DERECHO INFORMÁTICO

MANUEL ZOMETA

DERECHO INFORMÁTICO

Manuel Zometa

A la memoria de mi amigo Daniel Herrera...

INDICE

INTRODUCCION

El derecho de la informática, surge frente a la evolución de la misma como una disciplina que se enfoca en el tratamiento automático de la información; especialmente, en las relaciones que se establecen producto del tránsito automatizado de dicha información.

Para entender esta relación, hay que tener presente aquellos puntos importantes, en los cuales tanto derecho como la informática coadyuvan, dentro de los aspectos de la sociedad actual. pues dentro de todas las relaciones humanas existe una relación de derecho o se encuentran en contacto con algún aspecto axiológico del derecho pues éste es un regulador de la conducta, y cuando estas relaciones se llevan a cabo por medios informáticos, nacen nuevas conductas que deben ser reguladas.

Por otro lado, el constante desarrollo de la tecnología ha permitido que casi todos los aspectos de nuestra vida en sociedad estén vinculados a la informática, como producto de la sistematización de la

información creando cada vez nuevas formas de relaciones humanas. En ese sentido a lo largo de este estudio se entenderá como **DERECHO:** todas aquellas normas derivadas de la conducta humana que sirven para regular las relaciones entre dos o mas sujetos, entre los sujetos y el Estado, y entre sujetos y las cosas. Así mismo, para fines de este texto se entenderá por **INFORMÁTICA:** *"el tratamiento automático de la información a través de elaboradores electrónicos basados en las reglas de la cibernética"* acuñando el término planteado por Elías Gustavino[1]

Entonces en cuanto al tema en análisis, se pretende estudiar la vinculación que tiene el Derecho como regulador las relaciones humanas con el de la informática en aquellos puntos de coincidencia, de ahí que el vocablo derecho que antecede al término informático está orientado a aquellos factores que integran la idea de informática, (elaboradores electrónicos, cibernética, telemática, redes, etc.) en su aplicación a las relaciones humanas en el sentido axiológico y deóntico del derecho o vinculadas a este, de

[1] GUSTAVINO Elías, "Responsabilidad civil y otros problemas jurídicos en computación. Ed. La Rocca, 1987.

ahí el surgimiento de la categoría: **derecho informático.**

De este modo, en un sentido amplio se concibe el concepto de derecho informático. como: “el tratamiento sistemático y normativo tendiente a regular la informática en sus múltiples aplicaciones (burótica, robótica, telemática etc.)”. tal como lo plantea Felipe Rodriguez.[2] De esta definición se puede identificar que no existe un solo punto coincidencia entre el derecho y la informática, pues esta relación esta determinada por la complejidad misma de las relaciones sociales; Sin embargo, en este texto se aborda una parte específica de estas relaciones, que es aquella relacionada con los derechos de propiedad intelectual sobre las nuevas tecnologías de la informática, tal como el Software y Hardware. En particular, examina las implicaciones de la legislación salvadoreña en las relaciones económicas e intelectuales de los formatos de software "propietarios" y "libres" en sentido de su protección con derechos de autor, y estudia la protección del

[2] RODRIGUEZ Felipe. “Lecciones de derecho y ética para ingenieros, estudiantes de ingeniería y profesiones afines”. Libro VII Derecho informático. UNC, Argentina 2013. p. 13

hardware desde la perspectiva de la protección de la propiedad industrial.

Posteriormente trata sobre los delitos informáticos, haciendo una valoración de la clasificación de la ONU y de la Ley Especial Contra Delitos Informáticos y Conexos de El Salvador, como una forma de regulación de la conducta delictiva realizada por medios informáticos.

Luego del análisis de las relaciones entre el derecho penal y la informática, se hace un abordaje breve sobre la relación entre el derecho probatorio y la informática, especialmente en la parte de los peritajes informáticos, proponiendo una redacción estandarizada del dictamen pericial informático.

Finalmente, se realiza un análisis de la vinculación entre el derecho contractual con la informática, referido específicamente a la contratación civil y mercantil, ya sea en compraventa de bienes y prestaciones de servicios informáticos, y otro tipo de contratos conmutativos regulados en el código civil salvadoreño.

Capítulo I

Derecho a la propiedad intelectual

La legislación orientada a la protección de la propiedad intelectual es uno de los marcos jurídicos más extensos del Derecho, tiene presencia tanto en el derecho internacional como en el derecho interno y es conocido dentro de esta ultima área adquiere características especiales y procesos específicos para su protección.

El concepto de propiedad intelectual es abordado en sentido amplio por la Organización Mundial de la Propiedad Intelectual (OMPI) como:

"T*oda creación del intelecto humano. Los derechos de Propiedad Intelectual. protegen los intereses de los innovadores y creadores al ofrecerles prerrogativas en relación con sus creaciones."*[3]

El Convenio que establece la Organización Mundial de la Propiedad Intelectual de 1967 plantea una

[3] Organización Mundial de la Propiedad Intelectual. (2016). *Principios básicos del derecho de autor y los derechos conexos* (2nd ed., Vol. 1, ISBN: 978-92-805-2801-5). Ginebra, Suiza: OMPI. Atribución de licencia 3.0 IGO (CC BY 3.0 IGO) p3.

lista detallada de las producciones y descubrimientos que pueden ser protegidos por derechos de propiedad intelectual, dentro de los cuales se encuentran:

- las obras literarias, artísticas y científicas;
- las interpretaciones de los artistas intérpretes y
- las ejecuciones de los artistas ejecutantes,
- los fonogramas y las emisiones de radiodifusión;
- las invenciones en todos los campos de la actividad humana;
- los descubrimientos científicos;
- los diseños industriales;
- las marcas de fabrica, de comercio y de servicio y los nombres y denominaciones comerciales;
- la protección contra la competencia desleal; y
- "todos los demás derechos relativos a la actividad intelectual en los terrenos industrial, científico, literario y artístico".

La protección de la propiedad intelectual, surge primeramente como un **derecho reconocido a nivel internacional** en el *Convenio de París para la Protección de la Propiedad Industrial* de 1883[4] y posteriormente en el *Convenio de Berna para la Protección de las Obras Literarias y Artísticas*[5], de 1886. de los cuales la Organización Mundial de la Propiedad Intelectual es depositaria y actual administradora. Según la OMPI existen dos razones fundamentales que expresan la necesidad que los países promulguen una diversidad de leyes para la protección de la Propiedad Intelectual siendo estas las de:

• *"Amparar en la legislación, los derechos de los creadores y los innovadores sobre sus creaciones e innovaciones, de manera equilibrada con respecto al interés público de acceder a las creaciones y las innovaciones;*

• *fomentar la creatividad y la innovación, contribuyendo así al desarrollo económico y social*."

[4] Organización Mundial de la Propiedad Intelectual (n.d.). Convenio de París para la Protección de la Propiedad Industrial. October 03, 2017, from http://www.wipo.int/treaties/es/text.jsp?file_id=288515

[5] Organización Mundial de la Propiedad Intelectual . (n.d.). Convenio de Berna para la Protección de las Obras Literarias y Artísticas. Retrieved October 03, 2017, from http://www.wipo.int/treaties/es/text.jsp?file_id=283698

Desde la perspectiva del **derecho interno**, específicamente en El salvador, la protección de la propiedad intelectual esta recogida en la *Ley de fomento y protección de la propiedad intelectual*[6] que está en vigencia desde el 15 de julio de 1993, poco menos de 100 años después de su reconocimiento a nivel internacional, y abarca dos grandes áreas: **La propiedad artística, literaria o científica** y **la propiedad industrial**, haciendo uso de los preceptos planteados desde el derecho internacional con la convención de París y Berna; El derecho de propiedad intelectual entonces ha sido concebido en dos ramas principales que son: **El derecho de autor** y **la propiedad industrial.**

Los derechos de autor

De acuerdo con la OMPI el derecho de autor es aplicable a todas las creaciones artísticas, literarias y científicas, que pueden estar expresadas en libros, obras musicales, pinturas, esculturas, películas etc. también se consideran aquellas obras aquellas que no se clasifican como artísticas ni académicas, pueden ser aquellas que

[6] Decreto numero 604 de la Asamblea Legislativa de El Salvador

constituyen dibujos no industriales ni planos, pero se consideran como una obra arquitectónica, o son realizadas como producto de los avances tecnológicos, especialmente respecto de las computadoras como los programas informáticos (Software) y las bases de datos electrónicas.

La legislación salvadoreña considera al software **como obra literaria** debido a que lleva implícita una **acción semántica y sintáctica**; a pesar que no considera a las bases de datos como tal; El artículo 32 de la Ley de fomento y protección de la propiedad intelectual establece lo siguiente que:

"*Programa de ordenador, ya sea programa fuente o programa objeto, es la obra literaria constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador, o sea, un aparato electrónico o similar capaz de elaborar informaciones, ejecute determinada tarea u obtenga determinado resultado*."

Por lo tanto, todos los códigos utilizados para el desarrollo de material informático, son sujetos de protección de derechos de autor y no de derechos de propiedad industrial como erróneamente se cree.

El artículo 2 del Convenio de Berna estipula que : “Los términos ‘obras literarias y artísticas: comprenden todas las producciones en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión”.

y posteriormente en el convenio se encuentran los siguientes ejemplos de obras de esa índole:

“libros, folletos y otros escritos;

- conferencias, alocuciones, sermones;
- obras dramáticas o dramático musicales;
- obras coreográficas y pantomimas;
- composiciones musicales con o sin letra;
- obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía;

- obras de dibujo, pintura, arquitectura, escultura, grabado, litografía;
- obras fotográficas, a las cuales se asimilan las expresadas por procedimiento análogo a la fotografía;
- obras de artes aplicadas; ilustraciones, mapas, planos, croquis y obras tridimensionales relativas a la geografía, la topografía, la arquitectura o las ciencias;
- Estarán protegidas como obras originales, sin perjuicio de los derechos del autor de la obra original, las traducciones, adaptaciones, arreglos musicales y demás transformaciones de una obra literaria o artística"; y
- las colecciones de obras literarias o artísticas tales como las enciclopedias y antologías que, por la selección y la disposición de las materias, constituyan creaciones intelectuales, estarán protegidas como tales, sin perjuicio de los derechos de los autores sobre cada una de las

obras que forman parte de esas colecciones, según se dispone en el Convenio."

Sin embargo, para fines del presente texto nos limitaremos a abordar las concepciones jurídicas del software como objeto de protección por derechos de autor y del hardware como objeto de protección por patentes y otros.

Los derechos morales y patrimoniales

El derecho de autor es conocido también por su nombre en ingles copyright que se deriva etimológicamente de las palabras "copiar" y "derecho", lo que expresa en sí mismo una connotación de los derechos que el autor puede ejercer sobre su obra, así, el desarrollador de un código es reconocido moralmente como el dueño del mismo, más no lo es de las herramientas con las que creó su código ni de los productos resultantes de la aplicación del programa que funciona con su código. En este caso el desarrollador puede copiar u otorgar permisos para su reproducción, a esto se le llama otorgamiento de licencia, como lo hace Windows respecto de sus productos.

En este sentido, el derecho de autor es ejercido solamente por la persona o personas creadoras de una obra informática (código o base de datos), como se reconoce en la mayor parte de las legislaciones, y es el autor quien a partir de este derecho, comienza a gozar de derechos más específicos sobre sus creaciones, los cuales se denominan, tanto a nivel internacional como en El Salvador como derechos morales, que son según Ulises Hernandez[7] los que confieren:

"...el reconocimiento de la paternidad del autor sobre la obra realizada y el respeto a la integridad de la misma. Este derecho otorgan al autor facultades para:

1. Exigir que su nombre y el título de la obra sean mencionados cada vez que ésta se utilice, publique o divulgue;
2. Oponerse a las transformaciones o adaptaciones de la misma si esto afecta su buen nombre o reputación;

[7] Pino, U. H. (28 de mayo 2012). El Derecho de Autor en la Era Digital: Derechos Morales y Patrimoniales en el Derecho de Autor. Visitado el 05 de Octubre, en http://www.iered.org/miembros/ulises/representacion-ideas/Derechos Autor/derechos_morales_y_patrimoniales_en_el_derecho_de_autor.html Grupo de Investigación GEC Red de Investigación Educativa - ieRed Universidad del Cauca

3. Dejar la obra inédita o publicarla en forma anónima o bajo un seudónimo;

4. Modificar la obra en cualquier tiempo y retirarla de la circulación, previo el pago de las indemnizaciones a que haya lugar."

Así también se reconoce como derecho moral, el derecho a impedir la reproducción deformada del código o base de datos, es decir, aquel tipo de reproducción con alguna variante, pero que no afecte la esencia de la obra como en los casos de la piratería.

Los derechos morales se denominan así por que surgen junto con la creación de la obra, sin necesidad de registro, es decir que se reconoce la autoría sobre la obra desde que se encuentra en desarrollo por su creador, por eso se considera que se tiene derecho moral sobre las bases de datos aun que no se encuentren detalladas en la legislación salvadoreña.

Otro de los derechos específicos dentro del derecho de autor son los derechos patrimoniales que en sentido amplio es el derecho que tiene el autor de una obra de lucrarse de los beneficios que su obra produzca, estos beneficios son en general monetarios, y la

legislación salvadoreña los denomina "derechos pecuniarios" por la susceptibilidad de ser otorgados también, como garantía para determinadas obligaciones (prendas, hipotecas, pagos etc.). Según el autor en cuestión los derechos patrimoniales son aquellos que otorgan:

"*...la facultad de aprovecharse y de disponer económicamente de la obra por cualquier medio, por tanto se puede renunciar a ellos o embargarse, son prescriptibles y expropiables*."

También, estas facultades se ejercen cuando el autor otorga derechos de reproducción, distribución, alquiler e importación de su obra o derechos de interpretación, traducción adaptación, ejecuciones públicas, radiodifusión comunicación al público y de puesta a disposición publica; por la cual recibe una remuneración a cambio de lo que se denomina generalmente, un contrato de licencia.

La protección del Software

La forma más general de categorizar el software respecto al dominio, los patrones de uso y sus implicaciones de propiedad intelectual es dividirlo en

dos grandes categorías: (a software patentado; (b Software Libre o de Código Abierto. Nótese que el "software patentado" es solo el nombre de la clasificación pues el software adquiere protección de derechos de autor o Copyright y no de patentes.

El Software propietario

Como su nombre lo indica, el software propietario, privativo o patentado es un software de propiedad privada de una empresa (u ocasionalmente de un desarrollador de software individual). Su "propiedad privada" está protegida por varias leyes y regímenes de propiedad intelectual y por las licencias requeridas para su uso. Proteger (o no) el código fuente (el lenguaje de programación interno del software) está en el centro de la mayoría de los debates legales, políticos y prácticos sobre el software. El problema abarca tanto los programas del sistema operativo (por ejemplo, Windows), que administran la función interna de la computadora, como los programas de aplicación (por ejemplo, Microsoft Word, juegos, hojas de cálculo y otros procesadores de texto) que realizan tareas específicas de procesamiento de datos para los usuarios.

El código de un programa es lo que lo hace particularmente valioso y lo transforma, potencialmente al menos, en una herramienta creativa que puede usarse para resolver una variedad de problemas y actúa como un catalizador o un bloque de construcción para futuros desarrollos y nuevas aplicaciones. En otras palabras, el código fuente es lo que hace que el software sea una tecnología "viva" y adaptable capaz de mejorarse y modificarse, y no simplemente una solución informática fija y preempaquetada, no adaptable.

Por supuesto, el usuario de la computadora "promedio" no está interesado en obtener acceso al código fuente de un programa o en aprender a editar ese código. Pero muchos otros están interesados, y a menudo deben tener acceso al código fuente. Aquellos que realmente operan redes y sistemas de computadoras, ya sea en negocios, gobierno, instituciones educativas u organizaciones comunitarias, y aquellos con las habilidades necesarias en programación y escritura de software requieren acceso al código fuente y la capacidad ilimitada de modificarlo

para que el software comprado o personalizado funcione para sus necesidades específicas.

Con el software patentado, esto no es posible, a menos que el propietario otorgue licencias o permisos especiales en base a las leyes de propiedad intelectual nacionales e internacionales. Por lo tanto debe estar dentro del marco legal que restringe dicho acceso. Sin embargo, también se pueden establecer ciertas distinciones entre tipos algo diferentes de software libre: ya que puede ser software gratuito[8] o software de código abierto. (OSS).

En el caso del software privativo, estas restricciones clave se manifiestan por los términos de licencia particulares que aquellos que realmente licencian o que operan el software deben cumplir, nuevamente como una cuestión de ley. El software rara vez se vende, sin embargo se puede comercializar bajo los términos del llamado "Contrato de licencia de usuario final" que se aborda en la parte de derecho

[8] El software gratis (en inglés free software) significa en algunos casos que puede ser modificado, aunque en realidad esta denominación también puede significar que es gratis, y no necesariamente libre, por lo que se utiliza el hispanismo “libre” también en inglés) que es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, cambiado y redistribuido libremente.

contractual, este código fuente no puede ser copiado, compartido, modificado, redistribuido o modificado por otros desarrolladores o usuarios de software.

En la misma línea y como parte clave del modelo comercial del software propietario, la licencia generalmente permite el uso del software **en una sola computadora** y probablemente exigirá el pago de una licencia adicional por cada computadora adicional o estación de trabajo ("workstation") que utilice el software. Hay que tener en cuenta que el código utilizado para los programas de aplicación, que constituyen la mayor parte de los programas informáticos actuales, debe ser compatible con el código que se encuentra en el sistema operativo (OS). El problema entonces comienza a profundizar porque la mayoría de los sistemas de hardware vienen "precargados" con varios tipos de software patentado; el costo de dicho software está integrado en el precio de compra del sistema.

