1.− Seguridad

*La seguridad informática. Aquí se nos describe la importancia de la información en la sociedad actual, y algunos conceptos sobre seguridad.

*Las armas de los hackers. Como su propio nombre indica, aquí se trata de describir los métodos más utilizados por los hackers.

*Hackers y Crackers. Algunas diferencias entre los hackers y los crackers.

1.1 Seguridad Informática

La información e importancia de la información.

Para comenzar el análisis de la seguridad informática se ha de definir o estudiar el objeto de esa seguridad, y ese objeto es la *información*. La información es el conjunto de datos que nos aportan un conocimiento sobre un determinado tema.

La información es algo con mucho valor dentro de la sociedad actual, y así se reflejó en la Conferencia de la Quinta Generación celebrada en 1981 en Japón, donde el director del Proyecto japonés Toru Moto−Oka decía:

"La riqueza de las naciones que durante sus fases agrícola e industrial dependió de la tierra, del trabajo y del capital, de los recursos naturales y de la acumulación monetaria, en el futuro se basará en la información, en el conocimiento y en la inteligencia."

En realidad no es algo nuevo de nuestros tiempos, siempre ha sido muy importante la información, pero en nuestro tiempo toma una dimensión especial, básicamente por la existencia de la informática y las telecomunicaciones, mediante las cuales una determinada información puede llegar a todo el mundo en unos segundos.

De esta forma, situados en este contexto, podemos encontrarnos con situaciones algo peligrosas; tan sólo hemos de pensar en la cantidad de información recogida en ficheros informáticos sobre nosotros, que aisladamente pueden revelar poco de la persona, pero que en conjunto pueden darnos una visión bastante exacta de esa persona; o la cantidad de información tan valiosa que hay en ficheros del gobierno, militares, o empresariales, que pueden sumir en el caos a un país entero si esa información cae en manos de personas que sepan utilizarla contra ese país o empresa; estamos hablando, por ejemplo, de datos obtenidos por servicios de inteligencia, secretos empresariales sobre nuevos productos, o la interceptación de comunicaciones entre órganos gubernamentales, militares, o empresariales. De hecho, todas las agencias de seguridad de los EEUU, evalúan los efectos de la "ciberguerra", y las medidas a tomar, tanto de protección como de contraataque. Como podemos deducir, la cantidad y la "sensibilidad" de la información que hay en los sistemas informáticos o telemáticos, hace imprescindible que se tomen las medidas de seguridad oportunas, tanto físicas como lógicas, para evitar los problemas antes mencionados.

La seguridad

Cuando se habla de seguridad, a los profanos les viene a la cabeza la protección ante incendios, inundaciones,

robos, etc. Pero la seguridad no acaba ahí, se compone también de la seguridad lógica, es decir, salvaguardar la confidencialidad y la autenticidad de los ficheros, datos, sistemas, etc.

Pero para llevar a término esta tarea se ha de tomar conciencia de la importancia de la seguridad, especialmente por parte de los directivos. Como se suele decir, "una cadena es tan fuerte como eslabón más débil", es decir, los sistemas de seguridad, físicos y lógicos, pueden ser de última generación y a un nivel máximo, pero todo esto no sirve de nada si algún empleado es descuidado y no elimina los documentos confidenciales, o no guarda convenientemente su clave de acceso al sistema, o un tercero logra engañarle y obtiene la información que necesita para acceder al sistema sin estar autorizado (ingeniería social), etc. Todos estos aspectos son eslabones débiles de la cadena, y por tanto son puntos débiles que hay que reforzar, o nuestra cadena será tan débil como ellos.

Ningún sistema de seguridad, por bueno que sea, es fiable al cien por cien. Esta ha de ser la regla básica para conseguir una seguridad mejor; nunca se ha de estar conforme con el nivel de seguridad que se tiene, porque cada día aparecen nuevos métodos de vulneración de los sistemas de seguridad antiguos, y nosotros nos hemos de mover con los tiempos, y estar informados de cualquier cambio en ese sentido, pues, por ejemplo, en la seguridad lógica nos podemos quedar desfasados (y por ello inseguros) en muy poco tiempo, porque el campo de la informática cambia continuamente. Además hemos de tener en cuenta que en determinadas páginas web, listas de distribución, y grupos de noticias se divulgan todos los agujeros que se conocen de los sistemas de seguridad, ello quiere decir que si no se toman las medidas oportunas para remediar ese fallo, cualquier persona podrá fácilmente vulnerar nuestro sistema, ya que el fallo se divulga "a bombo y platillo", sobretodo entre la comunidad hacker.

La seguridad informática protege los siguientes campos:

La seguridad de las personas.

La seguridad de los datos y la información.

La seguridad de las comunicaciones.

La seguridad de los sistemas.

Lo fundamental, y por eso se cita en primer lugar, es la seguridad de las personas, pero si la seguridad la gestionara un hipotético sistema inteligente (como dice E. del Peso Navarro y M. A. Ramos González) nos diría que lo más importante son los datos, y nos preguntaríamos ¿por qué?, y el sistema nos respondería:

Las instalaciones han de estar cubiertas por seguros, y si hay problemas se debe poder procesar en otras instalaciones alternativas.

Los ordenadores han de estar cubiertos por seguros, y si hay problemas se debe poder procesar en otros alternativos.

Las personas han de estar cubiertas por seguros y han de ser sustituibles, y se debe proceder a llamar a otros técnicos que conozcan los sistemas o sean capaces de aprenderlos pronto.

La pérdida de los datos (y de los programas) puede estar cubierta por seguros, pero si se han destruido y no existen copias actualizadas sobran: instalaciones, equipos y personas.

Para establecer un buen sistema de seguridad, lo primero que hay que hacer es una evaluación de riesgos, para ello hemos de seguir los siguientes pasos:

Detección de fallos. Consiste en localizar los agujeros que tenga el sistema de seguridad. Es preferible que dicha detección la haga un tercero imparcial y experto (auditores informáticos).

Análisis. Se trata de medir las posibles pérdidas y la probabilidad de que se produzcan.

Solución. Establecer las medidas necesarias para reducir o eliminar las probabilidades de que ocurra, intentar reducir los efectos de una hipotética infiltración, o aceptar el riesgo si los daños o las probabilidades de que se produjeran fueran pequeños (si es posible no lo asuma nunca).

Lógicamente, cualquier sistema de seguridad requiere una inversión más o menos cuantiosa, dependiendo fundamentalmente de la clase de fallo que se detecte, y la mayor o menor facilidad para convencer a los directivos de hacer la inversión depende de las pérdidas que se puedan producir y las probabilidades de que se produzcan.

