministerio de Economía, cuenta con la capacidad y con los elementos técnicos para la generación de firmas electrónicas avanzadas, la emisión de certificados sobre su autenticidad y la conservación de mensajes de datos para que cuenten con las acreditaciones necesarias por los órganos o entidades correspondientes, según la normativa vigente. (Artículo 40 LRCFE)

El organismo licenciatario u órgano administrativo competente se define en el reglamento de la LRCFE como "Entidad Autorizadora: el Registro de Prestadores de Servicios de Certificación adscrito al Ministerio de Economía –RPSC-." Este último ejerce las facultades establecidas en la ley entre las que se encuentran autorizar la actividad de las entidades prestadoras de servicios de certificación, velar por el funcionamiento y la eficiente prestación del servicio por parte de las prestadoras de servicios de certificación, imponer sanciones a las PSC en caso de incumplimiento de sus obligaciones, emitir las regulaciones que considere basadas en las normas, regulaciones, criterios o principios internacionales reconocidos. (Artículo 49, LRCFE)

#### 4.8. Los certificados de la firma electrónica

En el caso de las firmas electrónicas la Autoridad de Certificación emitirá un certificado para autenticar la relación entre la clave y el emisor, en virtud que solo el emisor tiene control sobre la clave. El Certificado consiste en “registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten verificar que una clave pública pertenece a una determinada persona. Los certificados intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro. Contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número de serie del certificado y la firma digital del que otorga el certificado.” (Ramos, 2000) La finalidad esencial de los certificados es garantizar que la clave pública es auténtica y que corresponde al firmante (emisor), a la vez que establece que el contenido del mensaje no ha sido modificado o manipulado en el trayecto en la red. La LRCFE define certificado como “Todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma, usualmente emitido por un tercero diferente del originador y el destinatario.” (Art. 2)

#### 4.9. ¿Cómo Funciona la Firma Electrónica?

En algunos casos, dependiendo de la tecnología utilizada y la regulación al respecto, podrán existir algunas variaciones en el orden o fases para plasmar la firma, así como las diferentes clases de firmas. El sitio web de Firma Digital de Argentina

explica el procedimiento como “El firmante genera, mediante una función matemática, una huella digital del mensaje, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, que se enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento una marca que es única para dicho documento y que sólo él es capaz de producir. Para realizar la verificación del mensaje, en primer término el receptor generará la huella digital del mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que no hubo alteración y que el firmante es quien dice serlo.” (pki.gov.gt; 2009)

Puede ver el proceso de emisión de una firma electrónica o digital en el video editado por Firma Digital Argentina ([www.pki.gov.ar](http://www.pki.gov.ar)) accesible en [http://www.youtube.com/watch?v=x\\_0ANWyT2E](http://www.youtube.com/watch?v=x_0ANWyT2E).<sup>63</sup>

#### 4.10. Clases de firma electrónica

Las clases de firma electrónica varían tanto en doctrina como en la Ley Modelo y en la legislación extranjera, identificándose por los procedimientos utilizados para su generación, en especial, las creadas por medio de software, siendo las situaciones más comunes las siguientes: firma electrónica (firma electrónica simple) y firma electrónica relacionada con el mensaje de datos (denominada firma digital o firma electrónica avanzada).

<sup>63</sup> Respetando los derechos de autor se adjunta una copia del video en los anexos del presente documento.

La LRCFE define a la firma electrónica (simple) como “Los datos en forma electrónica consignados en una comunicación electrónica, o adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para identificar al firmante con relación a la comunicación electrónica e indicar que el firmante aprueba la información recogida en la comunicación electrónica.” (Art 2); además, define la firma electrónica avanzada condicionada a los requisitos siguientes: “Estar vinculada al firmante de manera única, permitir la identificación del firmante, haber sido creada utilizando los medios que el firmante puede mantener bajo su exclusivo control y estar vinculada a los datos a que se refiere, de modo que cualquier cambio ulterior de los mismos sea detectable.” (Art. 2).

#### 4.11. Principios de la Firma Electrónica

En el momento de redactar la legislación para regular la firma electrónica, cada Estado debe considerar los principios establecidos en la Ley Modelo. En forma esencial, deben considerarse dos principios fundamentales en este tema: el Principio de Neutralidad Tecnológica y el Principio de Equivalencia Funcional.

El principio de neutralidad tecnológica establece el reconocimiento de la firma electrónica sin apego a utilizar una o varias de las tecnologías existentes; lo importante es que deja abierto el camino para alguna tecnología que se desarrolle posteriormente. Los tipos de tecnologías utilizadas de mayor uso hasta el momento son la tecnología numérica o digital (software) y la tecnología biométrica.

El principio de equivalencia funcional establecido en la Ley Modelo de UNCITRAL indica que la firma electrónica debe tener los mismos efectos de la firma autógrafa. Al respecto, la ley de la materia establece

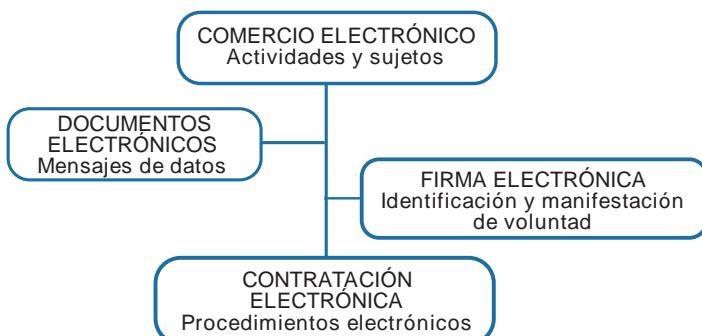
Artículo 33. Efectos jurídicos de una firma electrónica o firma electrónica avanzada. La firma electrónica o la firma electrónica avanzada, la cual podrá estar certificada por una entidad prestadora de servicios de certificación, que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta, según los criterios de apreciación establecidos en las normas procesales.

#### 4.12. Objetos o elementos que no son firma electrónica

El concepto de firma electrónica ha sido equivocado en su aplicación práctica por algunos usuarios, pero es más preocupante la equivocación en la actividad que desempeña la administración pública desvirtuando su finalidad y sus aplicaciones. No puede considerarse firma electrónica conforme a la doctrina y la técnica informática un password, escanear una firma autógrafa y reproducirla, e inclusive, una impresión dactilar incorporada electrónicamente; lo anterior en virtud que el sujeto responsable no tiene control sobre la forma de creación o generación de ese logo o imagen incorporada al documento electrónico.

## 5. Aspectos relevantes de la Ley de Comunicaciones y Firmas Electrónicas

El Decreto Número(47-2008) del Congreso de la República Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas contiene una serie de disposiciones relevantes para el conjunto de relaciones comerciales que surgen en el ambiente TIC. Podemos agrupar los temas principales con base en el siguiente esquema:



Como hemos tratado lo relativo al comercio electrónico, documentos electrónicos y firma electrónica, nos resta solo explicar brevemente la contratación electrónica y algunos aspectos procesales relevantes para su aplicación legal.

La contratación electrónica se define como “Un acuerdo de voluntades en el que las partes se comprometen a realizar una obligación consistente en dar, hacer o no hacer alguna cosa. Esta clase de contratos se caracteriza porque las declaraciones de voluntad que prestan los sujetos intervinientes se manifiestan a través de medios electrónicos, surgiendo problemas derivados del hecho de que el acuerdo de voluntades no pueda efectuarse de forma directa.” (Ramos; 2000)

La LRCFE establece el capítulo denominado Comunicaciones Electrónicas y Formación de Contratos a través de Medios Electrónicos, indicando que en “la formación de un contrato por particulares o entidades públicas, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de una comunicación electrónica. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación una o más comunicaciones electrónicas.” (Artículo 15. Formación y validez de los contratos.)