Dado el aumento dramático en el uso de computadoras en la última década, al menos en los países industrializados más ricos, y teniendo en cuenta

los recursos que provienen intrínsecamente de la "propiedad" del código, especialmente para un sistema operativo como Windows que se ha convertido en el estándar mundial, comienza a aclarar cómo el software de protección de fuente cerrada y propiedad intelectual puede llegar a representar una fuente importante de riqueza y poder. Por ejemplo, en 2004 el contrato para proporcionar software para el Servicio Nacional de Salud en el Reino Unido costaba aproximadamente 5.0 billones de libras esterlinas y Microsoft tomó la mayor parte de este negocio según datos de Cross,[9] sin embargo, esta región fue también la primera en utilizar software libre y abierto para los servicios gubernamentales desde 2014 aproximadamente.

El Software Libre y abierto.

Ambos tipos de software libre: el “libre” y de código abierto (libre, and open software) comparten una característica clave: todos los usuarios deben tener acceso abierto al código fuente, que se considera compartible y como recurso de no-propiedad, sin

[9] Cross, M. ìInside IT: High stakes in the battle for Britainî, THE GUARDIAN, (29 January 2004).

embargo, es necesario profundizar en las diferencias entre sus conceptos para entender el alcance de los derechos vinculados.

Software libre

Un informe titulado "Software libre / Código abierto: Oportunidades de la sociedad de la información para Europa"[10] ofrece una síntesis útil de las principales características que caracterizan al software libre y vale la pena citar este informe en detalle. Este enfoque alternativo significa que todos los usuarios tienen la libertad de:

1. Utilizar el software como lo deseen, para lo que deseen, en tantas computadoras como lo deseen, en cualquier situación técnicamente apropiada.

2. Tener el software a su disposición para adaptarlo a sus necesidades. Por supuesto, esto incluye mejorarlo, corregir sus errores, aumentar su funcionalidad y estudiar su funcionamiento.

[10] Working group on Libre Software, ìFree Software / Open Source: Information Society Opportunities for Europe?, (Version 1.2 - work in progress), (April 2000), http://eu.conecta.it/paper/paper.html.

3. Redistribuir el software a otros usuarios, que podrían usarlo de acuerdo con sus propias necesidades. Esta redistribución se puede hacer de forma gratuita o con cargo, no fijada de antemano.

Ahora es importante aclarar que estamos hablando de libertad y no de obligación. Es decir, los usuarios de dicho programa de software pueden modificarlo, si lo consideran apropiado. Pero, en cualquier caso, **no están obligados a hacerlo**. Del mismo modo, pueden redistribuirlo, pero, en general, no están obligados a hacerlo.

Con la finalidad de facilitar estas diversas libertades y asegurarse de que el código fuente no se convierta en la propiedad privada o exclusiva de un desarrollador de software en particular o un grupo de desarrolladores, los pioneros del movimiento del software libre, y en particular el programador informático de los EE. UU. Richard Stallman, desarrolló en la década de 1980 lo que se llama la Licencia Pública General (GPL por sus siglas en inglés). Su objetivo principal es garantizar y reforzar un espíritu de

intercambio con el código fuente de programas como Linux, el sistema operativo básico de código libre / abierto.

El enfoque de Software Libre para la concesión de licencias se basa en lo que se conoce como el principio de Copyleft. En contraposición al propósito habitual de los derechos de autor o la exclusividad: una licencia de Copyleft como la GPL significa que el código debe compartirse con otros y no permite a ningún usuario distribuir el código y sus modificaciones, mejoras y adiciones como parte de un esquema de propiedad. Además, la GPL requiere que las mejoras se licencien en los mismos términos que el código que el desarrollador recibió y utilizó inicialmente.

Software de código abierto

Otros desarrolladores de software, aunque creían que el código fuente de la computadora debería permanecer abierto y accesible, consideraron que el enfoque de "software libre" no proporcionaba la base para un modelo comercial comercial y establecieron en la década de 1990 otra organización, la Open Source Initiative (la "OSI"). -que opera en algunos principios

similares y otros diferentes- define Open Source como un software que proporciona los siguientes derechos y obligaciones:

1. No se cobran regalías u otros impuestos sobre la redistribución.
2. Disponibilidad del código fuente.
3. Derecho a crear modificaciones y trabajos derivados
4. Puede requerir versiones modificadas para ser distribuidas como la versión original más parches.
5. No discriminación contra personas o grupos.
6. No discriminación contra campos de esfuerzo.
7. Todos los derechos otorgados deben fluir a / con versiones redistribuidas.
8. La licencia se aplica al programa como un todo y cada uno de sus componentes.
9. La licencia no debe restringir otro software, lo que permite la distribución de software de fuente abierta y de código cerrado.

En particular, las licencias de software de código abierto permiten a los desarrolladores de software una protección exclusiva a las adiciones que realizan a un programa; estas mejoras proporcionan uno de los flujos de ingresos clave. Por ejemplo, un esquema de licencia alternativo a la GPL, conocido como el Contrato Social de Debian, otorga a los licenciatarios una mayor flexibilidad al permitirles agrupar el código de software que se desarrolló cooperativamente con el código propietario. En otras palabras, no se pueden imponer restricciones sobre otro software que se distribuye junto con el software licenciado, como es el caso con la GPL. Por lo tanto, un programa de aplicación de código abierto (por ejemplo, Oracle) ejecutándose, como software libre, en el sistema operativo Linux puede estar protegido por derechos de autor si su desarrollador / propietario requiere o desea dicha protección; a diferencia de una licencia de "Copyleft", esa adición no necesita ser compartida con otros. (Sin embargo, Linux, por sí solo, no tiene las características del software propietario). Además, una gran cantidad de software libre, como Apache, se ejecuta en Windows y

hay un montón de software libre que opera con una licencia algo diferente a GPL.

Propiedad industrial

La propiedad industrial es el objeto de protección más variado que se reconoce dentro del derecho de propiedad intelectual, pues puede constituir una multiplicidad de creaciones realizadas por un sin fin de medios. El convenio de parís expresa que:

"La propiedad industrial se entiende en su acepción más amplia y se aplica no sólo a la industria y al comercio propiamente dichos, sino también al dominio de las industrias agrícolas y extractoras y a todos los productos fabricados o naturales, por ejemplo: vinos, granos, hojas de tabaco, frutos, animales, minerales, aguas minerales, cervezas, flores, harinas."[11]

A pesar de la amplitud del objeto, según el convenio de París, las principales creaciones que son sujeto de protección, bajo la figura de la propiedad industrial, son:

[11]Convenio de París artículo 1.3 Constitución de la Union; ámbito de la propiedad industrial

"las patentes de invención, los modelos de utilidad, los dibujos o modelos industriales, las marcas de fábrica o de comercio, las marcas de servicio, el nombre comercial, las indicaciones de procedencia o denominaciones de origen, así como la represión de la competencia desleal."[12]

De la relación entre el derecho a la propiedad y la informática, tenemos que la propiedad industrial se ejerce principalmente sobre aquellas creaciones materiales o tangibles por lo tanto la propiedad industrial solamente puede ser ejercida sobre el Hardware y otros elementos periféricos que funcionan con instrucciones ingresadas mediante códigos de programación como los que ya fueron abordados en la parte del software.

Según la OMPI este tipo de ***"creación intelectual***" de la propiedad industrial consiste en ***"signos que transmiten información, en particular a los consumidores, en relación con los productos y servicios disponibles en el mercado."*** con la finalidad de protegerlos de cualquier utilización no autorizada de dichos signos, que en consecuencia, podría inducir a

[12]Artículo 1.3 Constitución de la Union; ámbito de la propiedad industrial

error a los consumidores, o constituirse como una práctica de competencia desleal.[13]

La legislación salvadoreña, establece que la protección de la propiedad industrial abarca a la invención, al modelo de utilidad y al diseño industrial, aun que la aplicación supletoria del convenio de París vincula a todas las antes mencionadas. Incluso la regulación de las marcas y signos distintivos esta regulada por una ley especial en sentido de protección del comercio.

Cabe hacerse la pregunta: ¿que es una invención? La OMPI aclara que en muchos países este concepto no esta definido pero en El Salvador, la legislación propone que una invención es:

"...una idea aplicable en la práctica a la solución de un problema técnico determinado." y además establece que una invención podrá referirse a un producto o a un procedimiento.." [14]

[13] OMPI. (2016).*Principios básicos de la propiedad industrial* (2nd ed., Vol. 1, ISBN: 978-92-805-2590-8). Ginebra, Suiza: OMPI. Atribución de licencia 3.0 IGO (CC BY 3.0 IGO) p.3

[14] LFPPI artículo 106

No importa que se trate de un problema que se ha abordado desde mucho tiempo atrás o de un nuevo problema; sino que **la solución sea nueva,** para poder ser considerada una invención.

No debe confundirse una invención con un descubrimiento, la invención requiere que sea producto del uso en determinada proporción de *"ingenio",* creatividad e inventiva; un descubrimiento si bien es importante no se considera una invención, pues consiste en el hallazgo de algo que era preexistente pero oculto hasta el momento de su verificación por lo tanto aquellos que hacen algún descubrimiento, pueden solamente nombrarlo como ellos mismos deseen aun que no pueden exigir derechos sobre el descubrimiento.

En algunos casos, la innovación, contribuye fomentar los descubrimientos, como la brocha de un arqueólogo, o la resistencia de un foco incandescente, en otros, los descubrimientos, pueden ser modificados o alterados a manera que de ellos surja una invención, por ejemplo, cuando los ingenieros romanos descubrieron el plomo, lo convirtieron en tuberías para abastecer sus ciudades; sin embargo, el mejor ejemplo

de la combinación de invención y descubrimiento es definitivamente el plástico.

Las Patentes de invención

La herramienta específica para dar protección a las invenciones de hardware y otros elementos de la propiedad industrial, se denomina "**patente",** es el equivalente al registro de licencia en los derechos de autor sobre el software y es una manera de proteger al inventor, por todo el tiempo y el esfuerzo que ha invertido en su producto. Además todos los derechos patrimoniales que ya se han estudiado en el apartado anterior, son también aplicables a las patentes.

El artículo 111 de la ley de fomento y protección de la propiedad intelectual establece que para que una invención sea patentable es necesario que *"sea susceptible de aplicación industrial,.. novedosa y tenga nivel inventivo."*

de este concepto, es necesario destacar algunos puntos importantes expresados en la misma ley:

1. **La aplicación industrial:** "Una invención se considera susceptible de aplicación industrial,

cuando su objeto pueda ser producido o utilizado en cualquier tipo de industria o actividad productiva. A estos efectos la expresión industria se entenderá en su más amplio sentido e incluirá, entre otros, la agricultura, la ganadería, la minería, la pesca, la construcción y los servicios".

2. **La novedad:** "Una invención se considera novedosa cuando no exista con anterioridad en el *estado de la técnica*. El estado de la técnica comprende todo lo que haya sido divulgado o hecho accesible al público, en cualquier lugar del mundo, ... antes de la fecha de presentación de la solicitud de patente en el país o, en su caso, antes de la fecha de presentación de la solicitud extranjera cuya **prioridad** se reivindicará."

3. **El nivel inventivo:** "Se considerará que una invención tiene nivel inventivo si, para una persona normalmente versada en la materia técnica correspondiente, la invención no resulta

obvia ni se habría derivado de manera evidente del estado de la técnica pertinente"[15]

El estado de la técnica que se menciona en el apartado 2, hace referencia a lo que la OMPI[16] señala sobre el convenio de París, respecto del denominado "**derecho de prioridad";** es decir que: tras haberse presentado una solicitud en un Estado parte en el Convenio de París, el mismo solicitante (o su causahabiente) tiene la facultad, de solicitar protección respecto de la misma invención en cualquiera de los demás Estados parte en el convenio.

La legislación salvadoreña establece que la patente es aquella herramienta que confiere a su titular el derecho de impedir que otras personas (terceras personas) puedan explotar la invención patentada y establece que el titular tiene siguientes derechos[17]:

1. Cuando la patente se haya concedido para un producto, el titular tiene derecho a:

[15] Véase artículos 112,113 y 114 LFPPI

[16] OMPI. (2016).*Principios básicos de la propiedad industrial* (2nd ed., Vol. 1, ISBN: 978-92-805-2590-8). Ginebra, Suiza: OMPI. Atribución de licencia 3.0 IGO (CC BY 3.0 IGO) p.8

[17] Véase artículo 115 LFPPI

a) Fabricar el producto;

b) Ofrecer en venta, vender o usar el producto; o importarlo o almacenarlo para alguno de estos fines;

2. Cuando la patente se haya concedido para un procedimiento el titular tiene derecho a:

a) Emplear el procedimiento;

b) Ejecutar cualquiera de los actos indicados en el literal anterior, respecto a un producto obtenido directamente del procedimiento.

Nótese que dentro de la propiedad industrial, si es posible, patentar un procedimiento, a diferencia de los derechos de autor en la propiedad intelectual, esto es debido a la orientación industrial que ya se ha explicado con anterioridad.

Entonces, lo que no es objeto de patente según la legislación salvadoreña son[18]:

a) Los descubrimientos, las teorías científicas y los métodos matemáticos;

[18] Véase el articulo 107 LFPPI

b) Los planes, principios o métodos económicos o de negocios, los referidos a actividades puramente mentales o intelectuales, y los referidos a materia de juego;

c) Los métodos de tratamiento quirúrgico, terapéutico o de diagnóstico, aplicables al cuerpo humano o animal; excepto los productos destinados a poner en práctica alguno de estos métodos; y

d) Las invenciones cuya publicación o explotación industrial o comercial sería contraria al orden público o a la moral; la explotación de la invención no se considerará contraria al orden público o a la moral solamente por una razón de estar prohibida o limitada tal explotación por alguna disposición legal o administrativa.

Finalmente, las patentes de invención, según la ley en cuestión, solamente tendrán una duración de 20 años contados a partir de la fecha de presentación de la solicitud en el Registro de Comercio, a excepción de las patentes de medicamentos que tendrán una duración de 15 años a partir de la fecha de presentación en el

registro. En ambos casos, se deberá cancelar anualmente el pago por el derecho de la patente según lo expresa el art. 108, con la condición que de no registrarse uno de estos pagos, podrá caducar la patente correspondiente. En todo caso, al caducar la patente, la invención pasará a ser de dominio publico.

Una de las patentes de hardware más famosas recientemente es la memoria USB según la revista Xataka Hay cierta discordia respecto a quién inventó realmente el primer USB. Por un lado, la primera patente fue presentada en abril 1999_con el nombre **"USB-based PC flash disk"**, y fue creada por Amir Ban, Dov Moran y Oron Ogdan, de la empresa Israelí **M-Systems**. La patente no describe esta tecnología comol la conocemos hoy, ya que la describe con un cable que conecta la memoria y el puerto USB.

Por otra parte, en septiembre de 1999 uno de los empleados de IBM, Shimon Shmueli, presentó una divulgación de invención[19], antes de su patente, en la que describía una unidad flash USB. Hoy en día, muchos

[19] La plena divulgación de la invención es un principio básico del derecho de patentes. El acceso a la información sobre la invención es una de las justificaciones tradicionales para conceder exclusividad temporal al inventor. IBM posterior mente lo registro bajo la patente: IBM Patent RPS8-1999-0201

afirman que Shmueli fué quienl inventó la memoria USB. Independientemente de eso, M-Systems se asoció con IBM para llevar al mercado en septiembre del 2000 uno de los dos primeros dispositivos de este tipo del mercado, al que llamaron **"DiskOnKey"**.

El primer dispositivo fué introducido al mercado para principios de ese 2000 por la empresa de Singapur **Trek 2000 International** que se convirtió en la primera en comercializar una de estas unidades, la cual llevaba el nombre de **"ThumbDrive"**. Esta empresa también asegura que es la que inventó la memoria USB, aunque la mayoría de fabricantes de estos dispositivos no lo hace licenciando sus patentes.

Pua Khein-Seng, un ingeniero de Malasia, fundó en 1999 junto a cuatro compañeros la empresa **Phison Electronics**. En el año 2000, según Khein-Seng, su empresa tecnológica presentó la unidad de almacenamiento USB con un único chip interno al que llamó **"Pen Drive"**.

Modelos de utilidad

En algunos casos, la invención puede recaer sobre un objeto que ya cuenta con una patente, o que su patente ya esta caducada y es de dominio público pero la innovación esta en una parte de este objeto. Para proteger esta innovación, se hace uso de la herramienta de protección denominada "**modelo de utilidad".** Según la OMPI[20] los modelos de utilidad pueden considerarse como "mejoras menores" en productos existentes o "adaptaciones" de dichos productos, todo sin que se cambie la esencia del mismo.

Los modelos de utilidad también son un derecho exclusivo que se concede a una invención y tiene los mismos efectos que la patente en sentido de su protección contra la explotación por parte de terceros.

La legislación salvadoreña establece que los modelos de utilidad son:

"*...toda forma, configuración o disposición de elementos de algún artefacto, herramienta, instrumento,*

[20] OMPI. (n.d.). ¿Cómo proteger las innovaciones mediante modelos de utilidad? Retrieved October 11, 2017, from http://www.wipo.int/sme/es/ip_business/utility_models/utility_models.htm

mecanismo u otro objeto, o de alguna parte del mismo que permita un mejor o diferente funcionamiento, utilización o fabricación del objeto que lo incorpora, o que le proporcione alguna utilidad, ventaja o efecto técnico que antes no tenía."[21]

Además establece establece como condición especial de registro, que este modelo de utilidad se nuevo y que tenga aplicación industrial. (es decir, que deben cumplirse los requisitos de **novedad** y de **aplicación industrial** que ya hemos abordado en la parte de las patentes.)

Los modelos de utilidad, según la legislación salvadoreña, solo tienen una duración de 10 años improrrogables, contados a partir de la fecha de presentación de la solicitud.