Las posibles amenazas son:

Acceso directo a los equipos y las instalaciones, donde el intruso puede apoderarse de la información que desea, tanto material (carpetas, expedientes, disquetes, papeles, etc.) como digital (ficheros, programas, etc.).

Ataque remoto. Un ataque remoto es aquel en el que el atacante inicialmente no tiene el control de la máquina a la que quiere asaltar (la máquina remota). Una máquina remota es aquella a la que se puede acceder a través de algún protocolo de Internet o de alguna otra red. En estos ataques la información contenida en soportes físicos no corre peligro, pero sí la contenida en la red.

Provocación de caídas de equipos, cortes en el suministro de energía, ruptura de las comunicaciones, etc.

Seguidamente, analizaremos algo más del ataque remoto, que es el utilizado normalmente por los hackers.

El típico objetivo para un pirata son las redes pequeñas y privadas, ya que carecen de firewalls (por su coste), y utilizan medidas de seguridad inferiores, además de otras razones:

Sus propietarios son nuevos en Internet, y no conocen todo lo que deberían sobre seguridad.

El administrador del sistema tiene más experiencia con LAN que con TCP/IP, y eso hace que los piratas se aprovechen de los fallos intrínsecos de dicho protocolo.

Tanto el equipo como el software son antiguos, y todos sus agujeros los conoce toda la comunidad de Internet.

Además las redes de grandes empresas o agencias del gobierno, son muy difíciles de asaltar, y se requiere un conocimiento muy alto de redes y de programación. Por otro lado, este tipo de entidades no dudan en gastar todo el dinero necesario para localizar al pirata, lo cual hace que no sólo haya que ser bueno en entrar al sistema, sino también en salir sin dejar rastros que lo identifiquen.

Obviamente, el principio general tiene sus excepciones, porque hay hackers que prefieran sistemas más complicados y que les produzcan mayor satisfacción personal.

Las herramientas que existen para la seguridad lógica requieren otro artículo, con lo que no haremos referencia a ellas ahora.

En conclusión, hemos de tener siempre presente que la seguridad informática es fundamental para cualquier persona física, organismo, empresa, o cualquier otro tipo de persona jurídica, pues de ella depende su futuro. Por otro lado, hemos de tener una visión global de la seguridad, para no dejar ningún resquicio por el que se

puedan colar personas no autorizadas, es decir, hemos de analizar las amenazas físicas y lógicas, tanto del interior de nuestro entorno como del exterior, y hemos de promover las medidas de prevención necesarias, y los medios para anular los efectos de un ataque, por si los medios de prevención son inútiles para evitar dicho ataque. Además no hemos de quedarnos estancados con nuestro sistema de seguridad, al contrario, hemos de ir actualizándolo cada cierto tiempo, para ir minimizando las posibilidades de un ataque.

1.2 Las armas de los hackers

A continuación se va a hacer una descripción de las herramientas o métodos que más suelen utilizar los hackers para sus ataques. Pero esta lista esta limitada desde el mismo momento en que se decide crearla, porque la mayoría de los hackers saben programación y se hacen sus propios programas para entrar a los sistemas, con lo que aquí se tratará de describir los métodos más habituales.

ESCÁNERES

Los escáneres han sido las herramientas más efectivas dentro del hacking, se dice que un escáner que vigile a un único puerto TCP/IP tiene más eficacia que miles de passwords.

Un escáner es un sistema que encuentra automáticamente los fallos de seguridad de un sistema remoto, es decir, una persona desde su habitación puede conocer los agujeros de seguridad de un sistema en otro país. Los escáneres son programas que atacan puertos TCP/IP, como pueden ser telnet o FTP, almacenando la respuesta que se obtiene, y así una persona puede obtener todo tipo de información de otro sistema, como, por ejemplo, si es posible que un usuario anónimo se registre.

Existen escáneres para todas las plataformas, tanto UNIX, Windows, Macintosh, etc. El construirse una persona su propio escáner no es difícil, pero no sería muy lógico teniendo en cuenta que hay programas muy buenos, gratuitos y comerciales, por ejemplo, NSS, Strobe, Satan, Jakal, IdentTCPScan, Connect, FSPScan, etc.

CAZADORES DE CONTRASEÑAS

Un cazador de contraseñas es un programa que desencripta las contraseñas o elimina su protección. Aunque estos programas no han de desencriptar nada, y además con determinados sistemas de encriptación es imposible invertir el proceso, si no es de forma autorizada. El funcionamiento es el siguiente: cogemos una palabra de una lista, la encriptamos con el protocolo que han sido encriptadas las claves, y el programa compara las claves encriptadas con la palabra encriptada que le hemos dado, si no coincide pasa a otra clave encriptada, si coincide la palabra en texto legible se almacena en un registro para su posterior visualización. Los cazadores de contraseñas que podemos encontrar son: Crack, CrackerJack, PaceCrak95, Qcrack, Pcrack, Hades, Star Cracker, etc. Hay cazadores de contraseñas para todos los sistemas operativos.

CABALLOS DE TROYA O TROYANOS

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto, p. ej. formatear el disco duro, modificar un fichero, sacar un mensaje, obtener información privilegiada del sistema, etc. Los troyanos los crean los programadores, ya sea creando ellos un programa original, e introduciendo el código maligno, o cogiendo el código fuente de otro programa e introduciendo el código maligno, y luego distribuirlo como el original.

SUPERZAPPING

Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador. El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del ordenador y modificarlo, su equivalente en un PC serian las Pctools o el Norton Disk Editor.

PUERTAS FALSAS

Es una practica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc. con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

HERRAMIENTAS DE DESTRUCCIÓN

Este suele ser el procedimiento de sabotaje mas utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá o modificara la información, o provocará el cuelgue del sistema. Podemos distinguir cuatro métodos de destrucción: mailbombing, flash bombs, aplicaciones especiales de negación de servicio, y virus.

Mailbombing: Este método se basa en enviar muchos mensajes de correo electrónico, al mismo usuario, lo cual provoca una gran molestia a dicho usuario. Las herramientas que existen para estos ataques son: Up Yours, KaBoom, Avalanche, Unabomber, eXtreme mail, Homicide, Bombtrack, etc. La mayoría de estas aplicaciones suelen ser gratuitas, y tenemos para todas las plataformas.

Flash bombs: Son herramientas que se utilizan en el IRC. Cuando nos conectamos a un IRC, hay varios canales o chats, y cada chat tiene su operador que es la autoridad en ese chat, y decide la persona que ha de marcharse del chat. Las personas expulsadas del chat toman represalias, y apareció el flash bombs. Las aplicaciones de flahs bombs que existen atacan en el IRC de una forma diferente, pero básicamente lo que hacen puede ser es expulsar a otros usuarios del chat, dejar colgado el chat, o llenar de basura (flooding) un canal. Las herramientas que tenemos a nuestra disposición son: crash.irc, botkill2.irc, ACME, Saga, THUGS, o The 7th Sphere.