Surge entonces, la duda para algunos abogados sobre la validez jurídica, o fuerza probatoria de los documentos electrónicos y de los contratos electrónicos. Aunque siempre han podido ser utilizados como medios probatorios; la ley de la materia establece al respecto:

Artículo 11. Admisibilidad y fuerza probatoria de las comunicaciones electrónicas. Las comunicaciones electrónicas serán admisibles como medio de prueba. No se negará eficacia, validez o fuerza obligatoria y probatoria en toda actuación administrativa, judicial o privada a todo tipo de información en forma de comunicación electrónica, por el sólo hecho que se trate de una comunicación electrónica, ni en razón de no haber sido presentado en su forma original.

Aclarada la duda, existe vacilación para poder ofrecer como medio de prueba un documento o contrato electrónico, sin embargo, se establece en la ley el valor probatorio (sistema de valoración) que le corresponde:

Artículo 12. Criterio para valorar probatoriamente una comunicación electrónica. Toda información presentada en forma de comunicación electrónica gozará de la debida fuerza probatoria de conformidad con los criterios reconocidos por la legislación para la apreciación de la prueba. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje: la fiabilidad de la forma en la que se haya conservado la integridad de la información: la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.



### EJERCICIOS DE AUTOAPRENDIZAJE

Se presentará una demanda contra el Estado de Guatemala en la Corte Interamericana de Derechos Humanos. Este ente jurisdiccional le informa que todos los escritos deberán presentarse en formato electrónico con firma electrónica debidamente registrada ante un ente competente.

Vea el video que encuentra en [www.pkai.gob.ar](http://www.pkai.gob.ar) en donde se explica la firma electrónica. Explique en un máximo de 20 líneas los aspectos que usted considera más relevantes.

Investigue en Centroamérica, qué países cuentan con legislación en materia de documentos y firmas electrónicas. Haga una comparación de la legislación.



## CAPÍTULO

# 5

### LOS DELITOS INFORMÁTICOS, EL CIBERDELITO Y LOS DELITOS MEDIANTE EL USO DE LAS NUEVAS TECNOLOGÍAS

En lo referido a la averiguación de los delitos, y en la medida en que la búsqueda y acopio de datos sobre hechos y su presunto autor constituye el sentido de toda investigación criminal, la aplicación a ella de nuevas tecnologías de tratamiento de la información deviene un elemento clave.

En este contexto habremos de plantearnos si estamos o no obligados a cambiar la forma en que hemos construido algunos de los axiomas firmemente asentados a fin de que puedan resistir los embates del vertiginoso cambio tecnológico. Corresponde cuestionarnos, por ende, si nuestro cuerpo normativo, jurisprudencial y doctrinal está anclado con la suficiente firmeza como para soportar las intensas sacudidas que vienen alentadas por la técnica o si, al menos, cuenta con la suficiente flexibilidad para que su adaptación a ellos no lo fracture inutilizándolo absolutamente.

Son evidentes las mejoras que con vistas a la instrucción de los delitos han propiciado avances técnicos inimaginables hasta hace muy poco (análisis genéticos, sistemas de localización geográfica, datos de tráfico de las comunicaciones, videocámaras, dispositivos de escucha directa, programas informáticos rastreadores, agentes encubiertos en Internet, etc.), sin perjuicio de que lo que está por llegar nos seguirá sorprendiendo ad infinitum.

Julio Pérez



Introducción de las nuevas tecnologías en el derecho  
Instituto de la Defensa Pública Penal

## CONTENIDO DEL CAPÍTULO

Los usuarios de ordenadores empezaron almacenando su información en archivos computarizados, crearon programas y bases de datos; después lograron compartir esa información por medio de redes internas y redes externas; surge la Internet y los usuarios descubren un sinfín de aplicaciones para todos esos datos y programas, aprovechando toda la tecnología, no solo para compartir información, sino para comunicarse, interrelacionarse, investigar, pero sobre todo, empiezan a celebrar negocios y prestar servicios.

También otras personas pusieron interés en el uso de las TIC, solo que con otros objetivos: realizar conductas reprochables, en principio, por los usuarios legítimos, y posteriormente, por la sociedad.

Surge el delincuente informático, el que con sus acciones afecta los derechos de los titulares de los sistemas de información y que con el creciente uso ilegal de las TIC, es identificado con el término de ciberdelincuente.





## Objetivos Específicos

- a) Fundamentar los elementos de tipificación de los delitos informáticos regulados en el Código Penal guatemalteco y en su caso, en otros ordenamientos legales.
- b) Determinar qué conductas realizadas por medio de las Tecnologías de la Información y de las Comunicaciones que afecten derechos, no son constitutivas de delitos.
- c) Analizar las iniciativas de ley existentes en materia de cibercrimen y otros delitos informáticos.



## LOS DELITOS INFORMÁTICOS, EL CIBERDELITO Y LOS DELITOS MEDIANTE EL USO DE LAS NUEVAS TECNOLOGÍAS

### 1. Los delitos informáticos y los cibercrimenes

Para prohibir conductas no adecuadas en el ambiente de la Informática que afectan a los usuarios y titulares de los derechos que emanan de los sistemas, el Estado incorpora nuevos delitos a los cuales se les denomina delitos informáticos, con algunas modalidades que hacen que algunos autores los denominen delitos electrónicos; pero el desarrollo constante y vertiginoso de los bienes que se desarrollan al integrar la Informática y las telecomunicaciones, tiene como consecuencia que el tradicional concepto de delitos informáticos no logre describir todas las conductas dañosas, y en su caso ilícitas, que pueden efectuarse por medio del uso indebido de las telecomunicaciones, y en especial, en Internet.

### 2. Definición de delitos informáticos

En doctrina, encontramos los términos delitos informáticos, delitos electrónicos, computer crime; en un principio, pueden considerarse como sinónimos, pero existen diferencias que parten de determinar las acciones que estos conceptos describen como delitos. Gabriel Andrés Cámpoli define como Delitos Informáticos Electrónicos “en los cuales el autor produce

un daño o intromisión no autorizada en aparatos electrónicos ajenos (...) pero que poseen como bien jurídico tutelado en forma específica la integridad física y lógica de los equipos electrónicos y la intimidad de sus propietarios.” (2004)

El autor Miguel Davara, citando a Correa, indica que la Organización para la Cooperación Económica para el Desarrollo –OCDE- define al delito informático como “cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos.” (2006); el mismo autor define el delito informático como “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.” (2006)

Se define entonces, en forma básica, como delito informático las acciones prohibidas por la ley cometidas en contra de uno o varios de los elementos que integran un sistema de información, o los derechos que se deriven (protección de datos, intimidad o privacidad, derechos de autor) a través del uso de equipo tecnológico.

### 3. Los sujetos responsables en los delitos tecnológicos

En el caso de los delitos que atentan contra los programas de ordenador, las bases de datos automatizadas, la información contenida en los sistemas informáticos y los instrumentos de las TIC (correo electrónico, páginas o sitios web,

transmisión electrónica de datos, servidores de los proveedores de Internet, entre otros), los sujetos responsables tienden a tener un alto grado de conocimiento y de recursos en el área de informática y TIC, en virtud de que estos delitos no pueden ser cometidos por cualquier persona, se necesita cierto nivel de conocimientos y estudio; esto contrario por ejemplo al delito de robo de una computadora portátil que puede ser realizado por cualquier sujeto.<sup>64</sup>

Por la influencia que tienen en el ambiente informático las grandes empresas de computación, en especial los titulares de los programas de ordenador comerciales, se acuñó el concepto pirata informático para describir a los sujetos que violan los derechos de autor del software, en especial aquellos que reproducen sin la debida autorización las distintas clases de programas de computación con o sin fines de lucro.