Diseños y dibujos industriales

La OMPI[22] plantea que los diseños industriales se refieren a aspectos ornamentales y estéticos de un artículo, incluidas las composiciones de líneas o colores

[21] Véase articulo 120 LFPPI

[22] MPI. (2016).*Principios básicos de la propiedad industrial* (2nd ed., Vol. 1, ISBN: 978-92-805-2590-8). Ginebra, Suiza: OMPI. Atribución de licencia 3.0 IGO (CC BY 3.0 IGO) p.11

en formas tridimensionales que otorgan una apariencia especial a un producto u obra de artesanía. El diseño debe ser atractivo estéticamente. Además, debe poder ser reproducido por medios industriales, es decir que debe cumplir con el requisito de aplicación industrial ya que esa es la finalidad esencial del diseño y razón por la que recibe el calificativo de "industrial". Sin embargo, se puede registrar un diseño industrial siempre y cuando este no cumpla con los requisitos del modelo de utilidad.

La ley establece que un diseño industrial es:

"cualquier forma bidimensional o tridimensional que, incorporado en un producto utilitario, le da una apariencia especial, y que es apto para servir de tipo o modelo para su fabricación."[23]

Al igual que los modelos de utilidad y que las patentes, los diseños industriales son el instrumento que confiere derechos del titular sobre su creación, y tiene una vigencia de 5 años, los cuales pueden ser

[23] Véase articulo 123 LFPPI

prorrogados por otro período igual previo el pago de los derechos de prorroga[24].

Los derechos sobre los diseños industriales se adquiere ya sea por haberse divulgado en el país o por haberse interpuesto la solicitud de registro. Es decir que la mera divulgación del diseño industrial, confiere derechos sobre su autor.

Un ejemplo de diseño industrial es el de las diferentes formas tridimensionales de las memorias USB de la misma estructura volumétrica y de la misma categoría de producto de los “pendrives” y “thumbdrives”.

Las Marcas y signos distintivos.

Según la OMPI[25], Por marca se entiende un signo o una combinación de signos que diferencian los productos o servicios de una empresa de los de las demás. Estos signos pueden ser palabras, letras, números, fotos, formas y colores o una combinación de

[24]Véase articulo 130 LFPPI

[25] OMPI. (2016).*Principios básicos de la propiedad industrial* (2nd ed., Vol. 1, ISBN: 978-92-805-2590-8). Ginebra, Suiza: OMPI. Atribución de licencia 3.0 IGO (CC BY 3.0 IGO) p.11

los mismos. Además, cada vez son más los países que autorizan el registro de formas menos tradicionales de marcas, como los signos tridimensionales (como la botella de Coca-Cola o la barra de chocolate Toblerone), signos sonoros (sonidos como el rugido del león que sale al principio de las películas producidas por la MGM), o los signos olfativos (como el olor de un tipo particular de un aceite de motor o de hilo de bordar).

Las marcas se utilizan para productos o en relación con la comercialización de productos o servicios. No solo se aplican a los productos propiamente dichos sino también al embalaje en el que se comercializan. En cuanto a su utilización para la venta de productos, se trata concretamente de la utilización del signo en anuncios, por ejemplo, en los periódicos, en la televisión o en escaparates.

En la legislación salvadoreña este concepto se encuentra en la ley marcas y otros signos distintivos[26] y establece que se entiende por marca:

"Cualquier signo o combinación de signos visualmente perceptibles que, por sus caracteres

[26] Decreto Legislativo numero 868 del 6 de julio del año 2002.

especiales, sirva para distinguir claramente los productos o servicios de una persona natural o jurídica, de los productos o servicios de la misma clase o naturaleza, pero de diferente titular;"[27]

Básicamente, el concepto de la legislación salvadoreña no presenta ninguna variante relevante respecto del concepto de la OMPI, pues como ya se menciona en el apartado de las patentes, las leyes salvadoreñas han adoptado los conceptos de derecho internacional de la OMPI.

El registro y protección de una marca busca garantizar el derecho exclusivo a utilizar la marca para identificar productos o servicios brindados por una empresa, también otorga la facultad de autorizar el uso de la misma por terceros a cambio del pago de una suma, que al igual que las patentes, corresponde al derecho de explotación.

Según el artículo 4 de la ley "las marcas podrán consistir, entre otros, en palabras o conjuntos de palabras, incluidos los nombres de personas, letras, números, monogramas, figuras, retratos, etiquetas,

[27] Artículo 2 Ley de marcas y otros signos distintivos

escudos, estampados, viñetas, orlas, líneas y franjas, o combinaciones y disposiciones de colores. Pueden asimismo consistir, entre otros, en la forma, presentación o acondicionamiento de los productos, o de sus envases o envolturas, o de los medios o locales de expendio de los productos o servicios correspondientes."

Este artículo establece entonces algunos elementos importantes para definir los principales tipos básicos de marcas. Así, los tipos de marcas son:

Marcas nominativas: son aquellas que se constituyen por una palabra o conjunto de palabras. Estas marcas deben cumplir con el requisito especial de ser fácilmente distinguidas fonéticamente, esto es, por que al pronunciarse la marca, no debe confundirse con el nombre del producto o servicio que se ofrece, ni con ningún otro de su misma especie. Algunos ejemplos de estas marcas son ZARA, como marca de palabra o Keneth Cole como conjunto de palabras o AND 1 como conjunto de letras y números; este tipo de marcas debe estar constituido solamente por la agrupación de letras (o letras y números) en el orden específico para

constituir la marca, es decir que la marca se constituye por la palabra en sí y no por la fuente de las letras o por las variaciones en su expresión.

Marcas Mixtas: las marcas mixtas se definen por la combinación de una marca nominativa más un símbolo, es decir, una marca figurativa. Generalmente son creadas para abarcar tanto la definición visual como fonética, y estas deben componer una marca en su conjunto, para fines de registro, la separación la palabra con la figura se constituye en una marca diferente, pues la marca mixta es aquella que siempre se va a constituir por la palabra o conjunto de palabras con números más una figura.

Marcas tridimensionales: Las marcas tridimensionales son utilizadas generalmente, cuando el producto en su forma natural no posee una forma específica o se puede confundir fácilmente con otros productos de su mismo género, por lo tanto el envase en el que se comercializa, se constituye también como parte de la marca, y representa una una representación gráfica funcional para lograr su finalidad que es la de identificarse como producto, las marcas

tridimensionales tienen la característica que no pueden constituirse en formas comunes (como una tuerca por ejemplo) ni pueden utilizarse como marca, envases estandarizados (como el de las botellas de vino).

La diferencia entre una marca tridimensional y un diseño o modelo industrial radica en que éste último esta en la obligación de cumplir con las características de novedad y singularidad al momento de su registro como tal, aun que el uso general de los diseños industriales es el convertirse finalmente en un distintivo de la marca. Por ejemplo: en el diseño industrial de una botella, el derecho que se protege, es aquel que se tiene sobre la forma, la línea, la configuración, densidad, volumen etc. es decir la cualidad estética del diseño mientras que se si esta botella es utilizada como una marca tridimensional, el derecho que se protege es el de la distinción comercial; por lo tanto no deben ser confundidos a pesar de sus semejanzas pues se constituye como una distinción jurídica de los conceptos.

Marcas Sonoras: Estas marcas son una derivación del denominado "Audio Branding" o

"identidad sonora" y se constituyen principalmente en un sonido o una combinación de sonidos que permiten la distinción comercial de una empresa. Esta marca se utiliza mayormente en el área de servicios, sin embargo es utilizada también como marca de productos. A pesar que la legislación salvadoreña no las reconoce como marcas, estas complen con la misma finalidad que las demás, y es la de proporcionar una identidad a la marca, lo que lo diferenciaría de una producción musical protegida por derechos de autor. Los ejemplos más comunes son los "ringtones" o los "slogan" acompañados por música, conocidos también como "giggles".

Por ejemplo la melodía de la compañía finlandesa NOKIA es una composición consistente en trece notas, en clave de sol y en compás 3/4. Que proviene de una composición española para guitarra denominada"Gran Vals" del autor Francisco Tárrega[28], escrito a principios del siglo XX, en la cual la compañía solamente utiliza los compases 14 al 16.

[28] Tony Skinner, Raymond Burley (2002).Classical Guitar Playing: Grade Seven (LCM). Registry Publications Ltd. p.10. ISBN 189846667X. Partitura original disponible en http://www.stormthecastle.com/classical_guitar/Collection/Tarrega_-_Gran_Vals.pdf

Finalmente, los artículos 8 y 9 de la ley de marcas y otros signos distintivos establecen las causales intrínsecas y por derechos de terceros respectivamente, de los que no se puede registrar como marca. Textualmente estos artículos rezan:

Marcas Inadmisibles por Razones Intrínsecas

"Art. 8.- No podrá ser registrado ni usado como marca o como elemento de ella, un signo que esté comprendido en alguno de los casos siguientes:

a) Que consista en la forma usual o corriente del producto al cual se aplique o de su envase, o en una forma necesaria o impuesta por la naturaleza del producto o del servicio de que se trate;
b) Que consista en una forma que dé una ventaja funcional o técnica al producto o al servicio al cual se aplique.
c) Que consista exclusivamente en un signo o una indicación que, en el lenguaje corriente, técnico o científico, o en la usanza comercial del país, sea una designación común o usual del producto o del servicio de que se trate;

d) Que consista exclusivamente en un signo o una indicación que pueda servir en el comercio para calificar o describir alguna característica del producto o del servicio de que se trate;

e) Que consista en un simple color aisladamente considerado;

f) Que consista en una letra o un dígito aisladamente considerado, salvo que se presente en una forma especial y distintiva;

g) Que sea contrario a la moral o al orden público;

h) Que comprenda un elemento que ofenda o ridiculice a personas, ideas, religiones o símbolos nacionales de cualquier país o de una entidad internacional;

i) Que pueda causar engaño o confusión sobre la procedencia geográfica, la naturaleza, el modo de fabricación, las cualidades, la aptitud para el empleo o el consumo, la cantidad o alguna otra característica del producto o del servicio de que se trate;

j) Que consista en una indicación geográfica que no se ajuste a lo dispuesto en el Art. 4 inciso segundo;

k) Que reproduzca o imite, total o parcialmente, el escudo, bandera u otro emblema, sigla, denominación o abreviación de denominación de cualquier Estado u

organización internacional, sin autorización expresa de la autoridad competente del Estado o de la organización internacional de que se trate;

l) Que reproduzca o imite, total o parcialmente, un signo oficial de control o de garantía adoptado por un Estado o una entidad pública, sin autorización expresa de la autoridad competente de ese Estado;

m) Que reproduzca monedas o billetes de curso legal en el país, títulos valores u otros documentos mercantiles, sellos, estampillas, timbres o especies fiscales en general;

n) Que incluya o reproduzca medallas, premios, diplomas u otros elementos que hagan suponer la obtención de galardones con respecto al producto o servicio correspondiente, salvo que tales galardones hayan sido verdaderamente otorgados al solicitante del registro o a su causante y ello se acredite al tiempo de solicitar el registro; y

o) Que consista en la denominación de una variedad vegetal protegida en el país o en el extranjero, si el signo se destinara a productos o servicios relativos a esa variedad.

Marcas Inadmisibles por Derechos de Terceros

Art. 9.- No podrá ser registrado ni usado como marca o como elemento de ella, un signo cuando ello afecte a algún derecho de tercero, en los siguientes casos:

a) Si el signo fuera idéntico a una marca u otro signo distintivo ya registrado o en trámite de registro a favor de un tercero desde una fecha anterior, que distinguiera productos o servicios comprendidos en una misma clase;

b) Los signos que por su semejanza gráfica, fonética o ideológica pueden inducir a error u originar confusión con otras marcas y demás signos distintivos ya registrados o en trámite de registro a favor de un tercero, si se pretende emplearlos para distinguir productos o servicios comprendidos en una misma clase;

c) Si el signo fuera susceptible de causar confusión por ser idéntico o similar a un nombre comercial o un emblema usado en el país por un tercero desde una fecha anterior, siempre que el giro o la actividad mercantil sean similares;

d) Si el signo constituyera una reproducción, imitación, traducción o transcripción, total o parcial, de un signo distintivo notoriamente conocido, perteneciente a un tercero, cuando su uso fuera susceptible de causar confusión o un riesgo de asociación con ese tercero, o un aprovechamiento injusto de la notoriedad del signo, con relación a productos comprendidos en una misma clase;

e) Si el signo constituyera una reproducción, imitación, traducción o transcripción, total o parcial, de un signo distintivo famoso perteneciente a un tercero, cuando su uso fuera susceptible de causar confusión o un riesgo de asociación con ese tercero, cualesquiera que sean los productos o servicios a los cuales el signo se aplique;

f) Si el signo afectara el derecho de la personalidad de un tercero, o consistiera parcial o totalmente en el nombre, firma, título, seudónimo, imagen o retrato de una persona distinta de la que solicita el registro, salvo autorización expresa del tercero o de sus herederos;

g) Si el signo afectara el derecho al nombre, a la imagen o al prestigio de una colectividad local, regional o nacional, salvo que se acreditase la autorización expresa de la autoridad competente de esa colectividad;

h) Si el signo fuera susceptible de causar confusión con una denominación de origen protegida;
i) Si el signo fuera susceptible de infringir un derecho de autor o un derecho de propiedad industrial de un tercero, salvo que medie su autorización expresa; y,
j) Si el registro del signo se hubiera solicitado para perpetrar o consolidar un acto de competencia desleal.

El uso de marca en buscadores de internet.

Los motores de búsqueda en internet son actualmente una herramienta fundamental en la búsqueda de información en la internet, por lo tanto son una manera directa de generar publicidad y de llegar a nuevos mercados. El flujo de usuario de estos buscadores es tal que han dejado de convertirse en meros intermediarios de información, sino que progresivamente se han convertido en impulsores de opinión y espacios para publicidad agresiva, lo que ha acarreado problemas legales en el área de derechos de autor, la privacidad, el uso de marcas ajenas etc.

Los primeros anuncios publicitarios en la web eran colocados solamente como avisos colocados en la parte superior o a los costados de los sitios web como meros *Banners* gráficos (generalmente imágenes con extensión .png), de modo que quien se anunciaba en dicho sitio, generalmente colaboraba con el funcionamiento de la página como una forma de "patrocinio de información" o "mecenazgo"; De hecho Google inició su modelo de negocios sin ningún tipo de publicidad en su buscador pues consideraban que la publicidad interfería con los resultados de las búsquedas. Consecuentemente, los altos costos de mantener un modelo como este llevaron a google a acceder al uso de publicidad online mediante un programa llamado *Adwords*, el cual utiliza una función basada en la idea del "*pay-per-click*" (pago por click) desarrollado por a empresa *Overture* utilizado a través del sitio www.goto.com lo que impulsó una demanda de violación de patente[29] en contra de Google hasta que Overture fue comprada por Yahoo y ambos llegaran a un acuerdo por 2.7 millones de dólares en acciones de

[29] Overture Services INC Delaware vs Google INC California Caso 3:02 -cv-01991 del 18 de julio del 2003.

Google a cambio de una licencia perpetua para el uso de una patente.

Luego de este acuerdo Google comenzó a insertar publicidad en su buscador mediante "enlaces patrocinados" (sponsored links o keyword ad), que eran básicamente, publicidad basada en la busqueda del usuario y según el programa "*pay-per-click*" Google recibiría una remuneración si el usuario hacía click en el enlace.

Esta práctica ho había tenido mayores consecuencias legales hasta que se comenzó a proliferar el uso de "*metatags*" o palabras ocultas utilizadas por los competidores de google con terminos coincidentes, estos m*etatags* se insertaban en el código HTML de sus páginas web desviando el tráfico de los sitios patrocinados hacia sus sitios. Incluso algunos nuevos negocios surgieron cuando algunos buscadores vendían las denominadas "*keywords*" o "palabras clave" que les permitieran a las marcas aparecer de forma prominente en los buscadores de Google y otros buscadores.

A nivel internacional, el "*meta-tagging*" está prohibido en muchos países, sin embargo en El Salvador

aun no es considerada como una práctica desleal.

Luego de los metatags, se utilizó el tipo de publicidad por ventanas emergentes (“*pop up advertising”*) el cual tambien trajo sus propios problemas legales pues estos funcionan con una línea de código introducida tambien en el código HTML que sobreimprimía una ventana encima del navegador del usuario con la publicidad patrocinada, esta pantalla obligaba al usuario a hacer click sobre ella para poder continuar con su busqueda, lo que generalmente hacía que el sitio patrocinado cobrara por omitir el anuncio (lo contrario a *pay per click).* Finalmente, los tribunales estadounidences juzgaron sobre este aspecto al dictar que los pop up no tenían “uso de marca” es decir que no coincidían en la mayoria de los casos con las busquedas, por lo tanto era una intrusión en la busqueda del usuario.

Capítulo 2

Los Delitos Informáticos

Otra de las áreas más importantes del derecho informático, es el aspecto relacionado con la cuestión del derecho penal, en sentido que se pueden perpetrar una serie de delitos a través del sistema informático. (hardware y software), En El Salvador, estos tipos penales se recogen en la Ley Especial Contra los Delitos Informáticos y Conexos[30], (LECDIC) que establece específicamente que se entenderá que se ha cometido un delito informático: "cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información"; sin embargo no ofrece un concepto específico, de hecho no existe a nivel internacional un concepto unificado.

[30] Decreto 260 del 26 de Febrero de 2016

En la doctrina se utiliza la clasificación de Tiedemann[31] para intentar esbozar el un concepto de "delito informático." a partir de la idea de los elementos que se integran en la definición de "Criminalidad mediante computadoras" así:

1. Los actos que afectan al soporte físico (hardware) o al lógico (software),
2. Utilización de la información contenida en el programa de computación.
3. La utilización ilegitima de un ordenador en beneficio propio o de tercero.

Dentro del primer elemento se abordan aquellos delitos relacionados o en contra de la propiedad, por ejemplo el apoderamiento indebido de los elementos que integran el sistema informático., (hardware o software), el hurto o robo, según la tipificación de los artículos 207 y 212 de Código Penal[32] respectivamente, es importante mencionar que para el caso del hurto de software, la acción antijurídica debe recaer sobre el

[31] Tiedemann, Klauss, "Poder informático y delito" Barcelona España 1985.