Aplicaciones de negación de servicio: Este tipo de ataques trata de dejar colgado o desactivar un servicio de la red saturándolo de información y dejándolo bloqueado, e incluso se obligará a reiniciar la máquina. Las utilidades que podemos encontrar para realizar este tipo de ataques son: Syn_floder, DNSKiller, arnudp100.c, cbcb.c, o win95ping.c.

Virus: Los virus son un grave problema, ya que a pesar de ser programas muy pequeños pueden hacer mucho, y más si se utiliza Internet como vía de infección. Un virus informático es un programa diseñado para que vaya de sistema en sistema, haciendo una copia de sí mismo en un fichero. Los virus se adhieren a cierta clase de archivos, normalmente EXE y COM, cuando estos ficheros infectados se transmiten a otro sistema éste también queda infectado, y así sucesivamente. Los virus entran en acción cuando se realiza una determinada actividad, como puede ser el que se ejecute un determinado fichero. Como hemos dicho los virus son programas, y para crearlos los programadores de virus utilizan kits de desarrollo de virus que se distribuyen por Internet, entre las que podemos destacar las siguientes: Virus Creation Laboratories, Virus Factory, Virus Creation 2000, Virus C destruction Est, o The Windows virus Entine. Por ello cualquiera que se haga con

alguno de estos kits y sepa programación pueda crear sus propios virus, en este contexto no es raro que la estimación de los virus que existen en la actualidad sea de más de 7.000.

ATAQUES ASINCRONICOS

Este es quizá el procedimiento mas complicado y del que menos casos se ha tenido conocimiento. Se basa en las características de los grandes sistemas informáticos para recuperarse de las caídas, para ello periódicamente se graban los datos como volcado de memoria, valor de los registros, etc. de una forma periódica Si alguien consiguiera hacer caer el sistema y modificar dichos ficheros en el momento en que se ponga de nuevo en funcionamiento el sistema éste continuará con la información facilitada y por tanto la información podría ser modificada o cuando menos provocar errores.

INGENIERA SOCIAL

Básicamente es convencer a la gente de que haga lo que en realidad no debería, por ejemplo, llamar a un usuario haciéndose pasar por administrador del sistema y requerirle el password con alguna excusa convincente.

RECOGIDA DE BASURA

Este procedimiento consiste en aprovechar la información abandonada en forma de residuo. Existen dos tipos: el físico y el electrónico. El físico se basa principalmente en los papeles abandonados en papeleras y que posteriormente van a la basura, p ej. el papel donde un operario apuntó su password y que tiró al memorizarla, listados de pruebas de programas, listados de errores que se desechan una vez corregidos, etc. El electrónico, se basa en la exploración de zonas de memoria o disco en las que queda información residual que no fue realmente borrada, p. ej. ficheros de swapping, ficheros borrados recuperables (por ejemplo, undelete), ficheros de spooling de impresora, etc.

SIMULACION DE IDENTIDAD

Básicamente es usar un terminal de un sistema en nombre de otro usuario, bien porque se conoce su clave, o bien porque abandonó el terminal pero no lo desconectó y ocupamos su lugar. El término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona.

SPOOFING

Mediante este sistema se utiliza una máquina con la identidad de otra persona, es decir, se puede acceder a un servidor remoto sin utilizar ninguna contraseña. ¿Cómo se hace esto? Pues utilizando la dirección IP de otro usuario, y así hacemos creer al servidor que somos un usuario autorizado. En máquinas UNIX se suelen utilizar para estos ataques los servicios "r", es decir, el rlogin y rsh; el primero facilita es procedimiento de registro en un ordenador remoto, y el segundo permite iniciar un shell en el ordenador remoto.

SNIFFER

Un sniffer es un dispositivo que captura la información que viaja a través de una red, y su objetivo es comprometer la seguridad de dicha red y capturar todo su tráfico. Este tráfico se compone de paquetes de datos, que se intercambian entre ordenadores, y estos paquetes a veces contienen información muy importante, y el sniffer está diseñado para capturar y guardar esos datos, y poder analizarlos con posterioridad. Un ataque mediante un sniffer se considera un riesgo muy alto, ¿por qué?, pues porque se pueden utilizar los sniffers para algo más que para capturar contraseñas, también pueden obtener números de tarjetas de crédito, información confidencial y privada, etc. Actualmente existen sniffers para todas las plataformas, ya que los sniffers se dedican a capturar datos, no computadoras, y por ello es igual la plataforma que se utilice. Algunos sniffers son los siguientes: Gobbler, ETHLOAD, Netman, Esniff.c (se distribuye en código fuente), Sunsniff, linux_sniffer.c, etc.

Algo que hace especialmente peligrosos a los sniffers es que no se pueden detectar, ya que son aplicaciones pasivas y no generan nada, con lo que no dejan ningún tipo de huella, y son especialmente indetectables en DOS y Windows 95 y trabajo en grupo, aunque en UNIX y Windows NT hayan más posibilidades de detectarlo

1.3 Hackers y Crackers

La red ha dado muchos titulares a los periódicos sobre vulneraciones de sistemas, obtención de datos secretos, etc. Y como había que llamarlos de alguna forma se los denomina, en círculos profanos, hackers. Principalmente la culpa la tienen los periodistas y los medios de comunicación, por no informarse sobre un tema antes de escribir o hablar sobre él, y todo esto ha creado en la sociedad una confusión sobre la denominación a estas personas, y se utiliza esta palabra para comportamientos diferentes, que no tienen ni punto de comparación con lo que ese término significa, y que "deshonra" a los verdaderos hackers.

Un hacker es una persona muy interesada en el funcionamiento de sistemas operativos; suele tener mucho conocimiento en lenguajes de programación. Además conoce la mayoría de los agujeros de un sistema operativo o de los protocolos de Internet, y los que no conoce los busca, y la única forma de buscarlos es intentar entrar en los sistemas de otro ordenador o servidor. Se puede decir que los hackers se mueven por fines de autorrealización y conocimiento, nunca provocan daños intencionados en las máquinas, y comparten su información de forma gratuita y desinteresada. Obviamente la difunden también para que se le reconozcan los méritos de su trabajo, pero eso sucede en todas las actividades humanas. No estoy justificando con esto la actividad de los hackers, pues en España su actividad por muy "pedagógica" que pueda parecer vulnera el derecho a la intimidad, un derecho fundamental que proclama la Constitución Española de 1978, y otros preceptos de nuestro ordenamiento jurídico; pero en cualquier caso hemos de dar a cada uno lo que se merece, y no atribuirle conductas que no hacen, y "desprestigiar" su nombre.