En el ambiente de las TIC, a los sujetos responsables de los delitos se les describe de varias formas, siendo las más comunes: Hacker, Cracker, Pirata informático o ciberdelincuente. Los términos anteriores provienen de las conductas que manifiestan estos sujetos cuando violan la seguridad informática de los sistemas, en virtud que todo sistema informático debe contar con los procedimientos de seguridad tecnológica necesaria, los cuales se

determinan en el análisis del sistema y por medio de auditorias informáticas.<sup>65</sup>

Existen varias clases y niveles de seguridad informática, pero en este punto se describe sólo a los sujetos que violan o rompen los niveles de seguridad de acceso, o de utilización de los programas.<sup>66</sup>

El identificado como hacker es el sujeto que utiliza su conocimiento en materia informática ingresando sin autorización a los sistemas informáticos. El término proviene del uso del vocablo del idioma inglés hack que traducido significa cortar, tajar, hachazo. La acción de cortar los niveles de seguridad de un sistema informático se denomina hacking. El término cracker proviene del vocablo inglés crack que traducido significa romperse, restallido, grieta; en la jerga informática se utiliza para describir una acción más grave que la del hacker. El cracker es el sujeto que utilizando sus altos niveles de conocimiento en materia informática ingresa sin autorización a los sistemas informáticos con la finalidad de causar un daño o apoderarse de los recursos del sistema o de la información contenida.

---

<sup>64</sup> Consideraciones relevantes cuando el sujeto que realiza la acción o acciones se encuentre en calidad de imputables (los menores de edad), en virtud que los niños y adolescentes por su facilidad de comunicación por medio de las TIC son propensos a incumplir la normativa del Estado.

<sup>65</sup> La Auditoría a la Función de Informática: Se define como “el examen o revisión de carácter objetivo, critico, sistemático y selectivo, que se efectúa mediante el empleo de recursos, metodologías y técnicas de evaluación, de las políticas, normas, prácticas, funciones, procedimientos e informes relacionados con los sistemas de información computarizados, para emitir una opinión profesional sobre la eficiencia en el uso de los recursos informáticos, la validez de la información y la efectividad de los controles establecidos...” (León Zavarce y Ceferino Martínez; 2002).

<sup>66</sup> Existen normas técnicas y procedimientos de seguridad para que los usuarios no ingresen a niveles no autorizados o que personas ajenas ingresen al sistema informático.

#### 4. La Clasificación de los delitos informáticos

El Decreto Número 33-96 del Congreso de la República, publicado el veinticinco de junio de mil novecientos noventa y seis y que entró en vigencia el tres de julio del mismo año, adicionó al Código Penal lo relativo a los delitos informáticos.<sup>67</sup>

El cuarto considerando del Decreto justifica la necesidad de implementar los delitos informáticos de la siguiente forma:

“Que los avances de la tecnología obligan al Estado a legislar en bien de la protección de derechos de autor en materia informática, tipos

delictivos que nuestra legislación no ha desarrollado;...”

En virtud de la naturaleza del bien jurídico que protege el Estado a través de regular los denominados Delitos Informáticos, estos fueron ubicados dentro del Título VI De los delitos contra el patrimonio. El legislador los ubica en este apartado en virtud que se protegen creaciones de la propiedad intelectual (propiedad industrial y derechos de autor), así como derechos humanos intrínsecos de las personas (intimidad personal), que para algunos doctrinarios no tiene carácter de patrimonio. Es importante establecer que el Decreto no contempla los casos de delitos culposos, es decir, debe existir dolo (artículos 10, 11, 12 Código Penal).

<sup>67</sup> DECRETO NUMERO 33-96

El Congreso de la República de Guatemala,

CONSIDERANDO:

Que el Derecho es cambiante y debe adecuarse a las necesidades sociales, principalmente el Derecho Penal debido a que de su buena aplicación depende la protección de bienes jurídicos en apoyo a la convivencia pacífica;

CONSIDERANDO:

Que el actual Código Penal y sus Reformas, establece los tipos delictivos y las penas que han de aplicarse a quienes los cometan, haciendo falta la inclusión en el mismo de otros delitos que por afectar bienes públicos como el patrimonio histórico y el ambiente, deben ser regulados en la legislación penal;

CONSIDERANDO:

Que el país requiere de una adecuada regulación penal para evitar conflictos sociales derivados de las usurpaciones de tierras;

CONSIDERANDO:

Que los avances de la tecnología obligan al Estado a legislar en bien de la protección de derechos de autor en materia informática, tipos delictivos que nuestra legislación no ha desarrollado;

CONSIDERANDO:

Que nuestro sistema político se basa en la democracia, que se vuelve directa cada vez que los ciudadanos acuden a emitir sufragio, en manifestación de su voluntad, la cual debe ser protegida por nuestra legislación para evitar coacciones y fraudes electorales,

POR TANTO,

En uso de las facultades que le otorga la literal a) del Artículo 171 de la Constitución Política de la República,  
DECRETA:

Las siguientes:

REFORMAS AL DECRETO 17-73 DEL  
CONGRESO DE LA REPUBLICA,  
CODIGO PENAL.

ARTICULO 12. Se reforma el nombre del capítulo VII título VI, el cual queda así:

DE LOS DELITOS CONTRA EL DERECHO DE AUTOR, LA PROPIEDAD  
INDUSTRIAL Y DELITOS INFORMATICOS

Para analizar cada uno de los delitos en cuanto al bien jurídico tutelado que protegen, es necesario recordar que un Sistema de Información es el conjunto de elementos que tienen por objeto procesar datos e información para facilitar la toma de decisiones, o proporcionar un servicio. Los elementos que componen ese sistema de información (automatizado) son: el hardware (equipo de computación), el software (los programas de ordenador), los usuarios (personas que accedan al sistema), la información (el conjunto de datos) y la documentación técnica (manuales y guías de utilización y referencia).

Los delitos informáticos regulados en el Código Penal protegen los elementos de los sistemas de información en determinadas hechos, en otros puede ser un delito común y/o puede darse la situación de un concurso de delitos.

Los delitos informáticos establecidos en el Código Penal pueden clasificarse según el elemento del sistema que protegen, en: a) delitos que protegen los programas de computación<sup>68</sup>: alteración de programas (Art. 274 "B"), reproducción de instrucciones o programas de computación (Art. 274 "C") y programas destructivos (Art. 274 "G"); b) delitos contra las Bases de Datos: destrucción de Registros Informáticos (Art. 274 "A"); c) delitos contra la Información contenida en los Sistemas: uso de información (Art. 274 "F") y manipulación de información (Art. 274 "E"); y d) delito de la Información contenida en los Sistemas cuando afectan

la Intimidad de las Personas: registros prohibidos. (Art. 274 "D").

## 5. Los delitos informáticos en el Código Penal

Los delitos informáticos regulados en el Código Penal se describen por el bien jurídico protegido en la norma tipo, siguiendo el orden de la clasificación establecida en el punto anterior.

### 5.1. Delito de alteración de programas

El Decreto Número 33-96 en el artículo 14 adiciona el artículo 274 "B" el cual establece: Artículo 274 "B". Alteración de programas. La misma pena del artículo anterior se aplicará al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras.