[32] Código penal de El Salvador decreto 1030 de la Asamblea legislativa.

disco (disk drivers) que es el elemento donde se encuentra la información, y no sobre el software propiamente pues éste no es susceptible de apoderamiento según lo plantea Felipe Rodriguez.-

El segundo elemento de Tiedemann, se enfoca en las conductas que recaen sobre la utilización del sistema informático como medio o instrumento para cometer un delito, como podría suceder con cualquier otro elemento, un palo, una ganzúa etc. siempre que esta conducta afecte un bien jurídico de los que proteje el codigo penal, por ejemplo, la difamación, la extorsión etc. cuando estas conductas se ejecutan mediante la inclusión de datos o información adicional falsa incluyendo su divulgación en todo el circuito informático.

El ultimo elemento esta enfocado en los ilícitos que se ejecutan como consecuencia de la alteración de las fuentes de información, acá se encajan la mayoría de delitos económicos,como la estafa, la clonacion de tarjetas de credito etc. Es importante enfatizar que los delitos informáticos no son cometidos por la computadora, pues es obvio que los delitos solo pueden

ser cometidos por seres humanos, sin embargo se ha producido un amplio debate sobre los posibles delitos cometidos por maquinas con inteligencia artificial, en sentido que, actualmente quien responde penalmente será su creador; por eso para fines de este estudio se entenderá que todos los delitos informáticos son cometidos por personas humanas utilizando los elementos de un sistema informático.

El concepto de delito informático

Como ya se mencionó en el apartado anterior, no se ha llegado a un consenso sobre el concepto universal de delito informático. sin embargo todos los autores sobre el tema estan de acuerdo que los delitos informáticos llevan implicitas actividades criminales que primeramente son figuras típicas del derecho penal común, tales como robos o hurtos, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc. Sin embargo, debido all uso de las técnicas informáticas se han producido una serie de nuevas figuras penales a partir del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de una regulación especial dentro del derecho informático.

Julio Téllez Valdés[33] señala que el problema de la conceptualización de delito informático recae en su misma denominación pues esta *"alude a una situación muy especial, ya que para hablar de 'delitos' en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión 'delitos informáticos' esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos, no ha sido objeto de tipificación aún".*

Por otro lado, Carlos Sarzana[34], propone que los crímenes por computadora comprenden *"cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".*

Rafael Fernández Calvo es más reservado al manifestar que el delito informático. es simplemente la

[33] Téllez Valdés, Julio.Derecho Informático. 2a. ed. México. Mc Graw Hill 1996. Pp.103-104. Zavala , Antelmo.El Impacto Social de la Informática Jurídica en México. Tesis. México. UNAM. 1996. REVISTAS

[34] Sarzana, Carlo. Criminalità E Tecnologia En Computers Crime. Rassagna Penitenziaria E Criminologia. Nos. 1-2. Ano 1. 1979. Roma,Italia. P.53

realización de una acción que reune las características que delimitan el concepto de delito y que se ha llevado a cabo "*utilizando un elemento informático. o telemático contra los derechos y libertades de los ciudadanos...*".

Reuniendo un poco estos elementos Julio Téllez Valdés conceptualiza al delito informático. en forma típica y atípica, estableciendo que en el primer grupo se encuentran las *"conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin"*, y en un segundo grupo estan las, *"actitudes ilícitas en las que se tienen a las computadoras como instrumento o fin".* Para el autor, este tipo de acciones presentan las siguientes características principales:

1. Son conductas criminales de cuello blanco (*white collar crime*), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

2. Son acciones ocupacionales, en cuanto a que muchas veces se realizan en entornos laborales o a través de relaciones laborales de confianza.

3. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

4. Generan un impacto económico, ya que casi siempre producen "beneficios", destrucción o inhabilitación de sistemas cuyo impacto es en los costos que esta inhabilitación o destrucción produce,

5. Ofrecen posibilidades de tiempo y espacio,

6. ofrecen dificultades para la individualización Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

7. Son muy sofisticados y relativamente frecuentes en el ámbito militar.

8. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

9. En su mayoría son imprudenciales y no necesariamente se cometen con intención. Ofrecen facilidades para su comisión a los menores de edad.

10. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

En fin, se debe entender que la delincuencia informática es aquella conducta tipificada como delito, en el derecho común o especial en donde la ejecución de la misma se apoya en el uso de la computadora a través de redes telemáticas y la interconexión de la computadora.

Aspectos generales del delito informático

Como toda definición de una conducta delictiva, existen elementos importantes de identificar, para que la misma sea considerada propiamente como tal. De los conceptos propuestos en el apartado anterior, se destaca que los delitos son cometidos por una persona en perjuicio de otra persona (obviamente no se puede delinquir en contra de

sí mismo) por lo tanto es necesario un sujeto activo (quien comete el delito) y un sujeto pasivo (en contra de quien se comete el delito) así mismo este delito debe recaer sobre un bien jurídico protegido, por el derecho penal comun, como la propiedad, la intimidad y el honor etc. por lo que se analizan estos elementos a continuación.

El bien jurídico protegido

Algunos autores como el Dr. Santiago Acurio del Pino establecen que la tendencia en la protección de los bienes jurídicos surge desde la perspectiva de los delitos tradicionales, a los cuales se les realiza una re-interpretación teleológica de los tipos penales que existen en el derecho comun de cada país, a la vez que se intenta abarcar las nuevas acciones derivadas de los "novedosos comportamientos delictivos".

Evidentemente esta reinterpretacíon a la que el autor hace referencia, ha sido una concpción astuta de los administradores de justicia, pues esto puede de algun modo facilitar la persecución y sanción del delito, así como su encuadre de típicidad.

La Doctrina establece que las tendencias en el uso de la tecnología de la denominada "Sociedad de la

Información" apuntan a que el bien jurídico predominante en estas relaciones es la **información** abordados desde la óptica de la propiedad intangible.

Partiendo de esta premisa Pablo Palazzi[35] plantea que la información como bien intangible debe ser tratada igual que los bienes físicos, en sentido de su valor intrínseco, que para el Dr. Acurio es su valoración económica, por tanto la información al igual que otros elelemtos intangibles son objetos de propiedad, la cual esta constitucionalmente es protegida. la protección de la información como bien jurídico protegido dentro de la tipificación de los delitos informáticos debe tener siempre en cuenta el principio general de la protección de los bienes jurídicos que establece la penalidad de las conductas que produzcan un "daño" o "lesividad" al referido bien.

En general, el bien jurídico protegido es la información, pero debe valorarse desde diferentes perspectivas, ya sea como un valor económico, como lo plantea Palazzi, o como valor intrínseco de la persona,

[35] PALAZZI Pablo Andrés, Virus Informáticos y Responsabilidad Penal, sección doctrina del diario La Ley, 16 de diciembre de 1992.

como lo establece Acurio del Pino, pues estos se equiparan a los bienes jurídicos protegidos tradicionales tales como los son:

1. **El patrimonio**, en el caso de los delitos económicos y fraudes informáticos así como las manipulaciones de datos que da a lugar.
2. **La intimidad, el honor y la protección de datos personales**: en el caso de agresiones por medios informáticos a la intimidad y al honor en forma general, especialmente en redes sociales o cualquier base de datos.
3. **La fe pública, probatoria y documental:** en el caso de falsificacion de datos o documentos probatorios vía medios informáticos.
4. **La propiedad privada:** en el caso de la información o los elementos físicos, materiales de un sistema informático., que es afectado por los de daños en el llamado terrorismo informático.

Por tanto el bien jurídico protegido esta basado en la confidencialidad, integridad y la disponibilidad de

la información y de los sistemas informáticos donde esta se almacena o transfiere.

El sujeto activo

Las personas que cometen "Delitos Informáticos" poseen ciertas características especiales respecto de los delincuentes comunes, pues se requiere que los sujetos activos tengan destrezas específicas en el manejo de los sistemas informáticos. Los autores de los delitos informáticos suelen conocer los lugares estratégicos donde se obtiene o procesa información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, desconocen los tipos de seguridad o el sistema que protege la información a la que apuntan y que faciliten la comisión de este tipo de delitos.

Según el Manual de las Naciones Unidas para la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos cometidos haciendo uso de la computadora fueron ejecutados por empleados de la propia empresa afectada, a este grupo se le denomina los agentes internos o **Insiders.** Mientras que otros estudios indican que el 23% de la actividad delictiva

informática es cometida por agentes externos al sujeto afectado es decir por **Outsiders**.

Del Pino plantea que las aptitudes de los delincuentes informáticos son tema de debate, pues algunos autores consideran que la capacidad de estos sujetos no es indicador de delincuencia informática en contraposición a aquellos autores que enmarcan a los delincuentes informáticos como personas listas, decididas y motivadas, con características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Autores como Edwin Sutherland sostienen que las características de las personas que cometen los "**delitos informáticos**", pueden ser comparados con los de las personas que cometen "**delitos de cuello blanco**" en sentido que estos sujetos son "*... personas de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.*"

A pesar de los debates sobre las características de los sujetos activos en la comisión de los delitos

informáticos, existen dos elementos que son "necesarios" en la configuración de estos sujetos independiente de los rasgos antes planteados; primeramente, es necesario que el sujeto posea conocimientos técnicos en informática y habilidades especiales para la comisión del delito, y en segundo lugar, es necesario que este sujeto cuente con una motivación especial para cometer el ilícito.

El sujeto pasivo

Haciendo uso de los términos del derecho penal común se entenderá que el sujeto pasivo es la persona física o jurídica sobre quien recae el daño o peligro causado por el sujeto activo, a este sujeto se le denomina también "la víctima" aun que a diferencia de los delitos comunes, si la extensión del daño involucra a otras personas, estas también serán consideradas como víctimas y no como ofendidos.

En el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones creditícias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros. La importancia del estudio del

sujeto pasivo radica en que éste ayuda a la tipificación de los delitos; es decir que es el sujeto pasivo quien ofrece la información que posteriormente es recogida ley positividaza en las diferentes leyes nacionales e internacionales.

Teoría del delito informático

De la acción y omisión

Al igual que en todos los delitos, la base para la concepción teórica de los delitos informáticos es la conducta humana, pues el eje conductor y sustrato material necesario para su existencia. Ya que la conducta humana es expresada mediante las acciones no puede concebirse la ejecución de un delito sin un acto en el que se plasme la consideración axiológica[36] del hecho punible desde un elemento causal o finalista derivado de dicha acción. Como ya lo han planteado Franz Von Liszt y Hans Welze respectivamente.

La Omisión también es una expresión pasiva de la conducta humana, que requiere, para su concepción

[36] Citados por: Muñoz Conde, Francisco; García Arán, Mercedes (2004). *Derecho Penal. Parte General* (6.ª edición). Valencia: Tirant lo Blanch. p. 205. ISBN 9788484561163. OCLC 318274714.

teórica y para la consideración axiológica del hecho punible, la abstención consistente de la realización de una acción. Por sí misma, la omisión no es un elemento constitutivo de delito, si no que debe reunir los aspectos de artículo 12 incisos segundo y cuarto del Código Penal, en sentido que se considerará realizado el hecho punible cuando la omisión se realiza *"en el momento en que debió tener lugar la acción omitida."*

El artículo 20 del mismo código, establece las condiciones bajo las cuales, se considerará cometido un delito por omisión, las cuales específicamente se derivan del deber jurídico de obrar para impedir el resultado; esto es cuando el sujeto tenga:

1. Obligaciones de cuidado,
2. Obligaciones de protección,
3. Obligaciones de vigilancia.

Por ejemplo, si un sujeto encargado de la seguridad de una base de datos, se abstiene voluntariamente de realizar alguna de las acciones para asegurarla con la finalidad de facilitar el acceso o la vulneración de dicha base de datos, automáticamente

estaría incurriendo en el delito de posesión de equipos o prestación de servicios para la vulneración de la seguridad, del artículo 8 de la Ley Contra Delitos Informáticos y Conexos, bajo la modalidad de comisión por omisión, pues fue la ausencia de la acción, mas la falta a su obligación de protección lo que "facilitó" la vulneración de seguridad.

Para el caso específico de los delitos informáticos, la acción u omisión es determinante para su consideración como delitos, pues la mayoría de acciones informáticas delictivas, tienen las mismas características de **los delitos de ejecución instantánea y no admiten el grado de tentativa**. Así el acto de crear un código ejecutable con la sintaxis de un virus de computadora, no es constitutivo de delito, hasta que sea realizada la acción considerada como punible, por ejemplo la del artículo 7 de la Ley Especial Contra Delitos Informáticos y Conexos exige que se destruya, dañe, modifique o se ejecute un programa con el fin de alterar el funcionamiento de un sistema informático, entonces, mientras no se produzca tal efecto, el acto de

desarrollar un virus de computadora no es constitutivo de delito.

Por otro lado, si tomamos el ejemplo del artículo 4 de la misma ley, se establece que: quien sin autorización o excediendo la autorización concedida "acceda" a un sistema informático será sancionado con prisión de uno a cuatro años; en este punto, la conducta punible es la acción de ingresar sin autorización o rebasando el límite de autorización establecido, por lo tanto no hay existencia de actos directos o apropiados para la consumación del delito pues este se consumó instantáneamente al realizarse la acción como esta establecido en el artículo 24 del Código Penal. La inexistencia de la voluntad de "accesar" a un sistema informático previo a la acción, se considerará entonces como desistimiento en los términos del artículo 25 del mismo código.

La tipicidad

Para Claus Roxin la tipicidad, es aquella adecuación de la conducta humana considerada como delito, dentro dentro de las leyes específicas y responde de manera directa al principio de legalidad, según el

cual, todos los delitos provocados por la acción u omisión voluntaria del sujeto, deben estar regulados por la ley.

Por regla general, en el tipo penal se deben establecer todas las características de la acción considerada como delictiva, sin embargo, la multiplicidad de actos que se pueden realizar por medios informáticos, dificulta el trabajo de tipificación, aun que, a fin de no vulnerar el principio de legalidad, se ha realizado en la legislación salvadoreña una tipificación general, que obliga a la consideración de los aspectos de cada caso para su abordaje, lo cual podría convertirse en si mismo en un campo de estudio, por lo tanto, debido al carácter introductorio de este texto no se abordarán estos tipos penales, pero es necesario destacar que la mayoría de los tipos penales de la Ley Contra los Delitos Informáticos y Conexos, requieren de una apropiada argumentación jurídica por parte del ministerio público para su tratamiento.

La antijuridicidad

Según Günther Jakobs, en términos axiológicos ,la antijuridicidad de los hechos delictivos, representa

aquellos antivalores de la conducta humana, es decir que son la clarificación que las conductas son contrarias a derecho. Para fines de este estudio, se pretende destacar, que en este nivel de la teoría del delito existen determinadas **causas de justificación** que son aplicables sobre aquellas acciones que han cumplido con las características antes planteadas y que por lo tanto podrían considerarse como delitos informáticos. Dichas causas de justificación son las siguientes:

Consentimiento del titular de bien jurídico protegido: no puede concebir la comisión de un delito cuando ha mediado el consentimiento expreso, tácito o presunto de quien fuera considerado como sujeto sujeto pasivo. Así en el caso del artículo 4 de la LECDIC si el titular de un sistema informático ha dado su autorización (sin que exista vicio) para que un tercero pueda accesar, no se configuran los extremos del delito, no solo por su atipicidad, sino que también por su antijuridicidad

Legítima defensa: se considera como una excepción de antijuridicidad cuando la acción del sujeto está orientada a repeler una agresión en progreso o

inminente en contra de cualquiera de sus bienes jurídicamente protegidos. La legitima defensa exige que el contraataque sea ejecutado en contra del agresor exclusivamente, que dicha agresión se injusta, y que este contraataque sea proporcional a la agresión, y que los medios para contraatacar sean racionales. Por ejemplo, en el año 2010 Google[37] repelió el famoso "*ataque aurora*" perpetrado por un grupo de hackers chinos, en el cual, google no solo accesó a los servidores de los agresores para detener el ataque, sino que descubrió varios ataques en contra de otras 30 compañías como Adobe y otros, lo que sirvió para prevenirlos.

Estado de necesidad: esta excepción, a diferencia de la legitima defensa, requiere que la acción orientada a salvaguardar el bien jurídico protegido recaiga sobre un tercero cuyos bienes son de un valor igual o menor al que se pretendía proteger, además que el daño cometido por el sujeto que repele la agresión, no sea cometido con dolo y que el daño a los bienes del tercero sea la única forma de protección.

[37] SANGER, D. E., & MARKOFF, J. (2010, January 15). After Google's Stand on China, U.S. Treads Lightly. Retrieved March 20, 2018, from http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?ref=technology

Ejercicio de un derecho: esta excepción surge cuando se causa algún daño a los bienes jurídicos de otro habiendo obrado en forma legítima, o cuando ha existido la necesidad racional del medio empleado. Por ejemplo, cuando para fines educativos, se requiere que los alumnos aprendan a identificar y repeler ciberataques, se pueden realizar actividades típicas de un delito pero en estas acciones, no solo media el consentimiento sino que también se está ejerciendo un derecho, por lo que no será constitutivo de delito.

Cumplimiento de un deber: se alega cuando se causa un daño a los bienes jurídicos cuando se está actuando de forma legítima en el cumplimiento de un deber, este deber puede nacer de la jerarquía en una relación laboral o en el ejercicio de una profesión etc. en todo caso siempre debe existir la necesidad racional del medio empleado.

La culpabilidad

Según De la Cuesta[38], en el nivel de la culpabilidad es donde se detallan aquellas

[38] De la Cuesta Aguado,*Culpabilidad. Exigibilidad y razones para la exculpación.* Madrid, 2004

circunstancias específicas objetivas y subjetivas que concurrieron en la persona del autor en el momento de la comisión del hecho ya calificado como típico y antijurídico. Se trata del elemento donde se discute la relación dialéctica del hecho cometido y la sanción impuesta por el Estado.