Los crackers son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas.

Pero estas definiciones son demasiado generales para denominar de una u otra forma a una persona, que se introduce en otros sistemas ajenos; deberíamos conocer sus motivos, intenciones, etc.

Un aspecto para diferenciar a un hacker de un cracker puede ser que el primero crea sus propios programas, ya que tiene muchos conocimientos en programación, y además en varios lenguajes de programación, mientras que el segundo se basa en programas ya creados que puede adquirir, normalmente, vía Internet. Otro aspecto diferenciador es que el interés de un cracker es destrozar la máquina que hay al otro lado, no es constructivo como un hacker, que trata de "mejorar" la red dando a conocer sus incursiones y los fallos que ha encontrado.

¿Por qué existen los crackers?

La existencia de los crackers es muy simple, al igual que en la vida real nos podemos encontrar personas constructivas y otras destructivas, en la red también sucede lo mismo. Además muchos crackers son como mercenarios, es decir, obtienen información restringida de los sistemas a los que entran y luego la venden al mejor postor, o puede ser incluso que haya sido contratado para que busque algo en concreto que interesa a alguien (normalmente empresas que quieren conocer secretos de otras). A estas personas se las suele denominar erróneamente hackers, pero no es así son crackers.

Como se ha dicho antes, los hackers comparten sus descubrimientos con el resto de usuarios de Internet, lo cual hace que se conozcan los fallos de seguridad en las redes, y se ponga remedio a esos fallos, con lo que cada vez conseguimos una red más segura y fiable, esto es lo que los diferencia de los crackers, los cuales sólo tienen un ánimo destructivo, pues venden información, destruyen datos, modifican ficheros, introducen en los programas códigos malignos, que crean problemas en el sistema donde se ejecutan, en definitiva, lo único que hacen es crear problemas en la red.

2. Delitos informáticos

*La Estafa Informática. Texto que versa sobre la regulación en el Código Penal de la estafa utilizando los medios informáticos.

*El Derecho a la Intimidad. Regulación y protección de este derecho en nuestro país.

*La Propiedad Intelectual. Aquí se desarrolla el tema de la propiedad intelectual en España.

*La Propiedad Industrial. En este documento se analizan los aspectos legales referentes a la propiedad industrial en España.

2.1 La estafa informática

Una de las cosas que proporciona la informática es poder realizar muchas tareas sin moverse de casa o la oficina. Esto supone que ya no existe un contacto directo entre las personas para acometer determinadas faenas. Como consecuencia de ello se ha producido un gran cambio en el mundo empresarial y de negocios, y, entre otras cosas, se han abierto nuevas perspectivas de consumo mediante el uso de Internet. Todos los que navegamos por Internet, conocemos que se venden cientos de productos, de diferentes marcas y modelos a través de la red, el ciberespacio se ha convertido en un nuevo sector a tener en cuenta para las empresas; lo cual es muy lógico, pues se ahorran muchos costes y amplían su potencial de mercado, por ejemplo, imagínese los costes que una empresa puede tener para establecer una sucursal en otra provincia de España, y ahora piense los costes que puede tener una empresa creando su propia página en Internet, con catálogos de sus productos o servicios, descripción de los mismos, precio, atención al cliente por correo electrónico, etc. (imagínese si lo que queremos es establecer una simple sucursal en otro país). Lógicamente todo depende del tipo de empresa de que se trate y del producto o servicio que venda, pero esta reflexión nos sirve para pensar en la importancia de la red para muchas empresas. Pero todo el monte no es orégano, y nos podemos encontrar con que la supuesta empresa nos manda productos que no son, no podemos reclamar directamente porque no sabemos dónde se ubica la empresa, o simplemente hemos hecho un pago con la tarjeta de crédito y no nos han dado el servicio o producto; todo esto afecta al consumidor, pero las empresas también pueden ser objeto en este comercio de una estafa, piénsese en dar número de tarjetas de crédito falsas pero que el robot acepta como válidas (conocido en el mundo de Internet como "carding"), etc. Con todo esto vemos que tanto empresas como consumidores pueden ser estafados usando medios informáticos, por supuesto estos sólo son unos ejemplos relativos a la red, pero también se pueden dar otros casos.

En definitiva, con la ayuda de las nuevas tecnologías, aparecen nuevos delitos y nuevas formas de comisión de delitos. Ante esto el legislador no se puede quedar de brazos cruzados y no regular este aspecto de la informática, y así ha sido. Un ejemplo claro de esto es la introducción de la estafa informática en el Código Penal, que no es otra cosa que una estafa cometida usando medios informáticos; y así se regula en dicho texto legal:

Art. 248. 2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la trasferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Este artículo es la mayor novedad del Código Penal de 1995, respecto de la estafa. Con este artículo se nos equipara con el resto de naciones de nuestro entorno cultural y social; pero además cubre la laguna legal que existía con anterioridad a este artículo, pues la informática, las telecomunicaciones, la tecnología, etc. avanza a pasos agigantados, y muchas veces el Derecho no reacciona a tiempo para regular las nuevas situaciones que se dan cada vez que hay un avance tecnológico.

Este artículo 248. 2 CP esta regulando una estafa normal y corriente, excepto que aquí no se engaña, ya que a una máquina no se la puede engañar, esto sólo se puede hacer a los humanos.

Obviamente como en cualquier otra estafa ha de haber un ánimo de lucro, la transferencia no consentida de cualquier activo patrimonial, y el perjuicio de un tercero.

El ánimo de lucro ha de ser entendido como la intención de obtener un enriquecimiento patrimonial correlativo al perjuicio ocasionado. Este ánimo de lucro constituye un elemento subjetivo del tipo, y su ausencia hace que la conducta realizada sea atípica, y por tanto impune.

Para que se dé la estafa ha de haber una transferencia no consentida de un activo patrimonial, en forma de entrega, cesión o prestación de la cosa, derecho o servicio.

Por último, ha de existir un perjuicio para un tercero, que es la diferencia de valor entre lo que se atribuye a otro y lo que se recibe (si es que se recibe): si la contraprestación es de igual valor que la prestación otorgada, no hay delito, aunque pueda haber un perjuicio indemnizable por la vía civil; y si la contraprestación es de menor valor, puede haber un delito de estafa, aunque no haya civilmente perjuicio alguno.

El concepto "manipulación informática" es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.

Con todo lo anterior podemos definir la estafa informática como la "manipulación o alteración del proceso de elaboración electrónica de cualquier clase y en cualquier momento de éste, realizada con ánimo de lucro y causando un perjuicio económico a un tercero" (Vives Antón − González Cussac).