En este artículo, se protege uno de los elementos de los sistemas de información como lo son las instrucciones o los programas de ordenador<sup>69</sup> (software), pero la protección es en cuanto a su funcionamiento. Al respecto, el legislador establece que la persona que inutilizare, es decir, dejar sin funcionar el programa. En cuanto a las instrucciones, considero que el legislador se refiere a que con dolo no se permita utilizar una o varias de las aplicaciones o funciones del programa de ordenador (inclusive podría ser un acceso).

<sup>68</sup> El Código Penal hace referencia a los Programas de Computación y la Ley de Derechos de Autor y Derechos Conexos a los Programas de Ordenador.

<sup>69</sup> Nótese que el Código Penal utiliza la denominación programas de computador, y la Ley de Derechos de Autor y Derechos Conexos el término programa de ordenador.

En cuanto al referirse a los programas, es que no funcionan en su totalidad o están “bloqueados”.

Existen ejemplos en la práctica, casos como las denominadas “bombas de tiempo”, que son programas que se adhieren en forma oculta a los programas de ordenador de los sistemas de información, para que en determinado tiempo o situación generen un bloqueo al funcionamiento del sistema, o impidan el acceso a los usuarios autorizados. En la mayoría de casos, son los administradores del sistema los que incurren en este ilícito, como alguna forma represiva contra la empresa; también se dan casos externos, pero llevan de por medio la comisión de otros ilícitos como estafa, chantaje o extorsión.

## 5.2. Delito de reproducción de instrucciones o programas de computación<sup>70</sup>

El Decreto Número 33-96 en el artículo 15 adiciona el artículo 274 "C" el cual establece: Artículo 274 "C". Reproducción de instrucciones o programas de computación. Se impondrá prisión de seis meses a cuatro años y multa

de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación.

En el artículo 274 "C" se protegen los derechos de autor y conexos del creador del programa de ordenador (se le denomina comúnmente el programador cuando es una persona individual) o la persona a quien cedió sus derechos.<sup>71</sup>

---

<sup>70</sup> La Ley de Derechos de Autor y Derechos Conexos, en el artículo 4 define:

Programa de ordenador: La obra constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma, que al ser incorporadas a un soporte legible por máquina, es capaz de hacer que un ordenador ejecute determinada tarea u obtenga determinado resultado.

<sup>71</sup> La Ley de Derechos de Autor y Derechos Conexos establece:

Artículo 5. Autor es la persona física que realiza la creación intelectual. Solamente las personas naturales pueden ser autoras de una obra; sin embargo, el Estado, las entidades de derecho público y las personas jurídicas pueden ser titulares de los derechos previstos en esta ley para los autores, en los casos mencionados en la misma.

Artículo 6. Se considera autor de una obra, salvo prueba en contrario, a la persona natural cuyo nombre o seudónimo conocido esté indicado en ella, o se enuncie en la declamación, ejecución, representación, interpretación o cualquier otra forma de difusión pública de dicha obra.

Cuando la obra se divulgue en forma anónima o bajo seudónimo no conocido, el ejercicio de los derechos del autor corresponde al editor hasta en tanto el autor no revele su identidad.

En materia de programas de ordenador<sup>72</sup> la persona (individual o jurídica) titular de los derechos de autor (morales, pecuniarios o patrimoniales, conexos) o sus herederos, tienen el derecho exclusivo a su reproducción, distribución, importación y exportación de copias, acceso, traducción, entre otros derechos.<sup>73</sup>

Lo anterior queda establecido en la ley especial y determinado en los contratos que celebre con quien ceda algunos de los derechos de que goza en su calidad de autor.

En la jerga informática, en el lenguaje comercial, en la publicidad de las empresas afectadas y en las campañas de prevención, se le denomina a este delito “Piratería”, pero en la legislación penal guatemalteca el delito de piratería se encuentra como un delito contra la

seguridad colectiva (Libro II, Título VII, Capítulo III, artículo 299, 230).<sup>74</sup>

Se puede establecer con base en la información y las estadísticas que proporcionan los medios de comunicación y los entes interesados, que este es el delito informático más cometido a nivel mundial y nacional. El acceso a equipo de computación y uso de la tecnología, facilitan la comisión de este delito; a ello le sumamos la falta de conocimiento en materia informática en aspectos técnicos y legales, el alto costo de algunos programas de ordenador y los errores en la redacción de los contratos de desarrollo y de licencia, aunque en principio ninguno de los aspectos indicados es causa de justificación para la comisión de este delitos cuando la conducta del sujeto activo encuadra en la norma tipo.

<sup>72</sup> La Ley de Derechos de Autor y Derechos Conexos establece:

Artículo 11. En los programas de ordenador se presume, salvo pacto en contrario, que el o los autores de la obra han cedido sus derechos patrimoniales al productor, en forma ilimitada y exclusiva, lo que implica la autorización para divulgar la obra y ejercer la defensa de los derechos morales en la medida en que ello sea necesario para la explotación del programa de ordenador.

Se presume, salvo prueba en contrario, que es productor del programa de ordenador la persona natural o jurídica que aparezca indicada como tal en el mismo.

<sup>73</sup> La Ley de Derechos de Autor y Derechos Conexos, en el artículo 4 define:

Copia ilícita: La reproducción no autorizada por escrito por el titular del derecho, en ejemplares que imitan o no las características externas del ejemplar legítimo de una obra o fonograma.

<sup>74</sup> Artículo 299.- (Piratería) Comete delito de piratería, quien practicare en el mar, lagos o en ríos navegables, algún acto de depredación o violencia contra embarcación o contra personas que en ella se encuentren, sin estar autorizado por algún Estado beligerante o sin que la embarcación, por medio de la cual ejecute el acto pertenezca a la marina de guerra de un Estado reconocido.

También comete delito de piratería:

- 1º Quien, se apoderare de alguna embarcación o de lo que perteneciere a su equipaje, por medio de fraude o violencia cometida contra su comandante.
- 2º Quien, entregare a piratas una embarcación, su carga o lo que perteneciere a su tripulación.
- 3º Quien, con violencia, se opusiere a que el comandante o la tripulación defienda la embarcación atacada por piratas.
- 4º Quien, por cuenta propia o ajena, equipare una embarcación destinada a la piratería.
- 5º Quien, desde el territorio nacional, traficare con piratas o les proporcionare auxilios.

El responsable de piratería será sancionado con prisión de tres a quince años.

Artículo 300. (Piratería aérea) Las disposiciones contenidas en el artículo anterior, se aplicarán a quien cometiere piratería Contra aeronaves o contra personas que en ellas se encuentren.



### 5.3. Programas destructivos

El Decreto Número 33-96 en el artículo 19 adiciona el artículo 274 "G" el cual establece: Artículo 274 "G". **Programas destructivos.** Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.

En este caso, se protege de los programas destructivos, fundamentalmente dos elementos de los sistemas de información<sup>75</sup> que son: los registros y los programas de ordenador (software)

En el ambiente informático y de las TIC existen unos programas denominados virus electrónicos, virus digitales, cibervirus, programas perjudiciales. Los virus se definen como los programas de ordenador que tienen por objeto introducirse en los sistemas informatizados para causar alguna clase de daño a la información, al sistema operativo, a los programas en general y se considera que algunos pueden llegar a dañar el hardware.