De estas circunstancias se destacan:

El Dolo: que consiste básicamente en el **conocimiento** que la acción a cometerse constituye un delito más **la voluntad** de realizar dicha acción, y no representa ninguna excluyente de culpabilidad.

La culpa: Consiste en el conocimiento que la acción está tipificada como delito, pero sin que concurra la voluntad de realizar dicha acción, la cual pudo haberse cometido por impericia o imprudencia del sujeto en la mayoria de los casos esta es una circunstancia atenuante de la responsabilidad penal junto con las planteadas en el artículo 29 del Código Penal. Cuando la acción culposa sea ocasionada por un error, se aplicará entonces la disposición del artículo 28 del mismo código.

Existe un último nivel en la teoría del delito, que es la Punibilidad, sin embargo, esta no está incluida en este apartado, por que la calidad del sujeto activo para cometer delitos informáticos no encaja en las circunstancias contenidas en este nivel, y las excepciones, deberán ser consideradas en cada caso, en fases procesales que no son parte de este análisis.

Clasificación de los delitos informáticos

Como ya se ha mencionado en los apartados anteriores, la diversidad de los delitos informáticos responde a la acción realizada por el sujeto activo sobre el sujeto pasivo, y de este modo es que se los delitos han sido clasificador en las diferentes legislaciones. Para fines de este estudio abordaremos la clasificación que la ONU y la clasificación de la Ley Especial Contra los Delitos Informáticos y Conexos de El Salvador junto con algunas consideraciones de Acurio del Pino[39].

[39] Acurio del Pino, Santiago, Delitos Informáticos: generalidades, chile, 2006

El fraude informático

El artículo 11 de la ley establece que **Fraude Informático** es *"...el que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado con prisión de tres a seis años."*

Este tipo de fraudes pueden realizarse por diferentes métodos, por ejemplo:

La inserción de datos falsos o engañosos (Data diddling), Esta forma consiste básicamente en una manipulación de datos de entrada al computador con el objeto de emular y producir movimientos falsos en transacciones generalmente de dinero. Este tipo de fraude informático. conocido también como **intruducción de datos falsos**, afecta principalmente a instituciones financieras y empresas que realizan transacciones con alto volumen de capital; Este delito es tambien uno de los mas comunes pues es fácil de

cometer y difícil de descubrir. Generalmente es realizado por personas que tienen acceso directo o indirecto a las transacciones .

“Caballos de Troya” (Troyan Horses) Este fraude busca alterar la lógica de los programas existentes en el sistema informático o insertar nuevos códigos a los programas o nuevas rutinas a fin de obtener información o manipular computadores de forma remota. De este modo la computadora realiza funciones no autorizadas paralelamente con sus funciones normales.

La técnica del salami (Rounching Down), Esta forma de delito se inserta en las repeticiones automáticas de los procesos de cómputo. Esta técnica separa “rodajas muy finas” de datos, apenas perceptibles, de transacciones financieras, y van desviando fondos repetidamente de una o varias cuentas a otra. Generalmente se inserta un código en el programa que realiza dichas transacciones con instrucciones que remita a una cuenta determinada, centavos de dinero de muchas cuentas corrientes.

Falsificación informática: según el dr. Acurio esta modalidad tiene dos dimensiones, la primera es **la falsificación como objeto:** que consiste en la alteración de los datos contenidos en los documentos almacenados en discos duros, servidores u otros medios de forma computarizada. La segunda es **la falsificación como instrumento:** En este caso, el delincuente se vale de los sistemas informáticos para realizar falsificaciones de documentos de uso comercial. Se modifican documentos que se imprimen luego e incluso se pueden crear documentos falsos sin tener que recurrir a un original. De esta posibilidad es que ha surgido un debate entre los teóricos del derecho penal, pues cuando se duplica un documento digital, en realidad se está creando otro documento original con los mismos datos que el anterior y con la posibilidad de ser editado o modificado de igual forma que el documento originario.[40]Por lo tanto existe dificultad para definir el alcance de los conceptos de falsificación o piratería.

[40] Se denomina documento originario, a aquel primer documento del cual se hacen las copias, pues se entiende que cada copia es un "original" con los mismos valores que el archivo del cual se duplicó.

Manipulación de los datos de salida: Es aquel que se realiza introduciendo comandos orientados a un objetivo que altere el funcionamiento del sistema informático. El ejemplo más común es la clonación de bandas magnéticas, principalmente utilizadas en tarjetas de crédito y débito; usualmente estos fraudes también pueden usar un equipo especializado de harware y programas de computadora para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito y así poder acceder a los cajeros electrónicos.

Pishing: Esta modalidad de fraude informático es muy comun en redes sociales en la actualidad, su finalidad principal es robar o suplantar la identidad del sujeto pasivo y de este modo obtener información, como números de tarjeta de crédito, contraseñas, cuentas en redes sociales u otros datos personales por medio de engaños.

El medio principal de este fraude son los mensajes de correo electrónico o de ventanas emergentes para las computadoras, en incluso notificaciones “push” en los dispositivos móviles. El

robo de identidad también se tipifica en otra serie de delitos ademas del fraude, sin embargo se ha incluido en esta parte por que la mayoría de las víctimas sufren agravios económicos en sus cuentas de tarjetas de crédito, incluso los delincuentes adquieren bienes o servicios utilizando la identidad del sujeto pasivo llegando incluso a solicitar hipotecas en nombre de su víctima.

El autor plantea ademas que existe una nueva modalidad de Pishing llamado Spear Pishing o Pishing segmentada, el cual funciona atacando a grupos determinados, buscando grupos de personas vulnerables y no a una sola persona.

El sabotaje informático.

La legislación salvadoreña considera el sabotaje como la destrucción, daño, modificación o ejecución que altere el funcionamiento o inhabilite parcial o totalmente un sistema informático[41] así como las demás acciones orientadas a borrar, suprimir o modificar sin autorización funciones o datos de computadora. Es

[41] Artículo 7 de la Ley Especial Contra Delitos Informáticos y Conexos

importante observar que la ley salvadoreña no solo enfatiza en la intención (el dolo) de obstaculizar el funcionamiento normal del sistema como requisito para el perfeccionamiento del acto, sino que también sanciona los actos realizados realizados por imprudencia, negligencia, impericia o inobservancia de las normas, lo que abre un debate sobre la sanción de los actos inintencionados según lo plantea Mauricio Zarceño[42], insertar una memoria infectada con un virus en un puerto USB de una computadora ajena, es una acción muy común que a pesar de estar exenta de dolo, podría encajarse en el tipo penal de la referida ley en su artículo 7, por lo que es necesario tomar en cuenta otros aspectos externos al tipo penal y a la teoría del delito para poder excluirlo como delito, es decir, se deben tomar en cuenta los vínculos por ejemplo entre el dueño de la computadora y el dueño de la USB entre otros aspectos subjetivos.

Mas allá de estos debates, a continuación se abordan algunos formas en las que se cometen los sabotajes informáticos:

[42] Mauricio Zarceño, Consideraciones sobre los delitos informáticos, entrevista personal del fecha 14 de Diciembre de 2017

Las Bombas lógicas (logic bombs), Esta modalidad retrasa el daño a causarse a un tiempo determinado o cuando se cumplan algunos requisitos específicos, generalmente este tipo de ataque apunta a la destrucción o modificación de datos en un momento dado del futuro, mediante la inserción de un programa oculto; A diferencia de los virus y los gusanos, las bombas lógicas son insertadas sin que estas ejecuten ninguna función inmediata, por lo que son difíciles de detectar, por eso, los daños que suelen causar son importantes y difíciles de revertir, especialmente en el caso que la bomba lógica haya sido programada para "detonar" en un momento vulnerable. Ademas proporciona suficiente tiempo al delincuente para que pueda ocultar sus rastros.

Los gusanos. Se desarrolla de manera similar al virus y con la misma finalidad de ser insertado en programas legítimos de procesamiento de datos para que pueda modificar o destruirlos, pero es diferente del virus pues este suele autodestruirse luego de causar el daño, generalmente los gusanos son orientados a un

solo objetivo, mientras que los virus tinen un rango más amplio de impacto.

Malware y virus informático, Estos elementos, emulan la reproducción biológica de las enfermedades, (de ahí su nombre) pues se alojan en su huesped, que en este caso puede ser una computadora o cualquier equipo informático y luego se reproducen, y extienden alijandose en todos aquellos dispositivos (o nuevos huespedes) a los que acceden, se "contagian" de un sistema a otro al igual que un vector.

En palabras de Ricardo Guibourg los virus son "*pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autorreporducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar"*[43].

El Ciberterrorismo: También denominado terrorismo informático son todos aquellos actos deliberados, orientados a ejercer presión sobre grupos

[43] GUIBOURG Ricardo A., ALENDE Jorge O., CAMPANELLA Elena M., Manual de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires, Argentina.

específicos, especialmente gobiernos o empresas haciendo uso de las técnicas propias del sabotaje informático, es decir que este delito se configura eminentemente por el sujeto pasivo más que por la técnica utilizada en el ciber ataque, es decir que puede ejecutarse con otro tipo de delitos informáticos, pues la condición para configurarse como ciberterrorismo es que esté basado en determinadas características; la primera, es que el delito debe estar orientado a provocar desestabilización del grupo objetivo por medio del terror. La segunda es que la desestabilización debe provocarse exclusivamente en el campo del ciber espacio, pues cualquier intervención física, convierte el delito en terrorismo común. Finalmente, algunos autores como Lacobucci[44] establece que el ataque de ciberterrorismo debe estar orientado a vulnerar infraestructuras críticas.

[44] Nelson, B. Choi, R. Lacobucci M. y otros, "Cyberterror: prospects and implications" Center for the study of terrorism and irregular warfare. Monterrey California. 1999.

El espionaje informático y el robo o hurto de software:

Fuga de datos (data leakage), se le conoce a este delito como la divulgación no autorizada de datos reservados, la legislación salvadoreña lo contempla en el artículo 24 de la ley especial contra delitos informáticos y conexos estableciendo que: *"El que sin autorización da a conocer un código, contraseña de acceso o cualquier otro medio de acceder a un programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse así mismo, a un tercero o para cometer un delito, será sancionado con prisión de cinco a ocho años."*

De esta tipificación hay que resaltar dos elementos importantes; El primero es que el delito se consuma cuando la información para acceder es entregada o revelada sin autorización, lo que quiere decir que esta información puede ser adquirida por medios lícitos, o en virtud de las actividades cotidianas del potencial delincuente y no necesariamente por medio de otros delitos, como en el caso de los fraudes; El segundo elemento es que la revelación de esta información debe contener un *ánimo de lucro*, es decir

que debe hacerse con la intención de lucrarse a sí mismo o a un tercero.

El ámbito más común para este delito es el espionaje industrial que sustrae información confidencial de una empresa. Como lo explica Luis Camacho Lozala complejidad en la definición del momento de la consumación del delito radica en "*la facilidad existente para efectuar una copia de un fichero mecanizado con tal magnitud, rapidez y simplicidad"...* por lo que es *"...una forma de delito prácticamente al alcance de cualquiera*"[45]

Finalmente, hay que destacar que ninguna información está segura en un 100%, para la protección ante la fuga de información, los expertos en seguridad informática, establecen una suerte de "obstáculos" que dificultan la adquisición de la información, como por ejemplo, la criptografía y otros métodos de seguridad informática que no se abordarán en este texto.

Reproducción no autorizada de programas informáticos. Sobre este delito existen diferentes

[45] CAMACHO LOSA, Luis, El Delito Informático, Madrid, España, 1987.

consideraciones, en diversas consideraciones, pues en esta clase de delitos, el bien jurídico no es la información sino los derechos de autor, sin embargo, segun otras legislaciones, la reproducción realizada por ejemplo por los denominados "crackers" si afecta a la información pues estos hacen uso de la ingeniería inversa o la piratería para "romper" (crack) la protección del software propietario para hacerlo accesible a todo el mundo. Aquí es de destacar que el móvil de los "crackers" o de quienes realizan este tipo de actos antijurídicos, no es el ánimo de lucro, sino la afectación económica del dueño del software propietario, es decir que el "crack" en sí no es constitutivo de delito, sino la reproducción sin autorización.

La legislación salvadoreña, no contempla la piratería informática, pues como ya se ha dicho anteriormente, una copia de un fichero, no constituye una copia "pirata" pues en la mayoria de legislaciones (al igual que la salvadoreña) la piratería implica una "copia de inferior calidad" mientras que la copia de un fichero es otro fichero exactamente igual, con las

mismas características e igual calidad, incluso con la misma susceptibilidad de ser modificado como un original.

El robo de servicios:

Hurto por medios informáticos. La ley en estudio establece que este delito consiste en apoderarse de bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro.[46] Un ejemplo de esto es el uso de Internet, en el cual las empresas proveedora de este servicio proporciona una clave WEP o WPA2 para la red WIFI de acceso al usuario de Internet, pero esta clave es hurtada mediante el uso de programas de obtención de claves WIFI, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

Apropiación indebida de información residual (Scavenging) Se establece como el aprovechamiento de la información que luego de haber sido utilizada en otros proyectos o programas autorizados y protegidos,

[46] Hurto por medios informáticos, artículo 13, Ley Especial contra delitos informáticos y conexos.

es abandonada sin ninguna protección como residuo de este. *"To scavenge"*, es la acción en de "recoger basura" por su traducción del inglés. Normalmente se hace tomando la información residual que ha quedado en memoria o soportes magnéticos o en la carpeta papelera de las computadoras.

Parasitos informáticos (Piggybacking) y Suplantación de personalidad (Impersonation), se refiere a cuando una persona se adhiere a otra persona que está autorizada para entrar en un área restringida, o pasar un determinado punto de control. Esta forma de delito se deriva de la acción física el "*Tailgate*" y hace referencia a aquellas personas que entran sin autorización a un espacio a aprovechando el acceso de otras personas, al colocarse relativamente cerca de ellas para aprovechar el tiempo en que se proporciona acceso para entrar al lugar al que no están autorizados.

En términos informáticos, estos dos actos se realizan de forma conjunta, ya que el parásito es el que obtiene la información de acceso, y luego el delincuente, puede entrar con la identidad de otra persona. Este acto se diferencia de la suplantación de

identidad como fraude en que el acto puede ser legal o ilegal, autorizado o no autorizado, según las circunstancias. Sin embargo, el término más a menudo tiene la connotación de ser un acto ilegal o no autorizado. En estos casos, obtiene el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado otro nivel de confianza en razón de su capacidad y posición al interior de una organización o empresa determinada, en la legislación salvadoreña esta tipificación se encuentra en el artículo 4 de la Ley Especial Contra los Delitos Informáticos y Conexos.

El acceso no autorizado a servicios informáticos:

Las puertas traseras (back doors), Es un método, a menudo secreto, de eludir la autenticación o el cifrado normal en un sistema informático, un producto o un dispositivo incorporado (por ejemplo, un enrutador doméstico) o su realización, como parte de un criptosistema, un algoritmo, un chipset o una

"computadora homúnculo[47]" (como la que se encuentra en la tecnología AMT de Intel). Las puertas traseras se utilizan a menudo para asegurar el acceso remoto a una computadora u obtener acceso a texto sin formato en sistemas criptográficos.

Una puerta trasera puede tomar la forma de una parte oculta de un programa que esta en uso o un programa separado (por ejemplo, *Back Orifice* puede subvertir el sistema a través de un *rootkit* como expresa Crhis Wysopal[48]) o bien puede realizarse a través de un código en el *firmware* del *hardware* o partes de los mismos sistema operativo como Microsoft Windows[49]. Aunque normalmente se instala como un acto ilícito, en algunos casos las puertas traseras son deliberadas y ampliamente conocidas pues este tipo de puertas traseras pueden tener usos "legítimos", como proporcionar al fabricante una forma de restaurar las contraseñas de los usuarios.

---

47 *Eckersley, Peter; Portnoy, Erica (8 May 2017).*"Intel's Management Engine is a security hazard, and users need a way to disable it". *www.eff.org. EFF. Retrieved 15 May 2017.*

48 Chris Wysopal, Chris Eng."Static Detection of Application Backdoors" (PDF). Veracode. Retrieved 2015-03-14.

49 *"Microsoft Back Doors". GNU Operating System. Retrieved 1 July 2017.*

Las contraseñas predeterminadas (u otras credenciales predeterminadas) pueden funcionar como puertas traseras si el usuario no las modifica. Algunas funciones de depuración también pueden actuar como puertas traseras si no se eliminan en la versión de lanzamiento. Un ejemplo del uso ilícito de esta técnica es la descubierta por Larry Mc Voy[50] en 2003, quien descubrió un intento sofisticado de plantar una puerta trasera en el kernel de Linux, añadiendo un pequeño cambio sutil de código al subvertir el sistema de control de revisiones. En este caso, apareció un cambio de dos líneas para verificar los permisos de acceso raíz (Root acces) de una persona que llama la función *sys_wait4*, pero debido a que se utilizó la asignación (=) en lugar de la comprobación de la igualdad (==), en realidad otorgó permisos al sistema. Esta diferencia podría pasarse por alto fácilmente, incluso podría interpretarse como un error tipográfico accidental, en lugar de un ataque intencional, sin embargo sus implicaciones eran importantes.

50 Larry McVoy (November 5, 2003) Linux-Kernel Archive: Re: BK2CVS problem. ussg.iu.edu

Un uso lícito es el uso de una puerta trasera en ciertos productos Samsung con Android, como los dispositivos Galaxy. Las versiones de Android propiedad de Samsung están equipadas con una puerta trasera que proporciona acceso remoto a los datos almacenados en el dispositivo. En particular, el software Samsung Android que está a cargo de manejar las comunicaciones con el módem, utilizando el protocolo Samsung IPC, implementa una clase de solicitudes conocidas como comandos de servidor de archivos remotos (RFS), que permite al operador de puerta trasera realizar a través de un módem remoto Operaciones de E/S (I/O) en el disco duro del dispositivo u otro almacenamiento. Como el módem se está ejecutando el software Android propiedad de Samsung, es probable que ofrezca un control remoto por aire que luego podría usarse para emitir los comandos RFS y, por lo tanto, para acceder al sistema de archivos en el dispositivo.