Se diferencia en las estafas informáticas de las cometidas dentro del sistema y las cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo, y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las manipulaciones de datos hechas antes, durante o después de la elaboración de los programas, siendo éstas las causantes del engaño que determina de disposición patrimonial.

Para que exista delito de estafa la suma de lo defraudado ha de superar las cincuenta mil pesetas, de lo contrario sería una falta de estafa regulada en el art. 623.4 CP donde se prevé un arresto de seis fines de semana o multa de uno a dos meses; mientras que el delito de estafa informática esta castigado con la pena de prisión de seis meses a cuatro años, obviamente cuando exceda las cincuenta mil pesetas, y cumpla todos los

requisitos del art. 248.2 CP.

2.2 Derecho a la intimidad

La Constitución Española de 1978 protege el derecho a la intimidad en su art. 18.4 CE emplazando al legislador para que lo desarrolle con una Ley posterior, y así lo hizo mediante la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD). Aparte de esta Ley también el Código Penal protege la intimidad en el art. 197 CP. Pero antes de comenzar este análisis de la intimidad la hemos de definir. La intimidad puede entenderse como la voluntad de una persona física o jurídica de que no sean conocidos determinados hechos que tan sólo ella o un número limitado de personas conoce (Muñoz Conde).

La intimidad y las nuevas tecnologías en el Código Penal.

Las nuevas tecnologías cada vez se van implantando más en nuestra sociedad, hasta el punto de que se ha hecho indispensable para determinadas tareas de vital importancia el uso de la informática y las telecomunicaciones, y además proporcionan un gran servicio a toda la sociedad. Aparte de esto que se ha expuesto, seguro que a cualquier persona se le puede ocurrir un buen número de beneficios que las nuevas tecnologías proporcionan; pero como cualquier cosa en este mundo tiene sus aspectos negativos, y en este sentido la informática y las telecomunicaciones son utilizadas para atacar uno de los bienes fundamentales, constitucionalmente reconocidos, de cualquier persona: la intimidad. La informática se ha convertido en el medio propicio para atentar contra la intimidad de las personas, ya sea por simple altruismo (piénsese en los hackers, mal llamados piratas informáticos), o con fines lucrativos; de cualquiera de las dos formas la intimidad de una persona se ve afectada.

Por todo ello, el legislador ha de regular una realidad social, y penar determinadas conductas lesivas de ciertos bienes fundamentales de la persona. Entre otras leyes tenemos el Código Penal de 1995, el cual dedica el Título X del Libro II, a los delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio. En nuestro análisis sólo nos interesan los preceptos referentes a los delitos contra la intimidad, y en concreto los que usen medios informáticos para ello.

Por un lado, tenemos el art. 197.1 CP donde se contempla el tipo básico de descubrimiento de secretos, que consiste (como su denominación indica) en apoderarse de secretos para descubrir, sin una posterior divulgación o publicidad; con ello vemos que el delito se consuma simplemente con el apoderamiento para descubrir, aunque no se descubra nada (STS de 8 marzo de 1974). La jurisprudencia ha entendido por apoderamiento la aprehensión u obtención ilícita, así como la retención de lo recibido por error.

Como se deduce del propio art. 197.1 CP, ha de existir la finalidad de conocer algo reservado, el sujeto ha de apoderarse del secreto para descubrirlo, pero no de revelar, pues en dicho caso estaríamos ante la figura agravada del art. 197.4 CP.

Pero, ¿qué se entiende por secreto?, es "el conocimiento reservado a un número limitado de personas, y oculto a otras"; secreto será pues todo conocimiento reservado, que el sujeto activo no conozca, o no este seguro de conocer, y que el sujeto pasivo no quiera que se conozca; pero no hemos de confundir el secreto con el objeto en el que materializa, que puede ser un papel, una carta, mensajes de correo electrónico o cualquier otro documento personal. También hemos de tener presente que cuando los documentos afecten a la seguridad nacional, nos hemos de remitir a lo regulado en los arts. 583.3 y 584 CP, que prevén penas de doce a veinte años, y de seis a doce años, respectivamente. Además cuando se trate de secretos de empresa, se ha de tener presente lo dispuesto en los arts. 278 y 279 del CP.

El art. 197.1 CP, también regula la interceptación de las comunicaciones mediante "... artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación...". La pena que se prevé en art. 197.1 CP, es de uno a cuatro años de prisión, y multa de doce a veinticuatro meses.

Por otro lado, tenemos el art. 197.2 CP. En éste el objeto material sobre el que ha de recaer la conducta típica son "datos de carácter personal o familiar ajenos". La conducta típica que se recoge en este art. puede ser tanto apoderarse, utilizarse o modificar, en perjuicio de tercero, es decir, toda acción de tomar, coger, o poner bajo su poder o control, p. Ej. copiar.

Como podemos observar hay elemento subjetivo del tipo, que es "en perjuicio de tercero", donde "en" denota intencionalidad, y el perjuicio ha de interpretarse en sentido amplio, y por tanto no solo incluye los daños económicos.

Los datos personales o familiares han de estar registrados, esto es, contenidos, recogidos, anotados, transcritos, o grabados en "ficheros o soportes", y por tanto puede ser en un sistema informático, electrónico o telemático.

El último inciso hace referencia a "acceder por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero". Vemos que las conductas típicas son acceder, alterar o utilizar, pero ya no datos reservados, sino "ficheros o soportes informáticos, electrónicos, o telemáticos". En resumen este artículo castiga básicamente el "hacking", esto es, acceder a un sistema, sin estar autorizado para ello, y visualizar los datos de éste. Además se pueden dar otras conductas, como puede ser aprovecharse de esa información, y alterar, modificar, cambiar o vaciar la información que el sistema vulnerado contenía. La pena con que se sanciona estas conductas es prisión de uno a cuatro años, y multa de doce a veinticuatro meses, al igual que el art. 197.1 CP.

Pero el Código Penal no se queda ahí, además contiene una figura agravada (asigna una pena de dos a cinco años de prisión), recogida en el art. 197.3.1º CP, en la que además de realizarse la conducta de apoderarse de un secreto, también se divulga ese secreto, con lo cual la vulneración de la intimidad es todavía más grave, y por ello el legislador ha penado esta conducta más gravemente. El concepto divulgación ha de entenderse como la comunicación a una o más personas de lo descubierto, incluso aunque estas personas no estén interesadas en su conocimiento. Por "revelar" hemos de entender el descubrir o manifestar el secreto. Por "ceder" se ha de entender transferir, o traspasar a otro una información.