El Estado de Guatemala ha tratado de evitar responsabilidades en la administración de sus redes de computación a través de norma legal. El reglamento que determina las Normas para el Uso del Sistema de Información de Contrataciones

y Adquisiciones del Estado GUATECOMPRAS, en el artículo 17 establece:

**ARTÍCULO 17. Virus.** El Estado guatemalteco ha tomado medidas para prevenir ataques de virus electrónicos. Aún así, no acepta ninguna responsabilidad por cualquier daño causado por virus.

En cuanto al hecho ilícito cometido es importante determinar si existe responsabilidad penal o no, en virtud que la norma establece "al que distribuyere o pusiere en circulación(...)". Cuando una persona (autor) crea el virus informático no tiene responsabilidad penal, es decir, el simple hecho de crear un programa perjudicial no constituye delito. Cuando se distribuye, o se pone en una u otras computadoras, en una red interna o externa o la Internet, es cuando concurren todos los elementos de tipificación del delito, aunque no logre el daño que se tiene propuesto en virtud de detección y eliminación por un antivirus, o no ingresa a la red por medio de un firewall ("pared de fuego" o "cortafuego").

### 5.4. Destrucción de registros informáticos

El Decreto Número 33-96 en el artículo 13 adiciona el artículo 274 "A" el cual queda así: Artículo 274 "A". **Destrucción de registros informáticos.** Será sancionado con prisión de seis meses

<sup>75</sup> Como tercer elemento que protegen se encuentra:  
Los equipos de computación (hardware)

<sup>76</sup> Lamentablemente la redacción de la norma deja algunos vacíos en el concepto registro, pero se interpreta que se refiere a la información almacenada (datos, bases de datos).

a cuatro años, y multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizarse registros informáticos. La pena se elevará en un tercio cuando se trate de información necesaria para la prestación de un servicio público, o se trate de un registro oficial.

Se define como registro informático la base de datos creada por el sistema informático utilizada para la toma de decisiones.

El artículo establece el que “destruyere, borrare o de cualquier modo (...); destruir información significa que el sujeto responsable del hecho destruya la información, lo que equivale a cambiar su naturaleza de tal forma que no pueda recuperarse por medios electrónicos (el original instalado). Al establecer “borrare”, se refiere a eliminar en forma física en los dispositivos de almacenamiento la información; considero que se refiere a borrar cuando los archivos por medio de un software especial pueden ser recuperados. La frase “o de cualquier modo (...)” deja una amplia gama de posibilidades que puede exemplificarse en el caso que con intención se grabe información sobre la existente, o utilice algún dispositivo para afectar el acceso a los registros informáticos (no al programa).

El artículo también divide los registros en privados y públicos, considerando como un agravante cuando es contra los registros públicos. En ausencia de legislación que determine qué debe entenderse por registro público se interpreta que se refieren a los registros a cargo de la administración pública y que contienen datos personales. Otro criterio

establece que se refiere a la naturaleza de los datos o información, es decir, que los registros serán públicos aún cuando sean almacenados, procesados y/o automatizados por un ente privado.

### 5.5. Uso de información

El Decreto Número 33-96 en el artículo 18 adiciona el artículo 274 "F" el cual establece: Artículo 274 "F". Uso de información. Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos.

En este caso, la redacción del artículo vuelve a denotar la confusión o el poco conocimiento que se tenía en el año 1996 sobre esta materia, en virtud que en un mismo artículo se quieren regular dos situaciones diferentes. Podemos determinar que se protegen dos bienes jurídicos o derechos: los registros informáticos (en cuanto a su utilización no autorizada) y el acceso debidamente autorizado a los bancos de datos (bases de datos) o archivos electrónicos.

En el caso de los registros informáticos, la persona que crea una base de datos (lícita), dispone de quienes van a tener autorización para hacer uso de ellos. La utilización autorizada de los registros puede ser directa del computador que los tiene almacenados, en línea (red interna y externa), o pueden ser copiados para ser trasladados a otro equipo de cómputo; esto lo puede realizar una o varias personas autorizadas, incluso, un usuario

autorizado para acceder al sistema, pero no para utilizar en forma distinta los registros informáticos.<sup>77 - 78</sup>

Cuando un sujeto sin la autorización del titular de ese registro informático hace uso de él, estaría incurriendo en el delito establecido. La redacción es muy limitada y puede hacer incurrir al operador de justicia en errores. En el caso de utilizar esos registros informáticos en otro sistema de información automatizado, se estaría incurriendo en el delito establecido, le genere lucro o no. Se puede dar la situación que sea una persona quien "extrae" el registro y otra persona la que lo utilice en su sistema. Esto puede estar en concurso con otros delitos.<sup>79</sup>

Es importante considerar que no es el simple uso de ese registro lo que lo convierte en delito, en virtud que es necesario determinar algunas características de esa información (que sean datos automatizados) para establecer

si es ilícita o no esa conducta. Un ejemplo claro es cuando una persona visita un sitio web por motivos de investigación, trabajos académicos, estudios, y en su trabajo hace uso de un registro informático sin la autorización, pero hace la correspondiente referencia (cita bibliográfica)<sup>80</sup>.

Es diferente cuando se da el acceso no autorizado a los bancos de datos o archivos electrónicos. Para ingresar a un sistema de información se debe estar autorizado. La autorización de acceso es el permiso o anuencia que se le otorga a un usuario para poder hacer uso del sistema de información en el nivel establecido. El reglamento que determina las Normas para el Uso del Sistema de Información de Contrataciones y Adquisiciones del Estado GUATECOMPRAS, en el artículo 3 establece:

---

<sup>77</sup> El Código Tributario (Decreto Número 2-91 del Congreso de la República) establece:

Artículo 101. Confidencialidad. Las informaciones que la Administración Tributaria obtenga por cualquiera medios previstos en este Código, tendrán carácter confidencial. Los funcionarios o empleados de la Administración Tributaria no podrán revelar o comentar tales informaciones, ni los hechos verificados. Es punible revelar el monto de los impuestos pagados, utilidades, perdidas, costos y cualquier otro dato referente a las contabilidades y documentación de los contribuyentes.

Los funcionarios y empleados públicos que intervengan en la aplicación, recaudación, fiscalización y control de tributos, sólo pueden revelar dichas informaciones a sus superiores jerárquicos o a requerimiento de los tribunales de justicia, siempre que en ambos casos se trate de problemas vinculados con la administración, fiscalización y percepción de los tributos. No rige esta prohibición en los casos que los contribuyentes y responsables lo autoricen por escrito, con firma legalizada.

Los documentos o informaciones obtenidas con violación de este artículo, no producen fe, ni hacen prueba en juicio. Ver además: Código Tributario, Artículo 101 "A".

<sup>78</sup> Ver además: Código Tributario, Artículo 101 "A".

<sup>79</sup> Ver Código Penal Artículo 358 Competencia Desleal.

<sup>80</sup> ARTICULO 66. Será lícito, sin autorización del titular del derecho y sin pago de remuneración, con obligación de mencionar la fuente y el nombre del autor de la obra utilizada, si están indicados:...

d) Incluir en una obra propia, fragmentos de otras ajenas de naturaleza escrita, sonora o audiovisual, así como obras de carácter plástico, fotográfico u otras análogas, siempre que se trate de obras ya divulgadas y su inclusión se realice, a título de cita o para su análisis, con fines docentes o de investigación.

**ARTÍCULO 3.** Control y registro de usuarios. Los usuarios con perfil comprador, contralor y administrador deben estar previamente registrados en el sistema GUATECOMPRAS para poder utilizarlo. Los usuarios con perfil proveedor y público pueden acceder a GUATECOMPRAS sin necesidad de estar registrados en el sistema.