La llave maestra (Superzapping), es un software informático que permite el acceso a cualquier fichero del computador pasando por todos sus sistemas

de seguridad,generalmente se utiliza con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador. Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación

La interrupción de líneas (Wiretapping), consiste en una interferencia de las líneas telefónicas de transmisión de datos con la finalidad de obtener o interceptar la información que circula por ellas, generalmente se interrumpe, un módem o una impresora. Aun que esta práctica ya no es tan comun debido a los avances en la criptografía que codifica la información y la transforma en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y por aplicación de las mismas claves, la información se recompone hasta quedar exactamente igual a la que se envió en origen.

Capítulo 3

Peritajes Informáticos

El análisis forense es un área principalmente del ámbito de la seguridad informática y ha adquirido mucha importancia a raíz del incremento de los diferentes incidentes de seguridad. Sin embargo, como el análisis forense se realiza posterior a los incidentes de seguridad, se relaciona también de forma directa con el derecho, principalmente con la propiedad, la imagen etc. y no importa que las acciones tengan una aplicación judicial, actualmente, las empresas y las personas estan haciendo uso cada vez mas de la informática forense para la solución de problemas de seguridad y otros conflictos.

De manera general muchos autores coinciden en que la informática forense es un conjunto de técnicas orientadas a la adquisición, preservación, análisis y presentación de la prueba informática, sin atribuirse ninguno de estos, la autoría del concepto. El Buró

Federal de Investigación de los Estados Unidos establece que la informática forense es *"la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional".*

Adicionalmente se le conoce a esta disciplina también como: Computación Forense (computer forensics) que es la disciplina que procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con un caso; también se conceptualizar como una disciplina científica y especializada que ofrece un análisis de la información residente en equipos informáticos.

Otros conceptos comúnmente utilizados como equivalentes a la informática forense son el análisis forense digital (digital forensics), examen forense digital debido a la forma de aplicar conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, estas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar

las características técnicas del uso aplicado a los datos y bienes informáticos.

Principalmente, la informática forense tiene dos usos específicos:

A) **Para la recuperación de datos**; por recuperación se entiende que se intenta accesar o reconstruir aquellos datos que han sido borrados, robados o que se encuentran en dispositivos dañados.

B) **Para la reconstrucción de líneas de tiempo (timelines);** que determinen lo que ha sucedido con los dispositivos informáticos, o para hacer comprobaciones de determinada actividad.

El perfil del perito informático

El perito en informática es más una carrera que un titulo como tal, desde un primer acercamiento podemos decir que existen dos grandes categorías, aquellos peritos denominados “de carrera”, que son aquellos que se dedican por completo a este ejecicio, y que generalmente se encuentran empleados en algun sector publico o privado que requiere sus habilidades, por ejemplo las agencias policiales, los organos

judiciales y del ministerio público etc, mientras que en el sector privado, existen agencias de peritos y de investigación que utilizan este recurso. La segunda categoría es aquella donde se encajan los peritos ocasionales o "*ad hoc*" es decir, que es posible contratar a un profesional de la informática, para que aplique sus conocimientos y pueda ejercer (para un caso específico) como perito.

En ambos casos, es indudable que el requisito primordial para hacer un peritaje informático es que el profesional sea un experto. Es decir que el perito debe tener formación y experiencia en el área objeto de la pericia, más que una formación forense como tal, esto es por que se requiere que pueda presentar un punto de vista basado en hechos y métodos científicos al respecto de las cuestiones que se le presentan. Además el perito debe ser en todos los casos, un profesional independiente e imparcial. Es decir que no debe tener vínculos con las partes del proceso, ni intereses en el conflicto; Tambien debe poseer un estado mental agudo y abierto que le permita emitir una opinión libre de prejuicios. Así la independencia se percibe desde un

enfoque objetivo por que se basa en circunstancias de hecho, mientras que la imparcialidad se percibe como desde un enfoque más subjetivo por ser un estado mental del profesional que sólo puede llegar a expresarse por medio de la conducta.

Es necesario que el perito tenga la habilidad de explicar lo que ha realizado con un lenguaje sencillo y fácil de comprender, especialmente porque debe presentar su dictamen a otras personas que probablemente no son del área como jueces o la parte que lo contrató, pero al mismo tiempo este dictamen debe tener suficiente sustento técnico para que pueda soportar un contraperitaje o verificación; por lo tanto, es importante tomar en cuenta que los dictámenes periciales deben exponer los resultados en la forma que fueron encontrados, aun que esto afecte a la parte que ha contratado al perito, pues el dictamen debe ser libre, comprobable y sin alusiones al caso principal, sino que solo al objeto de la pericia.

El peritaje informático y los peritajes en general tienen una función probatoria de los indicios que son motivo de controversia, por lo tanto su dictamen es

necesario para comprobar los puntos que sirven para resolver un caso pero no se orientan a todo el caso. En otras palabras, los peritos no son los encargados de resolver los casos pues su función no es investigativa sino probatoria es decir que trata de extraer hechos, comprobados a un nivel científico de las evidencias observadas y no de todo el caso. Por lo tanto el perfil del perito debe incluir conocimientos de las reglas que operan en el procedimiento que se está realizando y para el cual ha sido contratado.

Metodología de la pericia informática

En nuestro país no existe un lineamiento para la realización de peritajes informáticos ni una ley que regule esta práctica, pero consuetudinariamente y haciendo uso del derecho comparado se han consolidado a nivel internacional algunos elementos básicos para la realización de un peritaje informático standard, tomando encuentra algunos principios fundamentales del derecho probatorio y de la teoría general del proceso.

Formalización de la solicitud de peritaje

Dependiendo del tipo de proceso y de quien solicita el peritaje, la formalización de la solicitud o contratación de perito se clasifica en:

A) solicitud a petición de parte y B) requerimiento judicial; en el primero, son cada una de las partes interesadas en resolver un litigio (judicial o extrajudicial) quienes de común acuerdo o por separado, contratan los servicios de un perito informático para la realización de la pericia. En este caso son las partes en su conjunto, o la parte que ha contratado al perito quien incurre en el pago de honorarios. En el segundo caso, es mediante una orden judicial que se requieren los servicios del perito, ya sea para la elaboración de un dictamen pericial o para la evaluación de algún dictamen previamente propuesto por alguna de las partes, a esta practica se le denomina "contraperitaje". En todo caso, será el juez quien determine la forma de cubrir los honorarios del perito, ya sea mediante el uso del presupuesto para tal efecto, o adhiriéndolo a los costes procesales que deberá cancelar la parte que sea vencida en juicio.

En todo caso la aceptación de un encargo pericial debe quedar debidamente formalizado ya sea mediante un contrato (en caso de ser a propuesta de parte) o mediante escrito de aceptación (en caso de requerimiento judicial). En ambos casos, debe quedar explícitamente definido que el perito ha aceptado el encargo, los elementos sobre los cuales se realizará el peritaje, la infraestructura a las que tendrá acceso, etc. con el objeto de cubrir la responsabilidad del perito en cuanto al acceso a la información interesada, este tema se abordará mas profundamente en la sección de contratos informáticos.

Para el caso de requerimientos judiciales, es conveniente tomar en cuenta la jurisdicción en la que se ha abierto el caso (penal, civil, administrativo, etc) para poder informarse sobre el proceso que se está llevando a cabo según la ley procesal correspondiente. Naturalmente es imprescindible la referencia del caso y el juzgado. Es recomendable prestar atención a las partes en litigio para evitar cualquier conflicto de intereses.

Conservación de la cadena de custodia

Habiendo aceptado realizar una practica forense a petición de parte, quienes han requerido los servicios periciales y el perito, deberán comparecer ante un notario para levantar acta de la entrega de la evidencia, es importante aclarar que las pericias informáticas se realizan estrictamente en todos aquellos dispositivos que guardan información de forma digital haciendo uso de algún sistema informático o telemático. En ese sentido, normalmente la evidencia será: Computadores (PC y Laptop), teléfonos móviles, cualquier tipo de memorias (USB, SD, Stick Duo etc), discos duros etc.

Tanto el notario como las partes, levantarán un registro fotográfico y un inventario detallado de los elementos entregados al perito, haciendo constar en el acta: la cantidad de elementos entregados, la marca, modelo, numero de serie y el estado en el que se recibe (pues en algunos casos los dispositivos pueden presentar algún grado de deterioro o destrucción). Finalmente, las partes firman a conformidad y el notario procede a cerrar el acta y a autenticar las firmas de los presentes.

La doctrina establece tres categorías de evidencia:

1. Registros generados por computador: Son todos aquellos que son creados como efecto de la programación de un computador. Los registros generados por computador son por regla general inalterables por una persona, pues estos registros son generalmente registros de eventos de seguridad (*logs*) y sirven para demostrar el correcto y adecuado funcionamiento del sistema o computador que generó el registro en términos de prueba.

2. Registros almacenados por o en computadores: Por regla general estos registros son generados por una persona, y son almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras, fotos, videos, historiales de navegación etc. El valor probatorio de estos registros es lograr demostrar la identidad de quien generó esta información, y probar los hechos o afirmaciones contenidas en ella.

3. Registros híbridos: Los registros híbridos son aquellos que combinan ediciones humanas y *logs*, el

elemento que reúne esta condición es en la mayoría de los casos son los *hash*.

Cálculo de *Hashes*

Antes de comenzar a trabajar con la información, es necesario calcular los *hash* de todos los ficheros que se encuentran en los dispositivos que han sido entregados, y a partir de ahí, elaborar un registro en forma de bitácora, ya que si un juez, solicita al perito una ratificación de su informe, este solamente se remitirá a los *hashes* para determinar que sus resultados han partido desde ahí; También en caso que la parte contraria presente un peritaje con resultados diferentes, el registro de los *hashes* será el punto de partida para ambos. De hecho, para la realización de contraperitajes, el perito judicial, ratificará estos registros y el método que se ha plasmado en el dictamen pericial.

El cálculo de los *hashes* nos ayuda demostrar el estado en que se han recibido los datos, y también para comprobar una eventual modificación de ficheros durante una investigación para calcular los *hashes* existen una gran variedad de programas como **File**

Checksum Utility para Windows que es una herramienta diseñada para calcular fácilmente el hash de cualquier archivo o carpeta

Esta herramienta nos permite calcular distintas sumas de integridad utilizado distintos algoritmos:

- MD5
- SHA-1
- SHA-256
- SHA-512
- RIPEMD

Además, permite guardar la suma de los archivos en un documento de texto o una hoja de cálculo para que más adelante pueda ser recuperado.

Si se utilizan distribuciones de código abierto (GNU/Linux y Unix en general) los dispositivos del sistema se asocian a un punto estructurado en el sistema de ficheros. Los medios de almacenamiento, usan la siguiente estructura **/dev/nombre con nombre** en donde se utilizan los valores hda1, sda1, etc. La letra "a" hace referencia a la identificación del medio y el número "1" a la partición.

Estos medios de almacenamiento se "montan"[51] y se crea un conjunto de estructuras en el sistema operativo que enlaza el dispositivo (por ejemplo /dev/sda1,) con un punto de montaje (por ejemplo /media/disco1). Los medios de almacenamiento que se encuentran bajo **/dev** pueden ser accedidos directamente como dispositivos de bloques, sin ningún tipo de estructura, que correspondería a la capa de sistema de ficheros.

Una vez montados los dispositivos se puede proceder al calculo de los hash mediante siguiente comando.

root@kali:~$ find $@ ! -type d -print0 | xargs -0 sha1sum | tee /media/disk/

colocando al final la dirección del fichero a calcular. También se pueden calcular los otros hash utilizando los comandos **sha1sum, sha2sum y md5sum.**

Clonado de medios

Una vez se ha realizado el cálculo del los *hashes* de los ficheros que se han recibido, el siguiente paso es,

[51] Traducción literal del la función "mount"

hacer un clonado de medios; esto es para que las pruebas que se realicen no afecten los únicos archivos que tenemos, sino que por el contrario, sirvan para poder contrastarlos luego con los archivos originales para establecer conclusiones o líneas de tiempo como ya se ha dicho. Es necesario realizar una clonacion por cada prueba a realizarse como mínimo, y posterior a cada prueba, se deberán calcular de nuevo los hashes y anotarse en la bitácora de la pericia.

Existen diferentes herramientas para realizar el clonado de medios, pero para fines de este estudio se hará énfasis en el comando **dd** y sus derivados. El comando dd es el utilizado en las diferentes distribuciones con arquitectura Unix. Por tanto este comando es uno de los más comunes. Para Joaquim Anguas[52]Existen tres variantes principales de dd: **dd, dcfldd y dc3dd.**

Las opciones principales para dd son:

[52] Anguas, Joaquim. "Peritaje en Informática: escenarios, conceptos y técnicas básicas" Documentación adicional, Curso de peritajes informáticos noviembre 2011. disponible en https://www.anguas.com/e1m6/Docs/01_Documentacion_Adicional_Curso_Peritaje_CPEIG.pdf consultado el 03 de Enero 2018

- - **if / of** son ficheros o dispositivos de entrada y salida, en este caso siempre hay que tener mucho cuidado y verificar que se esta copiando origen sobre destino y no al revés, pues será muy difícil corregir este error.
- - **ibs / obs / bs** para duplicar por tamaño de bloque de entrada, salida y entrada/salida.
- - **conv** proporciona diferentes opciones de proceso. Las más comunes son **sync**, **no error** que indican que el comando debe continuar aun que encuentre algún error y que debe añadir ceros a la salida para conservar el volumen de datos de salida.

El comando **dcfldd** es una evolución de **dd**. Añade alguna funcionalidad interesante como el cálculo de hashes durante la operación y el progreso.

- hashes hash indica la función de hash(hash=sha1), hashwindow es el tramo de entrada para generar el hash, con un valor cero toma toda la entrada, y hashlog para indicar el fichero de salida del resultado.

Estructura del dictamen pericial

a) **Portada:** La carátula del dictamen debe contener, como mínimo, el título ("Dictamen pericial Informático") el juzgado, tribunal o instancia en el que será presentado, el número de referencia del caso o expediente, el nombre completo del perito, su número de identificación y finalmente la fecha en que se finalizó el informe. En algunos casos se puede firmar la carátula a fin de visibilizar la firma del perito, igualmente si el peritaje fue realizado por una institución técnica, deberá también consignarse el nombre de la institución después del nombre del perito, y es una buena práctica que la carátula tenga el membrete de la misma.

b) **Tabla de contenido:** La importancia de incorporar un índice de contenidos, tablas, gráficos y/o anexos no es una mera cuestión estética, sino que es de gran utilidad para que, tanto el juez como las partes interesadas puedan referirse a un punto específico del peritaje, en

consecuencia, todos los aspectos relevantes del peritaje deben estar relacionados en el índice.

c) **Glosario:** Los peritajes informáticos por regla general, tienen un alto nivel técnico, mucho del vocabulario dentro de la disciplina informático se encuentra en inglés, y no siempre tiene el mismo significado que su uso lingüístico cotidiano en ese idioma, por lo tanto, es importante que se adjunte un listado detallado con los términos que el perito considere son necesarios de aclarar a manera que las personas que no son versadas en el área puedan entender básicamente su aplicación. El artículo 62 de la Constitución de la República establece que el idioma oficial de El Salvador es el Castellano, por lo tanto hay que tener especial cuidado de no colocar las traducciones de estos términos, pues hay que tener en cuenta que para efectos del peritaje y como elementos de la disciplina informática, representan un nombre y no un vocablo, es por eso que debe consignarse la explicación del término y no su traducción.

d) **Antecedentes:** En esta parte del informe, se debe describir, todos los actos realizados por las partes para la asignación del perito, también se deben mencionar brevemente los dispositivos, o archivos sobre los cuales se le ha pedido que ejecute la pericia, así como lo que se pretende probar con el informe pericial, en términos generales.

e) **Objeto:** En esta sección deben detallarse cuales son los extremos procesales que se pretenden comprobar, con cada uno de los elementos sobre los cuales se ha ejecutado la pericia, y si el resultado obtenido se orienta a afirmar o a refutar dichos extremos.

f) **Introducción:** Esta parte del informe explica la estructura de todo el informe, detallando las partes que contiene, la metodología para su elaboración y la metodología seguida para cada realizar el peritaje en cada uno de los elementos descritos. También debe relacionarse el respaldo teórico de dichas metodologías y en caso de ser metodologías standard debe también

consignarse el nombre y describir brevemente en qué consiste.

g) **Resumen ejecutivo:** Este apartado no es obligatorio en todos los dictámenes periciales sin embargo es una buena practica presentarlo como un resumen de los antecedentes, el objeto, la introducción y una descripción breve de las conclusiones.

h) **Descripción Metodológica:** Esta sección es la parte central del dictamen pericial, en esta parte se describe el estado en el que se recibieron los elementos a los cuales se les ha practicado la pericia, luego se describe a profundidad el procedimiento realizado a cada elemento y los resultados arrojados como producto del mismo, hasta este punto no se debe hacer ninguna interpretación de los datos obtenidos, sino que se debe consignar de manera clara los resultados de la pericia, asegurando la veracidad de los mismos.

i) Análisis: este apartado se consignan los datos, obtenidos durante el peritaje, y se confrontan

con los extremos procesales que se desean comprobar. Por ejemplo, si el peritaje consistía en recuperar un fichero eliminado de un disco duro, (y este fue positivo), se consignaría que efectivamente existió tal fichero, y que los metadatos (o cualquier otro elemento obtenido) demuestran que se siguió el proceso de eliminación de ese fichero. Además se debe describir como el procedimiento realizado ayudó a la recuperación de dicho fichero.

j) **Conclusiones:** dentro de este apartado, el perito proporciona su punto de vista, porcentajes de probabilidad, nivel de certeza, recomendaciones, apreciaciones técnicas, criterios profesionales, etc. referido exclusivamente a su valoración de la prueba obtenida en el peritaje, es decir que el perito debe abstenerse de realizar acusaciones o de aludir a cualquier otro elemento del litigio.

k) **Apéndice:** a esta parte correspondes todos los anexos que sirven para respaldar la veracidad del peritaje, aquí se adjuntan las actas de entrega y devolución de los elementos a los cuales se les

practicó la pericia con las firmas debidamente autenticadas por notario, la declaración jurada del perito en el que manifiesta que ninguno de los resultados ha sido alterado, específicamente para los peritos informáticos, se adjunta un archivo digital, (en cd u otro tipo de dispositivo de almacenamiento) conteniendo el resultado del cálculo de los ***hashes*** de todos los ficheros originales antes del peritaje, para demostrar el estado en que fueron recibidos, también se adjuntan fotografías de los elementos de hardware recibidos y un inventarios conteniendo: marcar, modelos, números de serie, y otros que se estimen convenientes para identificar debidamente cada elemento.