Incluso el legislador ha previsto otro tipo agravado, el del art. 197.4 CP, si los hechos descritos en el tipo básico los realizan "las personas encargadas o responsables" de los ficheros, soportes, archivos o registros. Con ello vemos que la agravación (prisión de tres a cinco años, si se realiza la conducta de los párrafos 1 y 2 del art. 197 CP, y prevé la pena en su mitad superior si verifica la conducta del párrafo 3 del mismo artículo del CP) se produce por una especial circunstancia del sujeto activo. Por supuesto hemos de delimitar el concepto de "personas encargadas o responsables", y para ello lo debemos hacer de forma restrictiva, es decir, sólo serán encargados o responsables las personas que en virtud de una disposición legal o contractual posean esa condición, por ejemplo, el administrador del sistema, que normalmente es responsable en virtud de un contrato.

Por otro lado en el Código Penal, en su art. 197.5, se prevé otra agravación en función del contenido de los datos descubiertos, y en concreto cuando se traten de datos "sensibles", que son los referentes a la "ideología, religión, creencias, salud, origen racial o vida sexual". La agravación se produce porque tiene un mayor contenido de injusto el vulnerar la intimidad en sus vertientes más fundamentales y elementales. La agravación se manifiesta en aplicar en su mitad superior las penas previstas en sus respectivos artículos.

Otra figura cualificada es la contenida en el art. 197.6 CP, donde se prevén penas superiores cuando las

conductas descritas en el tipo básico se realicen con "ánimo de lucro", y a su vez distingue la punición dependiendo de si los datos son "sensibles" (art. 197.5 CP), o no lo son (párrafos del 1 al 4, del art. 197 CP); en el primer caso se prevé que se aplique una pena de cuatro a siete años, y en el segundo caso se prevé que se aplique al apena respectiva en su mitad superior. El ánimo de lucro se refiere a obtener una recompensa evaluable económicamente, con lo que su interpretación no plantea mayor dificultad.

LORTAD

La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal (LORTAD), nace como consecuencia de la remisión que establece el art. 18.4 CE a favor del legislador, así como de la necesidad material de regular este aspecto de la sociedad actual. Esta ley trata de dar una serie de derechos a los afectados y obligaciones a los responsables de los ficheros, para así hacer más transparente la gestión de todos los datos que son recogidos de una persona, y que no se vulnere el derecho a la intimidad, al honor, etc. de dicha persona, por ejemplo, divulgando esos datos.

Para ello lo primero que se necesita saber es qué ficheros existen con datos de carácter personal, y para ello se crea el Registro General de Protección de Datos, donde el creador del fichero tiene la obligación de inscribirlo en dicho registro (arts. 18.1 y 24.1 LORTAD) junto con una serie de detalles como son designar un responsable del fichero, la finalidad del fichero, el tipo de datos que contiene, etc. (arts. 18.2 y 25.1 LORTAD), a esos ficheros se le pueden realizar inspecciones a instancia de parte o de oficio (art. 28.1 Estatuto de la Agencia de Protección de Datos), por la Agencia de Protección de Datos (APD), para comprobar si son acordes al texto de la ley, estando el titular obligado a permitir el acceso a la APD a los ficheros que contienen dichos datos de carácter personal (art. 28.2 EAPD). Sobre esos ficheros el afectado tiene una serie de derechos.

Derecho de oposición (art. 5 LORTAD). Los afectados tienen derecho a saber determinados aspectos de la utilización de los datos que los propios afectados vayan a revelar, a saber:

a.− De la existencia del fichero, finalidad y destinatarios de la información.

b.− Del carácter obligatorio o facultativo de las preguntas que se le hagan.

c.− Consecuencias de la respuesta positiva o negativa.

d.− De los derechos de acceso, rectificación y cancelación.

e.− Identidad y dirección del responsable del fichero.

Se puede salvar este trámite si la naturaleza de los datos o las circunstancias en que se recaban se pueda deducir todo lo anterior.

Derecho de impugnación (art. 12 LORTAD). Se pueden impugnar los actos administrativos o decisiones privadas que impliquen una valoración del comportamiento del afectado cuyo único fundamento sea el tratamiento automatizado.

Derecho de información (art. 13 LORTAD). Cualquier persona tiene derecho a acceder al Registro General de protección de Datos, de forma gratuita, para conocer los ficheros que existen con datos de carácter personal, conocer sus finalidades, etc.

Derecho de acceso (art. 14 LORTAD). El afectado puede acceder a sus datos en todos los ficheros que existan. Esto se puede hacer sólo a intervalos mínimos de doce meses, excepto si tiene un interés legítimo, en cuyo caso lo podrá hacer antes.

Derecho de rectificación y cancelación (art. 15 LORTAD). Los datos que sean inexactos o incompletos serán rectificados y cancelados en su caso. Si hubieran sido cedidos, el responsable del fichero deberá comunicar la rectificación o cancelación al cesionario.

Derecho de tutela (art. 17 LORTAD). Cualquier actuación en contra de la LORTAD puede ser objeto de reclamación a la APD, según el procedimiento establecido. Contra las resoluciones de la APD cabe recurso contencioso−administrativo.

Existen ciertos casos en los que estos derechos enumerados se ven limitados, básicamente de los ficheros de titularidad pública. Según el art. 21 LORTAD, los ficheros policiales de las Fuerzas y Cuerpos de Seguridad del Estado están exentos de la aplicación de los derechos enumerados por la Ley, en los casos en que este en juego la defensa del Estado, la seguridad pública, la protección de derechos y libertades de terceros, etc. Por otro lado, el art. 21.2 LORTAD también extiende esta eximente a los ficheros de la Hacienda Pública cuando obstaculice actuaciones administrativas que traten de hacer cumplir las obligaciones tributarias, y en cualquier caso cuando el afectado este siendo objeto de una inspección tributaria. Por último también están los limites establecidos a estos derechos por el art. 22 LORTAD.

Paralelos a estos derechos tenemos una serie de deberes y obligaciones por parte del responsable del fichero, como son:

Deber de adoptar medidas de seguridad (art. 9 LORTAD). El responsable del fichero debe de garantizar, en la medida de los posible, que no se puede acceder a los datos, mediante medidas técnicas u organizativas.

Deber de secreto (art. 10 LORTAD). El responsable del fichero ha de mantener en riguroso secreto los datos que están contenidos en los ficheros, incluso después de cesar en el cargo.

Deber de rectificación y cancelación (art. 15 LORTAD). El responsable esta obligado a rectificar o cancelar los datos que sepa que son inexactos, en el plazo que determine la Ley.

Deber de información al cesionario (art. 15 LORTAD). Las rectificaciones o cancelaciones realizadas por el cedente han de ser comunicadas al cesionario.

Deber de conservación (art. 15 LORTAD). Los datos personales han de ser conservados el tiempo que determine la Ley o las relaciones contractuales que tenga el responsable del fichero.