Un ejemplo de autorización y de niveles de acceso lo tenemos en el sistema bancario, en donde los trabajadores tienen autorización para ingresar a determinados niveles<sup>81</sup> del sistema; el cajero del banco tiene acceso para administrar información en la recepción o entrega de dinero (depósitos monetarios), pero no puede acceder a los estados de cuenta (ver saldo exacto); el jefe de la agencia bancaria sí tiene esta última competencia, pero no puede otorgar transferencias electrónicas por determinados montos y así consecutivamente (según esté diseñado el sistema).

Cuando el acceso al sistema lo realiza una persona que no está autorizada, se encuadra esa acción a este delito. Es importante señalar que el simple hecho de acceder sin autorización al banco de datos o archivos electrónicos constituye delito, incluso si no realiza ninguna acción con la información. Esto se conoce en doctrina como el delito de hacking.

## 5.6. Manipulación de información

El Decreto Número 33-96 en el artículo 17 adiciona el artículo 274 "E" el cual establece: Artículo 274 "E". Manipulación de información. Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilice registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.

Este delito contra la manipulación de la información lo comete el titular, propietario o usuario de los datos, cuando utilizando programas de computación, o registros informáticos diseñados para incumplir obligaciones con el Estado, o engañar a otras personas (empresas de crédito, inversionistas, clientes o usuarios) altera la información automatizada. Parte de dos supuestos: el primero, ocultar, se refiere a esconder los datos para que no puedan ser encontrados (archivos ocultos); el segundo, alterar o distorsionar, se refiere a cambiar los datos (unos por otros), o darle a los datos un valor distinto al real.

Además, debe determinarse el grado de participación de la persona que es autor (creador) del programa de computación que permite esa administración ilícita de la información, la participación de la persona que ingresa la información y la persona que la utiliza; en

---

<sup>81</sup> Es una escala jerárquica que se ha establecido a un sistema de información y que permite tener grados de acceso a la información, lo cual se determina según la competencia de cada usuario.

el caso del autor del programa, la norma establece “al que utilizare(...)”, si el programador se limita a diseñar el programa conforme la solicitud del contratante no tendría ninguna responsabilidad en virtud que él no lo utiliza. En cuanto a la persona que ingresa los datos, tampoco tendría responsabilidad, porque ingresar datos para esconderlos, duplicarlos o alterados, no es un delito. La persona que los utiliza, es decir realiza la acción de ponerlos en conocimiento del Estado, o de otra persona, es la que comete el acto ilícito. Si el que ingresa los datos tiene conocimiento posterior del hecho tipificado como delito tendría la calidad de encubridor, y si tiene conocimiento que van a ser utilizados con fines ilícitos tendría participación como autor o cómplice, según el caso.

#### 5.7. Registros prohibidos.

El Decreto Número 33-96 en el artículo 16 adiciona el artículo 274 "D" el cual establece: Artículo 274 "D". Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Para poder definir el bien jurídico que protege el artículo 274 "D" (la intimidad de la persona), es importante recordar las definiciones de datos personales y de intimidad, así como los derechos que resultan de ellos.

#### 6. Delitos cometidos utilizando las TIC como medio o instrumento

Es importante determinar la naturaleza del bien jurídico que se regula a través de los delitos informáticos. Algunos autores consideran los delitos informáticos en sentido estricto, es decir, aquellos que atentan contra bienes creados por la Informática y las TIC; en sentido amplio, se considera como delitos informáticos, los cometidos contra los bienes de origen informático, así como aquellos en los que se haga uso indebido de los sistemas de información y que por medio de esa acción, se atente contra otros bienes jurídicos que se encuentran regulados en otros capítulos del Código Penal, distintos a los derechos de autor, como puede ser la falsificación de documentos por medio de un equipo informático que lo reproduce por medio de la impresora, o delitos contra el honor por medio de una página web. Se deben considerar, incluso, conductas que en otros Estados se encuentra prohibidas, pero que en Guatemala todavía no están tipificadas como spam, fraude informático, subastas ilícitas.

Las múltiples aplicaciones de las TIC, en especial su máxima expresión, la Internet, al aplicarlas como medios de comunicación, acceso a la información, megared, etcétera, permite que a través de ellas (medio), o utilizándolas como recurso (herramienta), se pueda cometer una serie de delitos que afectan bienes jurídicos no informáticos, sino bienes jurídicos de otra naturaleza (patrimonio, honor, administración pública).

En los últimos meses, la sociedad guatemalteca, a través de los medios de comunicación, ha empezado a percatarse de hechos ilícitos o contrarios a las normas de la sociedad, realizados por medio de la Internet y en los que los bienes tutelados afectados no son de naturaleza informática, por ello no se les denomina como delitos informáticos.

Es importante aclarar que en la o por medio de Internet pueden realizarse las siguientes acciones: acciones o hechos ilícitos contra bienes informáticos, denominados en el Código Penal como delitos Informáticos; acciones o hechos ilícitos contra bienes no informáticos, los cuales podríamos denominar delitos comunes cometidos por medio de las TIC y/o Internet; y, acciones o hechos que a pesar de ser contrarios a las normas del buen convivir social, no son delitos en virtud de no estar expresamente establecidos como delitos.

En virtud de que en la Internet cualquier persona puede “subir” información o comunicarse con otros individuos, tanto la información en formato de texto, fotografía o video, así como las acciones que se realicen, pueden estar sujetas a prohibiciones por ley. En Guatemala, se ha tenido conocimiento de delitos cometidos por medio de las TIC desde hace años, pero solo hasta ahora se está tomando conciencia de su trascendencia; ejemplos como videos de menores de edad teniendo relaciones sexuales exhibidos y puestos a la venta en la Internet, subastas de bienes del patrimonio nacional o de bienes prohibidos, extorsiones o chantajes por medio del correo electrónico, son solo algunos ejemplos.

Algunas de las fases del iter criminis<sup>82</sup> se realizan por medios informáticos. Existen actos preparatorios (planificación, obtención de los recursos), que se realizan a través de las TIC, en especial, aquellos delitos denominados de mayor trascendencia como narcotráfico, trata de personas, terrorismo, pederastia. Otros en que la fase de ejecución se realiza utilizando medios electrónicos de comunicación como son las transferencias electrónicas para cometer el delito de lavado de activos, sin descartar el ciberterrorismo, e inclusive, la ciberguerra.

## 7. Otros delitos relacionados con las TIC

Existen derechos que surgieron como consecuencia del desarrollo de las tecnologías de la información y comunicaciones, y que (...) por ejemplo, el Decreto Número 57-2008 del Congreso de la República de Guatemala, Ley De Acceso A La Información Pública, establece:

**Artículo 64. Comercialización de datos personales.** Quien comercialice o distribuya por cualquier medio, archivos de información de datos personales, datos sensibles o personales sensibles, protegidos por la presente ley sin contar con la autorización expresa por escrito del titular de los mismos y que no provengan de registros públicos, será sancionado con prisión de cinco a ocho años y multa de cincuenta mil a cien mil Quetzales, y el comiso de los objetos instrumentos del delito.

La sanción penal se aplicará sin perjuicio de las responsabilidades

<sup>82</sup> Iter Criminis: Se le denomina así en doctrina penal a la serie de fases o etapas del delito que inician en la mente del sujeto activo y que concluye con la consumación del hecho ilícito.

civiles correspondientes y los daños y perjuicios que se pudieran generar por la comercialización o distribución de datos personales, datos sensibles o personales sensibles.