Capítulo 4

Contratos informáticos

La contratación sobre bienes y servicios informáticos ha tomado una gran importancia en los tiempos modernos, tanto por el volumen y la diversificación de estos como por el impacto que estos tienen para cada una de las partes y para la actividad económica en general.

En la legislación salvadoreña así como en la legislación internacional los contratos informáticos, siguen las reglas básicas del derecho contractual, específicamente en la categoría de los contratos atípicos, pues una regulación específica de este tipo de contratos perdería legitimidad y vigencia rápidamente, debido a la dinámica misma de la informática y la tecnología en general. Por este motivo se dice que los contratos informáticos no cuentan con una autonomía conceptual y sistemática respecto de otros contratos regulados dentro del derecho civil y mercantil como atípicos por lo diverso de su objeto.

El concepto de **"contrato informático"** es extenso y complejo pues alude a la característica que tienen aquellos contratos donde los bienes y servicios informáticos constituyen su objeto sino que también abarca aquellos cuyo objeto se perfecciona mediante bienes informáticos, como el caso de las transferencias electrónicas y otras operaciones telemáticas como la firma electrónica y el uso del *blockchain* para certificar documentos etc. Es decir que el uso de la informática es el medio y no el objeto. En este sentido, es necesario detallar conceptualmente la diferencia entre contratación electrónica, contratación informática.

Entones se entiende como **"contratación electrónica o por medios informáticos"** aquella que se realiza a través de una serie de elementos electrónicos, cuyo impacto radica en la demostración o confirmación real e inequívoca de la voluntad, es decir, el otorgamiento o la interpretación de un acuerdo bajo mutuo consentimiento. Dede una perspectiva *lato sensu,* esta categoría conceptual comprende a todos los actos, acuerdos y contratos que se celebran por medios electrónicos y telemáticos. Sin embargo a *stricto sensu*

se considera que esta contratación existe solamente sobre aquellos contratos que se celebran a través de la transmisión electrónica de datos de ordenador a ordenador.

Por otro lado, el **"contrato informático"** es el que tiene por objeto bienes y servicios informáticos. Cabe destacar que los bienes informáticos pueden ser materiales en sentido todos aquellos que se constituyen de forma tangible como el "**hardware"** y demás periféricos; por otro lado, los bienes informáticos también pueden ser intangibles o materiales que son todos aquellos programas de ordenador, expresado en códigos, (fuente u objeto) que como ya se expresó en la sección de la propiedad intelectual, son aquel conjunto de órdenes, instrucciones y procesos que en su tratamiento automático dentro de un ordenador constituyen el soporte lógico del elemento informático, conocido también como "**software"**.

Finalmente, este tipo de contratos también pueden recaer sobre los **"servicios informáticos"** específicamente se refiere a todos aquellos servicios que se relacionan con el harware o software, e implican el

diseño, el análisis y el mantenimiento del sistema, reparación de periféricos, configuración de equipos etc.

Tipicidad de los contratos informáticos.

A pesar de ser un contrato atípico (por no contar con una figura específica), el contrato informático está comprendido en la legislación salvadoreña dentro de la definición del art. 1309 del Código Civil, que establece que: *"Contrato es una convención en virtud de la cual una o más personas se obligan para con otra u otras, o recíprocamente, a dar, hacer o no hacer alguna cosa"*. Debido a su naturaleza, el contrato informático siempre es oneroso por lo que también se relaciona el artículo 1312 del mismo código ya que *"...cada una de las partes se obliga a dar o hacer una cosa que se mira como equivalente a lo que la otra parte debe dar o hacer a su vez;"*. De ahí nace también su tipicidad dentro del artículo 964 del código de comercio en sentido que *"Las disposiciones... ...relativas a los contratos se aplicarán a los negocios, actos jurídicos, y en particular, a los actos unilaterales, que hayan de surtir efectos en vida de quienes los otorguen* ***y que tengan***

***contenido patrimonial**, en lo que no se opongan a su naturaleza o a disposiciones especiales obre ellos.*

Del mismo modo, si se retoma la definición conceptual que hiciera al comienzo de este capitulo, encontramos que la "contratación informática" en sentido amplio se encuentra regulada bajo el artículo 966 del código de comercio en sentido que: *"Los contratos mercantiles que se celebren por correspondencia, quedarán perfeccionados desde que el proponente reciba la respuesta en que se acepte lo que haya ofrecido; pero si en ella se proponen condiciones que modifiquen la propuesta original, el contrato con las modificaciones se perfeccionará hasta que se reciba la contestación aceptándolas."*

Obviamente las tecnologías de la información y la comunicación, han logrado que la "correspondencia" sea inmediata. Por lo tanto, en función del otorgamiento del consentimiento de las partes se utiliza supletoriamente la disposición del artículo Art. 968 del mismo código que textualmente dice que: *"La oferta y la aceptación por teléfono o radioteléfono, se considerarán entre presentes cuando las partes, sus representantes o mandatarios se comuniquen personalmente."* pues el

requisito al que hace referencia el artículo es el de **la comunicación personal,** que quiere decir, que esta debe ser realizada sin ninguna otra persona que resulte intermediario de la negociación.

El contrato informático guarda una estrecha semejanza con los contratos nominativos, no solo en los aspectos patrimoniales que recaen sobre su objeto, sino en el tipo de obligaciones que se constituyen en ellos; por lo tanto es importante saber distinguir este tipo de contratos de aquellos ya regulados previamente, como la compraventa o los contratos laborales. Dada la complejidad de su estructura tambien se debe ser cuidadoso para clasificarlos pues también existen contratos atípicos o innominados que comparten ciertas características como los contratos de locación u otros contratos de ingeniería.

Por ejemplo, la compraventa es un contrato en una categoría típica, entonces, cuando se habla de **compraventa de software**, en realidad no se hace referencia a un contrato informático, sino a una compraventa pura y simple. A diferencia de otras legislaciones nuestro código civil identifica solamente a

la “cosa” como objeto de la compraventa y no hace la distinción entre material o inmaterial, así el artículo 1597 establece que: *“La compraventa es un contrato en que una de las partes se obliga a dar una cosa y la otra a pagarla en dinero. Aquélla se dice vender y ésta comprar...”.*

Por otro lado, un **contrato de transferencia de tecnología** tiene todas las características de un contrato atípico, por lo que puede considerarse un contrato informático, pues su objeto es **el conocimiento**, y a diferencia de los otros bienes intangibles, en un contrato de transferencia el conocimiento adquirido puede o no rendir los resultados esperados, por lo tanto la “cosa” es inmaterial y a la vez es incierta, entonces, si este conocimiento atiende a las características antes descritas, -es decir que recae sobre la informática o se obtiene a través de medios informáticos- se constituye un contrato informático propiamente dicho.

Tirso W Sáenz[53], clasifica los elementos a los cuales se vinculan los conocimientos tecnológicos el contrato informático podría recaer sobre:

> •Conocimientos incorporados en objetos (hardware): Materiales, maquinarias, equipos.
>
> •Conocimiento incorporados en registros (software): bancos de datos, procedimientos manuales.
>
> • Conocimientos Incorporados en el hombre (humanware): conocimientos, habilidades.
>
> •Conocimientos Incorporados en instituciones (orgware): estructuras y formas organizativas, interacciones, experiencia empresarial.

En otras palabras, el contrato se convierte en un contrato informático por que el objeto recae sobre un elemento informático, o bien, se realiza por medios informáticos a través de la telemática y criptografía etc. y no se encuentra regulado como un contrato típico en la legislación.

53 Morejón Grillo Ailed. (2015, marzo 5). *Fundamentos teóricos de la transferencia de tecnología*. Recuperado de https://www.gestiopolis.com/fundamentos-teoricos-de-la-transferencia-de-tecnologia/

Otro ejemplo un poco más común es el denominado **acuerdo de uso** *o "user agreement"* que es aquel contrato informático de adhesión en el que el usuario otorga su consentimiento y acepta determinadas condiciones, cuando se adquiere o se utiliza algún servicio generalmente ofrecido por la internet, como las cuentas de correo electrónico,(gmail, outlook, icloud) en redes sociales, (facebook, twitter etc.) servicios de música o video (spotify, Netflix, I music) etc.

Clasificación de los contratos informáticos

Los contratos informáticos, si bien son una especie atípica o innominada como se ha expresado antes, son susceptibles de ser clasificados según sus características específicas pues como lo expresa Tellez Valdez[54] estos tienen como objeto principal regular el nacimiento y transmisión de derechos derivados de la prestación de bienes y servicios informáticos. Según

[54] Tellez, Valdéz, Julio. Derecho informático 4ta ed. Instituto de investigaciones Jurídicas, UNAM. Mc Graw Hill. México, 2008.

Silvia Marcela Ibarguren los contratos informáticos pueden corresponder a:

1) **Equipamiento:** unidades centrales de procesamiento; periféricos para entrada, salida o almacenamiento de datos; equipos de comunicaciones; etc.

2) **Software:** Código fuente y código objeto, ejecutable o de aplicación.

3) **Servicios:** de análisis y diseño de sistemas; desarrollo, instalación, capacitación, asesoría y consultoría; mantenimiento; etc.

La misma autora, propone que los contratos también pueden ser clasificados según el negocio jurídico que se celebre y cita la clasificación realizada por *Bonneau*[55]**:**

1) Contratos de venta.

2) Contratos de leasing.

3) Contratos de locación.

[55] Bonneau, Jacques-Roger, 'La pratique du droit de l'informatique dans l'enterprise. Les relations entre constructeurs utilisateurs et conseils', Ed. de l'Usine Nouvelle, París, 1984, p.29.

4) Contratos de horas máquina.

5) Contratos de mantenimiento.

6) Contratos de prestaciones intelectuales: de estudios previos; pliego de condiciones; formación del personal; contrato llave en mano; etc.

7) Contratos de prestación de servicios.

Ambas clasificaciones responden a la definición típica a la que se hace referencia en el apartado anterior, por lo tanto, es importante no confundirlos con los contratos típicos.

Aspectos Generales de la contratación informática

Los contratos informáticos, contienen a su base, algunas disposiciones fundamentales de los contratos civiles, en ese sentido, Tellez Valdez[56] propone que las partes deben convenir mínimamente en los siguientes aspectos:

[56] Tellez, Valdéz, Julio. Derecho informático 4ta ed. Instituto de investigaciones Jurídicas, UNAM. Mc Graw Hill. México, 2008.

1) En la prohibición de ceder cualquiera de las obligaciones derivadas del contrato: salvo aquellas excepciones previamente establecidas por la ley.

2) El reconocimiento del contrato como instrumento probatorio para el reclamo de obligaciones.

3) Los casos de incumplimiento del contrato por nulidad.

4) La necesidad de un instrumento anexo para realizar modificaciones al contrato.

5) El valor relativo de cada cláusula, a fin de determinar en caso de contradicción cuales cláusulas prevalecerán.

6) La preeminencia del contrato sobre los demás contratos accesorios, y sobre los demás contratos otorgados por las partes frente a terceros.

Los elementos personales y técnicos

Como ya se ha mencionado, la estructura de los contratos informáticos también sigue la estructura establecida en el derecho común, es decir que se compone de elementos personales y de elementos técnicos.

Dentro de los elementos personales, tenemos a **los sujetos del contrato**, que según Guardia[57], en el derecho informático se les denominan: proveedores y usuarios; los primeros son todos aquellos, desarrolladores, fabricantes, distribuidores, vendedores de bienes informáticos así como los prestadores de servicios informáticos. Cabe mencionar que este sujeto puede ser una persona natural o jurídica, plural o singular y que asu vez puede actuar por sí misma o por su representante.

Los segundos son aquellos sujetos quienes requieren que sea satisfecha una necesidad a través de los bienes y servicios informáticos; estos también pueden ser, naturales o jurídicas, singulares o plurales,

57

e incluso pueden ser sujetos públicos (El Estado) o sujetos privados.

Las obligaciones que tienen los sujetos, serán las establecidas por el código civil para el efecto de los contratos y sus obligaciones, del artículo 1416 y 1421 cuando este recaiga sobre los bienes informáticos y los artículos 1424 y 1426 cuando se trata de servicio informático.

Deber de información y de control

Debido a la complejidad técnica, sobre la que recaen los contratos informáticos, la doctrina y jurisprudencia ponen a cargo del proveedor una serie de deberes que adquieren dimensión especial en esta materia, a estos se les denomina **"deberes de información y consejo"** es decir que, amparados en el principio *pacta sunt servanda* o de buena fe, del artículo 1417 del código civil, dentro de la etapa de negociación y de ejecución del contrato existe una obligación tácita de información, que se traduce a un deber de veracidad, en el cual se debe hacer saber a la otra parte ciertos hechos que podrían influir en su decisión.

Es importante no confundir los derechos de propaganda e información ya que la propaganda forma parte de un método de comercialización en el que se deben mencionar principalmente los rasgos más atractivos e importantes del bien o servicio, sin embargo el deber de información exige que se exprese detalladamente la calidad, función, y todos aquellos datos relacionados al objeto del contrato.

A su vez, el usuario, debe tener completo control sobre el proceso de formalización de un contrato según el articulo 1429 del código civil, no podrá imputar dolo sobre el proveedor, pues por la misma obligación que este tiene de informar, el usuario no podrá alegar la nulidad del contrato por desconocimiento de las cualidades del objeto una vez pactado el contrato, es decir que el deber de consejo tiende a orientar la decisión del cliente, e incluye tanto la obligación de información en sentido estricto, como la obligación de no abstenerse de la ejecución, una vez firmado el contrato.

En todos caso, el artículo 1437 del Código Civil establece que cuando no se puedan aplicar ninguna de las

reglas de interpretación generales, el contrato se regirá haciendo la interpretación de las cláusulas ambiguas que más favorezcan al usuario, por que se presumirá que dichas cláusulas ambiguas han sido dictadas así por la parte que tenía más interés en que su sentido no fuera claro; esto aplica a los contratos informáticos con más precisión por la alta complejidad técnica que media en estos y por la presunción del conocimiento más amplio del proveedor que del usuario.

Objeto de los contratos informáticos

En términos generales, la doctrina establece que los contratos informáticos, son aquellos instrumentos que sirven para regular la creación, transmisión y exigibilidad de derechos y obligaciones surgidas de cualquier relación contractual que tenga como objeto o que recaiga sobre cualquier bien o servicio informático. Entonces dentro de este convenio entre partes, el usuario pretende satisfacer sus necesidades a través de la adquisición de determinados bienes o servicios que le proporcionen resultados funcionales; mientras que el proveedor busca satisfacer esta necesidad mediante la provisión de bienes informáticos o se servicios que permitan garantizar dicha funcionalidad.

Para Silvia Ibarguren esta relación contractual tiene su base en la dicotomía anglosajona denominada "**contracting for results"** citando a Rosello[58]. Quiere decir que el carácter de las obligaciones que asume el proveedor es directamente proporcional al de la necesidad planteada por el usuario, es decir la consecución de un fin; por lo tanto, si se adquiere una obligación de resultado, lo que se garantiza es el cumplimiento de la finalidad perseguida por el usuario. Según Bergel[59] en materia informática las obligaciones del proveedor son por regla general obligaciones de resultado, pues es necesaria la concreción de determinados objetivos funcionales, ya que su ausencia equivale a la completa inutilidad del sistema (en el caso del software) y afecta directamente su valor económico.

En este sentido, la autora apunta al planteamiento de, De Lamberterie[60] quien destaca la necesidad de contar con un objeto cierto que forme la

---

58 Rossello, C., " I contratti dell'informatici", a cargo de Guido Alpa, giuffrè, Milán, 1984, p. 98 .

59 Bergel, S., 'Informática y responsabilidad civil' en Informática y Derecho, De palma, Buenos Aires, 1988, vol.2, p. 168.

60 De Lamberterie, I., 'Contratos en informática', en derecho y tecnología Informática, No 1, Bogotá, 1989, p. 63.

materia del compromiso, En sentido que el surgimiento del acuerdo es dado a partir de dos manifestaciones concordantes de voluntad en la negociación de un contrato, debiendo esta manifestación de voluntad recaer en los mismos términos pactados en el instrumento.

Contratos Accesorios y garantías

Debido a la multiplicidad de bienes y servicios informáticos, la materialidad o inmaterialidad de su objeto y el contenido basado en otros contratos atípicos, es que los contratos informáticos con frecuencia requieren de modificaciones o de garantías específicas sobre los resultados, ya que la dinámica misma de la tecnología abre la posibilidad a interpretaciones distintas sobre un mismo objeto, a lo que Rosello[61] denomina como "**atipicidad estandarizada".**

En esa misma linea de pensamiento Pavone La Rosa[62] propone que los contratos informáticos, se encuentran vinculados con el concepto de "sistema", y

[61] Rossello, C., 'I contrati dell'informatici. Spunti di reflessione in comparazione con l'sperienza estatunitense e francese', en I contratti di utilizzazione dei computers, a cargo de Guido Alpa, Giuffrè, Milán, 1984, p.110

que por lo tanto no sería posible tener un contrato con esquemas fijos como los contratos típicos; pues lo más probables es que sus cláusulas sean distintas en cada negocio o con una pluralidad de prestaciones.