Deber de información al afectado (art. 25 LORTAD). El responsable del fichero ha de comunicar al afectado cualquier cesión, y los datos correspondientes establecidos en este mismo artículo.

Deber de cooperación con la APD (art. 38 EAPD). El responsable del fichero esta obligado a dejar acceder a la APD a los ficheros que tiene, y en caso contrario se considerará infracción leve, según el art. 43.2 LORTAD, lo cual conllevaría a una sanción de entre 100.000 ptas. y 10.000.000 ptas.

Respecto de la cesión de los datos de carácter personal la LORTAD en su art. 11.1 establece que los datos han de ser utilizados para fines vinculados a las funciones legítimas del cedente y del cesionario, y siempre con el consentimiento del afectado. Pero también la necesidad de consentimiento del afectado puede omitirse en los supuestos que el art. 11.2 LORTAD establece, a saber:

Cuando la Ley prevea otra cosa.

Cuando se trate de datos recogidos de fuentes accesibles al público.

Cuando el establecimiento del fichero implique la necesaria conexión con otros ficheros, siempre y cuando se

ciña al fin que la justifique.

Cuando el cesionario sea el Defensor del Pueblo, el Ministerio Fiscal, o Jueces y Tribunales, en el ejercicio de sus funciones legítimas.

Cuando la cesión se produzca entre Administraciones Públicas, y el cesionario los utilice para los mismos fines que la Administración cedente (art. 19.1 LORTAD).

Cuando la cesión de los datos referentes a la salud sea necesaria para solucionar una urgencia o para realizar estudios epidemiológicos, según lo establecido en el art. 8 de la Ley 14/1985, de 25 de abril, General de Sanidad.

Las sanciones que prevé la LORTAD están recogidas en los arts. 43 y 44. En el art. 43 LORTAD, se establecen los casos en que una infracción es leve, grave, o muy grave; y en el art. 44 LORTAD se fijan las multas que corresponde a cada tipo de infracción, y son:

Leves: multa de 100.000 ptas. a 10.000.000 ptas.

Graves: multa de 10.000.001 ptas. a 50.000.000 ptas.

Muy graves: multa de 50.000.001 a 100.000.000 ptas.

Según el art. 46 LORTAD las infracciones muy graves prescriben a los tres años, las graves a los dos años, y las leves al año.

Por todo ello, las empresas deberán tomar medidas para no ser castigado con alguna de las sanciones que se prevén en el art. 44 LORTAD. Entre otras medidas proponemos:

a.− .Responsabilizar del fichero a una persona física con independencia de que ante la APD aparezca una persona jurídica.

b.− Adoptar las medidas de seguridad necesaria.

c.− Crear procedimientos de acceso a los ficheros precisos.

d.− Prever la posibilidad de Auditorías Informáticas.

e.− Comprobar si los tratamientos previstos están controlados según la Ley.

f.− Prever la información que se debe suministrar al afectado.

g.− Prever los procedimientos de notificación.

h.− Incluir en los cuestionarios que la empresa emita aquellos datos informativos que la Ley exija que se han de dar al afectado.

Por otro lado la Agencia de Protección Datos también hace sus propias recomendaciones a los usuarios de Internet:

Información en la recogida de datos

Cuando suministre datos personales a cualquier organización (proveedores de acceso, proveedores de

contenido, vendedores a través de comercio electrónico, etc.) sea consciente de a quién se los facilita y con qué finalidad.

Procure averiguar la política de sus proveedores y administradores de listas y directorios en lo que se refiere a venta, intercambio o alquiler de los datos que les suministra. Solicite que sus datos personales no vayan unidos a su identificación de acceso a Internet.

Finalidad para la que se recogen los datos

Desconfíe si los datos que le solicitan son excesivos para la finalidad con la que se recogen o innecesarios para el servicio que se le presta.

Tenga en cuenta que cuando introduce su dirección de correo electrónico en un directorio, lista de distribución o grupo de noticias, dicha dirección puede ser recogida por terceros para ser utilizada con una finalidad diferente, como por ejemplo, remitirle publicidad no deseada.

Cuando navegue por Internet, sea consciente de que los servidores Web que visita pueden registrar tanto las páginas a las que accede como la frecuencia y los temas o materias por las que busca, aunque no le informen de ello. Asimismo, su pertenencia a determinados grupos de noticias y listas de distribución puede contribuir a la elaboración de perfiles más o menos detallados sobre su persona.

En el caso de que no desee dejar constancia de sus actividades en la red, utilice los mecanismos para preservar el anonimato que se describen en el cuerpo de este documento.

Seguridad en el intercambio de datos

Utilice, siempre que sea posible, las últimas versiones de los programas navegadores, ya que cada vez suelen incorporar mejores medidas de seguridad. Considere la posibilidad de activar en dichos programas las opciones que alerten sobre los intercambios de datos no deseados y no rellene aquellos datos que no desee hacer públicos (por ejemplo, dirección de correo electrónico, nombre, apellidos, etc.).

No realice transacciones comerciales electrónicas a través de proveedores con sistemas "inseguros" o no fiables. Consulte el manual de su navegador para averiguar cómo informa de que se ha establecido una conexión con un servidor seguro.

Recuerde que existen sistemas de dinero electrónico que preservan el anonimato de sus compras en Internet.

Utilice los mecanismos de seguridad que tenga a su alcance para proteger sus datos de accesos no deseados. El medio más fiable para conseguirlo es el cifrado de los mismos.

Salvo que se utilicen mecanismos de integridad, autenticación y certificación (firma digital, notarios electrónicos, etc.) no confíe ciegamente en que la persona u organización que le remite un mensaje es quien dice ser y en que el contenido del mismo no se ha modificado, aunque esto sea así en la inmensa mayoría de las ocasiones.

Para terminar

Siempre que se le soliciten datos personales que no esté obligado legalmente a suministrar, sopese los beneficios que va a recibir de la organización que los recoge frente a los posibles riesgos de utilización irregular de los mismos.

Ante cualquier duda sobre la legalidad de la utilización de sus datos de carácter personal, póngase en contacto

con la Agencia de Protección de Datos.

2.3 La Propiedad Intelectual.

El ser humano es un ser creativo (aunque muchas veces también destructivo), es decir, es capaz de crear obras de artísticas, científicas, literarias, etc. En un principio, estas creaciones tenían "solo" un valor moral, pero conforme se fue avanzando en los tiempos se vio la necesidad de regular este sector, pues se daban al principio casos de plagio, para atribuirse una persona los méritos del trabajo de otra; pero además se llegó a un punto en el que todas estas obras tuvieron un valor patrimonial, valían dinero porque estaban en el comercio, las personas comerciaban, y comercian, con estas obras, con lo que era muy fácil el que una persona obtuviera beneficios económicos, por el trabajo intelectual de otra, sin autorización de esta última, que es su autor original. Por todos estos motivos se vio la necesidad de proteger a los autores de estas obras, para que así se les reconociera socialmente por su trabajo, y además obtuvieran un beneficio patrimonial de ese trabajo, lo cual es totalmente legítimo. Por ello apareció el concepto de propiedad intelectual.