**Artículo 65. Alteración o destrucción de información en archivos.** Quien sin autorización, altere o destruya información de datos personales, datos sensibles o personales sensibles de una persona, que se encuentren en archivos, ficheros, soportes informáticos o electrónicos de instituciones públicas, será sancionado con prisión de cinco a ocho años y multa de cincuenta mil a cien mil Quetzales.

La sanción penal se aplicará sin perjuicio de las responsabilidades civiles correspondientes y los daños y perjuicios que se pudieran generar por la alteración o destrucción de información en archivos.

## 8. El cibercrimen

El ámbito espacial en los delitos tecnológicos es sumamente importante, en especial por las múltiples formas de comunicación que establece Internet; al respecto el Código Penal establece el principio al territorio de Guatemala: Salvo lo establecido en tratados internacionales, este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción. (Artículo 4)

El problema en el ambiente de las TIC es que la comunicación y relaciones no son solo de carácter nacional, también son internacionales, es decir fuera de las fronteras de Guatemala y por ende algunos hechos ilícitos son cometidos en un lugar distinto al territorio de Guatemala (en el ciberspacio).

### 9. Proyectos o iniciativas de ley con relación a los delitos informáticos

Existe una serie de acciones que realizan las personas en el ámbito de las TIC y que no son constitutivas de delitos en Guatemala, por no estar expresamente prohibidas en virtud del principio de legalidad; en otros Estados, estas conductas se encuentran tipificadas como delitos, en virtud que algunas afectan a los sujetos, ya sea el usuario, el proveedor de servicios, o incluso, a los servidores; la afectación puede ser patrimonial, o contra sus derechos a la intimidad entre otros; ejemplo de ello son el Spam o envío masivo de correos electrónicos no solicitados, el Spyware que consiste en introducir programas que posteriormente enviarán la información sustraída del sistema al sujeto que lo instaló, el denominado phishing por la idea de “pescar” información en la Internet a través de correos electrónicos o formularios y que en muchos casos tiene por objeto “robar la identidad” de las personas.

Además, existen otras conductas ilícitas que han tenido variaciones relevantes al ejecutarse por Internet, como el fraude informático, robo informático, subastas ilegales, publicaciones obscenas<sup>83</sup> o pornografía infantil, entre otros.

<sup>83</sup> El delito de Publicaciones y Espectáculos Obscenos se encontraba establecido en el artículo 196 del Código Penal Decreto Número 17-73 del Congreso de la República. En el año 2002 fue reformado por el Decreto Número 27-2002; posteriormente quedó sin vigencia por sentencia de Inconstitucionalidad Expediente Número 1021-2002, sentencia de fecha 29/5/2003, publicada en el Diario Oficial el 26/6/2003.

En el Congreso de la República de Guatemala, existen actualmente dos iniciativas de ley que tienen por objeto, tipificar conductas delictivas realizadas por medio de las TIC.

#### 9.1. Iniciativa de ley contra el cibercrimen

La iniciativa de Ley contra el Cibercrimen (Cybercrime) identificada con número 4054 fue conocida por el Pleno del Congreso de la República el día dieciocho de agosto de dos mil nueve. Dentro de la exposición de motivos de la iniciativa de ley en mención, se menciona lo siguiente: “que con el crecimiento exponencial de usuarios de Internet, se abre la puerta a la comisión de un mayor número de “ciberdelitos(...)” lo que remarca la importancia de contar con medidas especiales de prevención, detección e inicio de acciones judiciales contra los “ciberdelincuentes”. A diferencia de otros delitos, el “cibercrimen cuenta con características distintivas comunes como son la novedad, la potencialidad lesiva, la cualificación técnica del autor, su dimensión transnacional, su constante evolución y, derivado de todo ello, la dificultad de su persecución (...).” (2009)

A medida que se incrementa el uso de Internet como medio para realizar transacciones on-line en las que los usuarios deben indicar datos personales, los ciberdelincuentes buscan la forma de acceder a esa información con el objetivo de utilizarla posteriormente, ya sea con fines lucrativos o de otra índole. La ciberdelincuencia ha evolucionado en forma notable en los últimos años; de los hackers tradicionales la amenaza ha pasado a grupos de delincuentes que utilizan la más alta tecnología que hay a su alcance para

llevar a cabo ciberdelitos organizados, sistemáticos y complicados de poder perseguir.

Derivado de lo anterior, surge la necesidad de que en nuestro país se cree una normativa legal que tipifique y regule las distintas conductas contrarias a derecho realizadas a través de la Internet, así como también que se establezcan los medios de investigación especial que han de aplicarse para la averiguación de un hecho delictivo cometido en estas circunstancias.

La iniciativa de ley indicada contiene una serie de delitos que aún no se encuentran regulados dentro de la Legislación Penal guatemalteca, tales como Códigos de acceso, clonación de dispositivos de acceso, acceso ilícito, acceso ilícito para servicios a terceros, dispositivos fraudulentos, interceptación e intervención de datos o señales, daño o alteración de datos, sabotaje, atentado contra la vida de la persona, robo mediante la utilización de alta tecnología, obtención ilícita de fondos, estafa especial, chantaje especial, robo de identidad, falsedad de documentos y firmas, uso de equipos para invasión de privacidad, comercio ilícito de bienes y servicios, difamación especial, injuria pública, atentado sexual, pornografía infantil, delitos relacionados con la Propiedad Intelectual y afines, y delitos de telecomunicaciones.

Entre las propuestas de la iniciativa se encuentra crear una Comisión contra Crímenes y Delitos de Alta Tecnología (CDAT), la cual tendrá como finalidad coordinar y cooperar con gobiernos e instituciones nacionales y extranjeras para prevenir y reducir la comisión de actos ilícitos de alta tecnología en la República de Guatemala y en el resto del mundo.

## 9.2. Iniciativa de Ley de delitos informáticos

La iniciativa denominada Ley de Delitos Informáticos fue conocida por el Pleno del Congreso de la República el día dieciocho de agosto de dos mil nueve e identificada con número 4055. El objeto de esta iniciativa de ley es la regulación de normas especiales que protejan todo lo relativo con la información, siendo ésta, el bien jurídico tutelado por la presente iniciativa de ley; y que se sancionen todos aquellos actos ilícitos de naturaleza informática que sean cometidos en Guatemala o que surtan efectos jurídicos en su territorio.

La iniciativa de ley de Delitos Informáticos pretende establecer un marco regulatorio sobre posibles usos indebidos que perjudican transacciones y comercio electrónico. Asimismo, contempla definiciones legales propias para el tema de cibercrimen y desarrollo de la normativa pertinente para sancionar, entre otros, los actos de hacking (acceso sin autorización), cracking (daño o sabotaje), phishing, smishing, vishing (invitación de acceso a sitios o sistemas informátivos falsos o fraudulentos) y pornografía infantil.

Esta iniciativa de ley tipifica los siguientes delitos informáticos: acceso sin autorización, daño informático, posesión de equipos, o prestación de servicios para daño informático, fraude informático, uso fraudulento de tarjetas inteligentes, o instrumentos análogos, provisión indebida de bienes o servicios, posesión de equipo para falsificaciones, falsificación informática, invitación de acceso, pornografía infantil, y alteración de imágenes.