De esta pluralidad de prestaciones es que surgen los llamados contratos mixtos y los contratos conexos. Ambas categorías tienen su fuente tanto en aquellos detalles técnicos vinculados a la naturaleza de los contratos informáticos, como en las garantías necesarias para el logro del fin específico del convenio. Para Bertrand[63] esta multiplicidad de contratos son producto de la especificidad de su objeto; por lo tanto tiende a convertirse en una clase de "contrato complejo", un ejemplo de contrato mixto, puede ser un contrato de suministro de equipo informático, el cual incluye como como parte del contrato una sección relativa al servicio de soporte técnico, dentro de la cual también se establecen costos adicionales y cláusulas especiales, como si fuera un contrato dentro de otro contrato, ante la duda en la interpretación del contrato

[62] Citado por Pietro Gobio Casali. En "I contrati del software: qualificazione, responsabilitá e garanzie" Argomenti I singoli contratti 04 2014.

[63] Bertrand, André, 'Contrats informatiques. Services et conseils', Ed. des Parques, París, Francia, 1983, p. 25

se se aplicará el artículo 1434 del código civil en la forma expresada en la parte del deber de información.

Uno de los contratos conexos más comunes son las garantías, los cuales pueden insertarse como cláusulas en el contrato principal, (lo que lo convertiría en un contrato mixto o complejo) y también pueden ser adheridos como instrumentos individuales por separado, pero siempre vinculados al contrato principal, pues su función es la de asegurar las obligaciones plasmadas en el contrato principal y definir los mecanismos para dicho aseguramiento. Tellez Valdez propone que en los contratos informáticos, las principales garantías son:

a) Garantías de conformidad

b) Garantías de buen funcionamiento

c) Garantías de evicción

d) Garantías contra vicios

Específicamente en el área de servicios informáticos, existe también un contrato accesorio en el que se estipulan de manera detallada los niveles de dicho servicio, esto a través de una serie de parámetros

objetivos que son propuestos y establecidos de mutuo acuerdo entre las partes, así, se pretende dejar constancia a nivel de cláusula contractual el nivel operativo del funcionamiento,las penalizaciones por caída, interrupción o suspensión del servicio, delimitación de responsabilidades, etc. a estos contratos se les denomina: **Acuerdo de Nivel de Servicios** (Service Level Agreement, SLA).

En los contratos SLA se toman como principales acuerdos:

a)Tipo de servicio.
b)Soporte técnico y asistencia.
c)Provisiones para seguridad y datos.
d)Garantías del sistema y tiempos de respuesta.
e)Disponibilidad del sistema.
f)Conectividad.
g)Multas por fallas o caídas del sistema.

Contratos unilaterales, de adhesión o con condiciones predispuestas

La mayoría de contratos por servicios informáticos, especialmente aquellos que se prestan por

internet son contratos de adhesión, a estos contratos también se les denomina contratos discrecionales, predispuestos, paritarios, tipo standard, o uniformes, pues son celebrados mediante formularios prerredactados. Este tipo de contratos, han sido objeto de debate por muchos años, pues uno de los principios rectores de la legislación clásica de los contratos es la negociación *vis à vis* entre ambas partes.

En la actualidad, este tipo de contratos han tenido mucho auge por su utilización masificada por parte de instituciones financieras y otros proveedores de servicios, quienes reservan para sí la formulación de cláusulas generales y especiales, mientras que la autonomía de la voluntad de la otra parte queda reducida a la simple aceptación o el rechazo de los términos y a la vez del servicio ofrecido, sin contar con la posibilidad de formular una contraoferta.

A pesar de la ausencia del principio de igualdad económica como el que planteaba Spota[64], se presume para el caso en estudio, que cuando el usuario acepta todas las cláusulas del contrato propuesto por el

[64] Spota, Alberto, 'Instituciones de derecho civil, Contratos' Ed. Depalma, 1975, vol. 1, pag. 222.

proveedor, esta prestando su consentimiento libremente, sin dolo, violencia o error y este contrato adquiere el efecto los efectos del artículo 1426 y 1424 del código civil.

Dentro de la contratación informática, este tipo de pactos son muy comunes para la prestación de servicios de correo electrónico, apertura de cuenta en redes sociales, servicios en línea e interacciones de videojuegos, aplicaciones, entre otros, bajo el nombre de **"términos y condiciones de uso"** el cual cumple con todas las características antes planteadas sobre los contratos de adhesión. Cabe mencionar también, que en nuestro país, este tipo de contratos, se rige por las reglas del derecho civil, pues en muchos de los casos, este tipo de contratos no tienen una contraprestación económica en dinero, sin embargo, no son gratuitos contrario a lo que se cree, sino que son conmutativos, en los términos del 1312 del código civil en sentido que *"cada una de las partes se obliga a dar o hacer una cosa que se mira como equivalente a lo que la otra parte debe dar o hacer"* así, esta contraprestación equivalente la representan los datos del usuario; entonces, para el caso

concreto, en los contratos denominados, términos y condiciones de uso, el usuario, se adhiere a las cláusulas preestablecidas por el proveedor a fin que éste le preste de un servicio informático a cambio de la disposición de todos los datos del usuario que estén vinculados a dicho servicio con las limitaciones que el usuario ha admitido[65].

Es importante destacar que si este contrato oneroso, tiene a su base una contraprestación en dinero, entonces estará bajo el régimen de los contratos innominados del Código Mercantil siendo esa la única diferencia en relación a los contratos innominados civiles aquí tratados.

[65] Bergel, Salvador, 'Las cláusulas limitativas de la responsabilidad en los contratos informáticos', Revista del Derecho Industrial, Ed. Depalma, no 21, set.-dic. 1985, t.7, p. 474.

Bibliografía

Baldini, N. (2006). The Act on Inventions at Public Research Institutions: Danish Universities' Patenting Activity. *Scientometrics*, Vol. 69, No. 2, pp. 387-407.

Barba, E. (2011). *Innovación: 100 CONSEJOS para inspirarla y gestionarla*. Madrid: Libros de Cabecera S.L.

Botero, C. A. (2009). Cinco tendencias de la gestión educativa. *Revista Iberoamericana de Educación*. Colombia: Politécnico Colombiano Jaime Isaza Cadavid.

Cervantes, M. (s.f.). *Academic Patenting: How universities and public research organizations are using their intellectual property to boost research and spur innovative start-ups*. Recuperado de:

http://www.wipo.int/sme/es/documents/academic_patenting.htm

Conceição, P., Heitor, M. V. & Oliveira, P. O. (1998). University –based technology licensing in the knowledge based economy. *Technovation*, Vol. 8, No. 10.

Drucker, P. F. (2006). *Drucker para todos los días*. Bogotá: Editorial Norma.

Etzkowitz, H., Webster, A., Gebhardt, C. & Cantisano Terra, B. R. (2000). The future of the university and the university of the future: evolution of ivory tower to entrepreneurial paradigm. *Research Policy* 29, pp. 313–330. Forbes (2014). *Las universidades mexicanas con más patentes*. Recuperado de:

http://www.forbes.com.mx/las-universidades-mexicanas-con-mas-patentes/

IMPI en Cifras (2015). Recuperado de: http://www.impi.gob.mx/ Labariega Villanueva, P.A. (2011). *Organización Mundial de la Propiedad Intelectual*.

México: Instituto de Investigaciones Jurídicas de la UNAM. Lima, M. C. (2004). *Políticas de Gestión de la Propiedad Intelectual en las Universidades Nacionales*. Buenos Aires: Universidad Nacional de la Plata, Argentina. Macho-Stadler, I & Pérez-Castrillo, D. (2010). Incentives in University Technology Transfers.

International Journal of Industrial Organization, Vol. 28. Masó Dominico, Y. (2014). *Estrategias de enseñanza para los estudiantes de licenciatura que reciben la materia de Derechos de Autor en la Universidad Interamericana para el*

Desarrollo, Sede Zacatecas (Tesis de Maestría). Universidad Interamericana para el Desarrollo, Zacatecas.

OCDE (2003). Turning science into Business: Patenting and Licensing at Public Research Organisations. Recuperado de: www.oecd.org/bookshop/

OMPI (2011). *Informe sobre la propiedad intelectual en el mundo. Los nuevos parámetros de la innovación*. Suiza: Serie de la OMPI "Economía y Estadística".

OMPI (2013). *Informe mundial de 2013 sobre la propiedad intelectual*. Suiza: Serie de la OMPI "Economía y Estadística".

OMPI (2014). Recuperado de: http://www.wipo.int/portal/es/ Oppenheimer, A. (2014). *Crear o morir: la esperanza de Latinoamérica y los cinco secretos de la innovación*. México, D.F.: Océano. Pavón Morote, J. y Hidalgo Nuchera, A. (1997). *Gestión e innovación: un enfoque estratégico*. Madrid: Editorial Pirámide.Pesquera, M.A., Casares-Hontañón, P.C., Coto Millán, P. e Inglada López, V. (2010).

Innovación Empresarial, Clase Creativa y Desarrollo Económico en España. España: Editorial: Tirant lo Blanch. PILA México (2009). *Análisis del nivel de concientización y uso de la PI en Las IES: necesidades formativas*. Recuperado de: http://www.pila-network.org/ PILA Network (2011). *PILA Network: La red de propiedad intelectual e industrial en Latinoamérica Recuento de 3 años de colaboración*. Recuperado de:

http://www.pila-network.org/blog/pila-network-la-red-de-propiedad-intelectual-e-

industrial-en-latinoam%C3%A9rica-recuento-de-3-a%C3%B1os

Ponjuán, G. (1999). *El éxito de la gestión o la gestión del éxito*. Anales de Documentación, (2) 39-47. Recuperado de http://www.redalyc.org/articulo.oa?id=63500203

Rogers, E. M., Takegami, S. & Yin, J. (2001). Lessons learned about technology transfer. *Technovation*, Vol. 21.

Rubio Martín, G. y López-Cózar Navarro, C. (2007). Los intangibles en las empresas farmacéuticas. Palma de Mallorca: Decisiones basadas en el conocimiento y en el

papel social de la empresa: XX Congreso anual de la Asociación Española de Dirección y Economía de la Empresa (AEDEM), Vol. 2.

Saravia André, M. (2012). *Gestión integral de la propiedad intelectual. Una guía para su planificación e implementación*. Recuperado de: https://www3.wipo.int/confluence/download/attachments/21758676/13%20- %20Gestion%20Integral%20de %20PI.pdf?api=v2

Siegel, D. S., Waldman, D. A., Atwater, L. E., & Link, A. N. (2004). Toward a model of the effective transfer of scientific knowledge from academicians to practitioners: qualitative evidence from the commercialization of university technologies. *Journal of Engineering & Technology Managemen*t, Vol. 21.

Vela Valdés, J. (2000). Educación Superior: inversión para el futuro. La Habana: Universidad de la Habana. Conferencia impartida en el 50 aniversario de la Unión Latinoamericana de Universidades (UDUAL). *Revista Cubana Edución Media Superior*; 14 (2): 171 – 183.

BERGEL, Salvador D., "Notas sobre contratación informática", en Revista

de Derecho Privado, Ed. Rubinzal-Culzoni, Buenos Aires.

BRIZZIO, Claudia, "Contratación electrónica y Contratos informáticos" en Revista La Ley, Sec. Doctrina, T. 2000 A.

CORREA-NAZAR ESPECHE-CZAR DE ZALDUENDO-BATTO,

"Derecho Informático", Ed. Depalma, Buenos Aires, 1994.

DE LAMBERTERIE, Isabelle, "Contratos Informáticos", en Informática y Derecho - Aportes de Doctrina Internacional, Ed. Depalma, Vol. 4, Buenos Aires, 1998.

ALESTUEY DOBÓN, María del Carmen. “Apuntes sobre la perspectiva criminológica de los delitos informáticos”, Informática y Derecho No 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi.

ÁLVAREZ DE LOS RÍOS, José Luis. "Delitos Informáticos". Ponencia en las Jornadas sobre Marco Legal y Deontológico de la Informática, Mérida 17 de septiembre de 1997.

ANDRADE SANTANDER, Diana. El Derecho a la Intimidad, Centro Editorial Andino, Quito – Ecuador, 1998.

BAÓN RAMÍREZ, Rogelio. "Visión general de la informática en el nuevo Código Penal", en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial / Consejo General del Poder Judicial, Madrid, 1996.

BARATTA Alessandro: Derecho Penal Mínimo, Editorial Temis S.A. Santa Fe de Bogotá, Colombia, 1999.

BARBIERI Pablo, Contratos de Empresa, Editorial Universidad, Buenos Aires, Argentina, 1998.

BARRIUSO RUIZ, Carlos. "Interacción del Derecho y la informática", Dykinson, Madrid, 1996, pág. 245 a 252.

BECCARIA Alessandro, De los Delitos y las Penas, Editorial Temis S.A. Santa Fe de Bogotá, Colombia, 1997.

BERDUGO GOMEZ DE LA TORRE, Ignacio: Honor y libertad de expresión. Tecnos. Madrid, 1987.

BETTIOL Giusseppe, Derecho Penal, Editorial Temis, Bogotá, Colombia, 1990 BUENO ARÚS, Francisco. "El delito informático", Actualidad Informática Aranzadi No 11, abril de 1994.

CABANELLAS, Guillermo, Diccionario de Derecho Usual, Tomo 1, Editorial Heliasta. 1990.

CANO JEIMY, Inseguridad Informática: Un concepto dual de la Seguridad Informática. Universidad UNIANDES 1994

CASTILLO JIMENEZ, María Cinta, RAMALLO ROMERO, Miguel. El delito informático. Facultad de Derecho de Zaragoza. Congreso sobre Derecho Informático. 22-24 junio 1989.

CHOCLAN MONTALVO, José Antonio. "Estafa por computación y criminalidad económica vinculada a la informática", Actualidad Penal No 47, 22-28 diciembre 1997 CORREA Carlos María, El Derecho Informático en América Latina, Publicado en Derecho y Tecnología Informática, Edit. Temis, Bogotá, Mayo de 1990. CREUS

Carlos, Derecho Penal Parte Especial, Edit. Astrea, Buenos Aires, 1998, Tomo 2.

CUERVO José, Delitos Informáticos y Protección Penal a la Intimidad, Publicación hecha en Internet URL: www.derecho.org

DALLAGLIO Edgardo Jorge, "La Responsabilidad Derivada de la Introducción y Propagación del Virus de las Computadoras", publicado en El Derecho, año 1990.

DAVARA RODRÍGUEZ, Miguel Angel, Análisis de la Ley de Fraude Informático, Revista de Derecho de UNAM. 1990.

DAVARA RODRÍGUEZ, Miguel Ángel. "De las Autopistas de la Información a la Sociedad Virtual", Editorial Aranzadi, 1996.

DAVARA RODRÍGUEZ, Miguel Ángel. "Manual de Derecho Informático", Editorial Aranzadi, Pamplona, 1997.

DONOSO ABARCA, Lorena, Análisis del tratamiento de las figuras Relativas a la Informática tratadas en el título XIII del Código Penal Español de 1995.

FERNÁNDEZ CALVO, Rafael. "El Tratamiento del llamado "Delito Informático" en el proyecto de Ley Orgánica de Código Penal: Reflexiones y propuestas de la CLI (Comisión de Libertades e Informática), Informática y Derecho No 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996.

FERREYROS SOTO, Carlos. "Aspectos Metodológicos del Delito Informático", Informática y Derecho No 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.

FÍGOLI PACHECO, Andrés. El Acceso No Autorizado a Sistemas Informáticos, Uruguay 1998, Publicación hecha en Internet, www.derecho.org.

FROSINI Vitorio, Informática y Derecho, Editorial Temis, Bogotá, Colombia, 1988.

FUMIS Federico, Informática y Derecho de Daños, Boletín Hispanoamericano de Informática y Derecho, 1998, Buenos Aires, Argentina. URL: Http//ww.ulpiano.com

GARCÍA GIL, F. Javier. "Código Penal y su Jurisprudencia. Adaptada a la Ley Orgánica 10/1995, de 23 de noviembre", Editorial Edijus, Zaragoza, 1996.

GARCÍA VITORIA, Aurora. El Derecho a la Intimidad en el Derecho Penal y en la Constitución de 1978. Editorial Aranzadi, Pamplona – España, 1983.

GÓMEZ PERALS, Miguel. "Los Delitos Informáticos en el Derecho Español", Informática y Derecho No 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi.

GUASTAVINO, Elías P., Responsabilidad Civil y otros problemas jurídicos en computación, Ediciones La Rocca, Buenos Aires, 1987.

GUIBOURG Ricardo A., ALENDE Jorge O., CAMPANELLA Elena M., Manual de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires, Argentina.

GUTIÉRREZ FRANCÉS, María Luz, Fraude Informático y estafa.

GUTIÉRREZ FRANCÉS, Ma Luz. “Fraude informático y estafa”, Centro Publicaciones del Ministerio de Justicia, Madrid, 1991.

HANCE OLIVIER. Leyes y Negocios en Internet. México. De. Mc Graw Hill Sociedad Internet. México. 1996.

HANSSENER Winfried, “Derecho Penal”, Editorial Azalea, 1998.

TELLEZ VALDÉS, Julio. “Los Delitos informáticos. Editorial Temis 1999.

TELLEZ VALDÉS, Julio. “Los Delitos informáticos. Situación en México”, Informática y Derecho No 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, pág. 461 474.

TIEDEMANN, Klauss. “Poder económico y delito”, Barcelona, 1985.

TORTRAS Y BOSCH, Carlos. “El delito informático”, número 17 monográfico de ICADE, Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales.

ZABALA BAQUERIZO Jorge, Delitos contra la Propiedad, Tomo 2, Editorial Edino, Guayaquil, Ecuador, 1988.

ZANONI Leandro. Los Hackers, la nueva cara de los piratas de Fin de siglo, Revista de Informática y Derecho. De Palma, Buenos Aires Argentina 1998.