Según el Texto Refundido de la Ley de propiedad intelectual, ésta se compone de derechos de carácter personal y patrimonial que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas por la ley.

Según esta definición la propiedad intelectual se compone de un aspecto moral y otro patrimonial. Esta dimensión patrimonial la vemos reflejada en el art.270 CP, cuando hace referencia de forma expresa al ánimo de lucro del sujeto activo. Sin embargo, el contenido moral no aparece por ningún lado en el Código Penal, el cual se ve dañado cuando se realiza la conducta típica.

De acuerdo con el art. 1 de la Ley de propiedad intelectual, la propiedad intelectual es del autor de la obra por el mero de hecho de haberla creado él, con lo que la inscripción registral no es necesaria para que se realice el tipo del art. 270 CP. Por otro lado, hemos de tener muy en cuenta, y según el sentido literal de dicho art. 270 CP, que el consentimiento del autor excluye el tipo.

La conducta descrita en el art. 270 CP se ve agravada por las circunstancias previstas en el art. 271 CP, que son: la especial trascendencia del beneficio económico y la especial gravedad del daño causado. Cuando se da alguna de estas circunstancias la pena se agravará, en concreto se pasa de la pena de prisión de seis meses a dos años (tipo básico), a prisión de un año a cuatro años (tipo agravado). Para determinar la gravedad del daño causado tendremos que orientarnos con las previsiones de la Ley de propiedad intelectual.

Según el Código Penal, además de la respectiva pena, el Juez puede decretar también el cierre provisional o definitivo del local, industria o establecimiento del condenado.

Las conductas descritas en el art. 270 CP son reproducir, plagiar, distribuir, comunicar, importar, y exportar obras literarias, artísticas, o científicas, sin la autorización de los titulares de los derechos de propiedad intelectual.

Especial referencia merece el tercer párrafo del art. 270 CP, ya que esta castigando expresamente la tenencia o fabricación de mecanismos que vulneren la protección de los programas informáticos, es decir, en base a este artículo es ilegal tener o fabricar programas para "crackear" otros programas. Esta idea es muy conveniente tenerla en mente, pues en Internet hay multitud de páginas en las que se nos ofrecen estos programas de "cracking"; por ello si se quiere tener una página especializada en el "cracking" y quieres ayudar a encontrar los programas a los que te refieres lo mejor es poner un "link" a otra página en la que esté el programa, pues el tenerlo en tu cuenta o en tu disco duro o un disquete puede conllevarte problemas. También se da mucho el caso de acceder a una página de esta índole y aparecer un mensaje de advertencia en el que se nos apercibe de la posible ilegalidad de tener en nuestra posesión estos programas, pero se nos exceptúa su ilegalidad en los casos en que se utilice con carácter educativo o investigador. Obviamente se puede alegar la eximente de

ejercicio legítimo de un derecho, oficio o cargo −p. Ej. Si se es profesor de alguna rama relacionada, personal investigador, etc.− regulado en el art. 20. 7º CP, por supuesto habrá que demostrarlo suficientemente, y que el Juez lo aprecie.

Como se desprende del art. 270 CP y de la Ley de propiedad intelectual, el medio que se utilice para realizar la conducta típica es indiferente, pues tanto en la Ley de propiedad intelectual, como en el Código Penal se nos dice que puede ser por "cualquier medio", y con ello quedan englobados tanto soportes físicos como digitales. Asimismo, objeto de propiedad intelectual puede ser cualquier obra original art. 10 LPI, por ejemplo, las fotografías, y por ello puede ser punible en base al art. 270 CP la venta de fotografías por personas no autorizadas por su titular. Como hemos dicho anteriormente, el ánimo de lucro es un elemento subjetivo del tipo, y sin el cual la conducta es atípica, y atípico sería el utilizar imágenes de cualquier sitio para ponerlas en tu página web, lo cual no quiere decir que no se pueda castigar en base a otros preceptos penales, civiles, o administrativos, siempre hay que atender a las circunstancias del caso concreto para determinar si se ha cometido una ilegalidad o no.

2.4 Delitos contra la propiedad industrial

La propiedad industrial es un derecho sobre un bien inmaterial, consecuencia de la inteligencia humana. Son bienes capaces de ser transformados en un bien material y físico, el cual puede ser transmitido, poseído, utilizado, etc.

La regulación y protección de la propiedad industrial en el Código Penal se encuentra en los arts. 273 a 277, que se ven completados por la Ley de patentes de invención y modelos de utilidad de 1986, y la Ley de marcas de 1988.

Lo que se trata proteger con estos artículos es el derecho a la utilización reservada de determinados objetos: la explotación exclusiva de un invento u objeto (art. 273 CP); un signo registrado, ya sea de una marca, un nombre comercial, o un rótulo de establecimiento (art. 274 CP); o de una denominación de origen, o indicación geográfica representativa de una determinada calidad (art. 275 CP).

En cualquiera de los casos anteriormente mencionados el objeto, logotipo, etc. Ha de estar registrado conforme a la Ley de marcas, en caso contrario no hay protección alguna, en base al Código Penal.

Las conductas típicas que se describen en cada artículo no requieren mayor explicación, y basta con leerlos para comprender lo que en ellos se dice, pues, están bastante claros.

A la hora de interpretar el art. 275 CP hemos de tener presente lo que se dispone en la Ley 25/1970, Estatuto de la viña, el vino y los alcoholes, y los Reales Decretos 1573/1985, y 1396/1993, relativos a productos agroalimentarios.

En todos los tipos se prevé una pena de prisión de seis meses a dos años, y multa de seis a veinticuatro meses, para las conductas que verifiquen el tipo correspondiente.

Para terminar este análisis de la regulación jurídico−penal, haremos referencia a lo dispuesto en el art. 276 CP, esto es, la agravante que atiende al especial valor de los objetos producidos o a la especial importancia de los daños ocasionados. Si se da éste caso la pena asciende a prisión de dos a cuatro años, y multa de ocho a veinticuatro meses, e inhabilitación especial para el ejercicio de la profesión relacionada con los delitos cometidos por un período de dos a cinco años.

Derechos

Y

delitos Informáticos

Consejos de la APD

Manifiesto de Free

La OCDE y la Criptografía

I. T. INFORMÁTICA DE SISTEMAS

Derechos y delitos Informáticos

Esther Joglar Alcubilla 24