Es importante establecer que no por el hecho de cometer delitos utilizando computadoras, redes, o la Internet, se convierte en delitos informáticos (en sentido estricto). Por ejemplo, si una persona coloca un sitio web que simula ser una empresa que ofrece alguna clase de servicios y con ardid o engaño un usuario efectúa un pago económico por el supuesto servicio, el delito sigue siendo una estafa; si utiliza una computadora y una impresora para falsificar una certificación del Registro General de la Propiedad, el delito sigue siendo falsificación; si un individuo lanza un teclado a otro y le provoca una contusión u otra clase de daño físico, el delito es lesiones. No por el hecho de utilizar un instrumento propio de la informática se convierte en los denominados delitos informáticos; hoy en día muchos de los delitos denominados comunes utilizan como instrumento a una computadora o las TIC. Además, puede suscitarse que al cometer alguno de los delitos comunes, se encuentre en concurso con los delitos informáticos, como podría ser cometer un delito informático necesario para cometer un delito común.

Lo que es necesario reformar son los denominados, en el Código Penal, como delitos informáticos, actualizando la redacción (en el supuesto de hecho) a las situaciones prohibidas. Además, se deberán prohibir determinadas conductas que actualmente no se establecen en materia penal y que afectan, no solo a los bienes informáticos, sino a todos los bienes jurídicos que debe tutelar el Estado.



Introducción de las nuevas tecnologías en el derecho  
Instituto de la Defensa Pública Penal



## EJERCICIOS DE AUTOAPRENDIZAJE

- 1) Realizar un análisis de Derecho Comparado con las legislaciones de naturaleza penal de los Estados Centroamericanos.
- 2) Lea el Convenio Sobre la Ciberdelincuencia de la Unión Europea y determine qué conductas se consideran ilícitas y que no se encuentran reguladas en Guatemala. Posteriormente, coteje su resultado con las iniciativas de ley existentes en el Congreso de la República de Guatemala.



## BIBLIOGRAFÍA



Acosta, Miguel citado por Reyes, Alfredo (2003);  
La Firma Electrónica y las Entidades de Certificación;  
México.

Agencia Española de Protección de Datos (2009);  
[www.agpd.es](http://www.agpd.es).

Asociación de Usuarios de Internet (2000);  
Madrid, España; [www.aui.es](http://www.aui.es).

Barrios, Omar (2007);  
Derecho e Informática, Aspectos Fundamentales,  
Guatemala.<sup>84</sup>

Calderón, Cristian (2000);  
Perú: El Impacto de la Era Digital en el Derecho;  
Revista Electrónica de Derecho Informático No. 21;  
s/p; Perú.

Cámpoli, Gabriel (2004);  
Derecho Penal Informático en México; Instituto  
Nacional de Ciencias Penales, México.

Carnelutti, Francesco (2000).  
La Prueba Civil. Argentina.

Davara, Miguel (2006).  
Manual de Derecho Informático, Madrid, España.

Diccionario de Informática (1995);  
Equipo Dos; Acento Editorial; Madrid, España.

Elías, Miguel (2001);  
Situación legal de los datos de carácter personal  
frente a las nuevas tecnologías; Revista Electrónica  
de Derecho Informática; Buenos Aires, Argentina.

---

<sup>84</sup> Un porcentaje de los contenidos brindados en el presente módulo fueron extraídos de la obra indicada, sin que por ello se renuncie a los derechos de autor correspondientes al autor de la obra original.

- Hance, Olivier (1996);  
Leyes y Negocios en Internet; McGraw-Hill; Página (181); México.
- Hernández, Victor (2000).  
El Derecho Administrativo en la Sociedad de la Información. UNAM, México.
- Herrera, Rodolfo (2000);  
El Derecho en la Sociedad de la Información: Nociones Generales sobre el Derecho de las Tecnologías de la Información y Comunicaciones; Chile.
- Iñigo de la Maza y Cruz (2004);  
Contratos por adhesión en la plataformas electrónicas; Chile.
- Llamas, Manuel y Gordillo, José (2007).  
Medios Técnicos de Vigilancia. Madrid, España.
- Maresca, Fernando (2007);  
Aspectos Jurídicos del Software Libre, Buenos Aires, Argentina
- Morton, Scout; citado por Andrea Viviana Sarra (2001);  
Comercio Electrónico y Derecho; Buenos Aires, Argentina.
- Oliver, Daniel (2007).  
Comunicaciones Comerciales, Privacidad y Derecho en la Sociedad de la Información. Buenos Aires, Argentina.
- Proyecto de guía para la incorporación al derecho interno del Régimen Uniforme de la CNUDMI (UNCITRAL) para las Firmas Electrónicas.
- Proyecto de guía para la incorporación al derecho interno del Régimen Uniforme de la CNUDMI (UNCITRAL) para las Firmas Electrónicas.

- Real Academia Española (2009);  
[www.rae.es.](http://www.rae.es)
- Ramos Fernando (2000);  
Como Aplicar la Nueva Normativa sobre Firma Electrónica; Madrid, España.
- Ramos, Fernando (2002);  
La Firma Digital: Aspectos técnicos y legales.
- Rojas, Victor. (2000);  
El Uso de Internet en el Derecho; México D. F.
- Rico, M. y Herrera, R. (2007).  
Derecho de las Nuevas Tecnologías. Argentina
- Pérez, Antonio (1996);  
Manual de Informática y Derecho; Editorial Ariel;  
España.
- Pérez, Antonio (2001);  
Ensayos de Informática Jurídica; D. F. México, 2001.
- Política uniforme de solución de  
controversias en materia de nombres  
de dominio, (2009);  
Corporación de Asignación de Nombres y Números  
de Internet; [www.gt](http://www.gt).
- Téllez, Julio (2004);  
Derecho Informático; México.
- Rebollo, Lucrecio (2008).  
Introducción a la Protección de Datos; Madrid,  
España.
- Remolina, Nelson (2007).  
Protección de Datos en Entornos Electrónicos;  
Buenos Aires, Argentina.
- Sarra, Andra (2001);  
Comercio electrónico y derecho; Buenos Aires,  
Argentina.

Tomas y Valiente, citado por Alfredo Reyes (2003);  
La Firma Electrónica y las Entidades de Certificación; México.

Tembourg, Miguel (2000);  
Derecho de Internet: La prueba de los documentos electrónicos en los distintos órdenes jurisdiccionales; España.

Wikipedia (2009);  
[www.wikipedia.org](http://www.wikipedia.org)

## ANEXOS



Los anexos que se adjuntan son sugeridos a consideración de las autoridades del IDPP; ello en virtud de los derechos de autor de los videos adjuntos.

Iniciativa de Ley contra el Cibercrimen (Cybercrime) número 4054  
[www.congreso.gob.gt](http://www.congreso.gob.gt)

Iniciativa de Ley de Delitos Informáticos número 4055.  
[www.congreso.gob.gt](http://www.congreso.gob.gt)

Ley para el Reconocimiento de Comunicaciones y Firmas Electrónicas  
<http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativa/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2008/pdfs/decretos/D047-2008.pdf>

Warriors of the net (Video)  
Derechos de autor: Elam, G; Stephanson, T; Hanberger, N. All Rights Reserved.  
Copyright 2002.  
<http://warriorsofthe.net/movie.html>

La Firma Digital (video)  
Derechos de autor: Firma Digital Argentina ()  
Accesible en: [http://www.youtube.com/watch?v=x0A\\_NWyt2E](http://www.youtube.com/watch?v=x0A_NWyt2E)

La Agenda Nacional de la Sociedad de la Información y el conocimiento de Guatemala  
[www.concyt.gob.gt](http://www.concyt.gob.gt)

Este módulo se terminó  
de imprimir en enero de 2011  
La edición consta de 600 ejemplares



INSTITUTO DE LA DEFENSA  
PÚBLICA PENAL



UNIFOCADEP