Capítulo 13.- Seguridad y aspectos legales en Telepatología

LUIS ALFARO FERRERES

La seguridad es uno de los problemas más importantes y acuciantes desde que el crecimiento de Internet ha convertido los ordenadores en algo accesible a distancia. Se trata de una cuestión de gran complejidad, que requiere importantes esfuerzos e inversiones por parte de las compañías que desarrollan programas, y sistemas operativos. Como usuarios finales los patólogos no podemos llegar a dominar y entender todos las posible fallos de seguridad a los que estamos potencialmente expuestos, y los entresijos del funcionamiento de los programas que los permiten. Esto deben resolverlo los desarrolladores de programas y los administradores de redes. Por nuestra parte si debemos conocer algunas medidas básicas que no creen vulnerabilidades en los equipos que empleamos, y que puedan ser aprovechadas por otros.

En este capítulo se describen medidas de protección, y conductas ante nuestros ordenadores para evitar caer en fallos de seguridad y unas nociones de aspectos legales en relación con la Telepatología.

13.1.- Seguridad en el correo electrónico.

13.1.1.- Virus informáticos

El correo electrónico se ha convertido probablemente en la fuente más común de transmisión de virus informáticos. Es importante estar alerta ante la posibilidad de que la recepción de un virus no ponga en peligro los datos almacenados en nuestros discos, o "abra puertas" para que puedan ser accesibles por otros.

A través del correo electrónico podemos recibir mensajes con texto, páginas web y ficheros adjuntos (*attachments*).

Los mensajes que incluyen únicamente texto no pueden causar ningún problema. No es posible que un mensaje con texto contenga un virus. Los virus son programas informáticos que realizan una serie de operaciones de naturaleza muy variada pero potencialmente muy peligrosa; y es imposible que un texto estático de ordenes o ejecute comandos en nuestro ordenador. Por lo tanto podemos estar tranquilos ante cualquier mensaje de correo electrónico que contenga texto exclusivamente.

Los ficheros adjuntos a través del correo electrónico, son la vía esencial de transmisión de virus. La transmisión de ficheros es una función muy útil, y a pesar de su potencial peligrosidad no debemos renunciar a ella. Sí conviene conocer y recordar una serie de conceptos. La recepción de un correo con un fichero adjunto infectado no suele ser suficiente para que afecte nuestro ordenador. La infección se produce casi siempre en el momento que abrimos el fichero infectado. Por tanto **la primera medida ante la recepción de mensajes con ficheros de procedencia dudosa o de contenido incierto, es no abrirlos**. Si disponemos de algún programa antivirus, podemos revisar antes el fichero sospechoso para prevenir riesgos. Algunos virus utilizan mecanismos para no generar sospechas. Cuando infectan un ordenador entre las posibles acciones que realizan, una de ellas puede ser la de reenviarse por correo electrónico a los contactos registrados en la libreta de direcciones del ordenador infectado. Por lo tanto quien reciba el virus verá un remite de una persona conocida, lo cual no le inducirá a sospechar del fichero adjunto que lo incorpora.

La forma más sencilla de hacer telepatología es simplemente enviado ficheros adjuntos con imágenes en el correo electrónico. Esto es una práctica relativamente segura ya que los ficheros gráficos raramente contienen virus. Así que antes de abrir un fichero en el correo electrónico debemos ver la extensión del fichero para saber de qué tipo se trata.

Las extensiones de ficheros gráficos como .jpg .gif .tif .bmp no son especialmente peligrosas. Los virus casi siempre vienen incluidos en ficheros con extensión de archivos ejecutables (.exe) ó en otras ocasiones ficheros del tipo .vbs.

Es aconsejable que nuestro ordenador tenga activada la opción para ver las extensiones de los ficheros. Ello se activa en cualquier ventana del explorador de archivos, por ejemplo, pulsando sobre **Mi PC**, abriendo el menú **ver,** seleccionando **opciones de carpeta,** y en la solapa **ver,** desactivando (quitando la cruz) la opción de: **ocultar extensiones para los tipos de archivos conocidos.**

[Los ficheros llevan un nombre de longitud variable, seguido de un punto y una extensión de tres letras que indica que clase de fichero es].

Esto es importante pues los virus que nos llegan muchas veces intentan esconder su extensión real, e incluyen en su nombre una parte final acabada en .txt (por ejemplo *nombre.txt.exe*). Si nuestro ordenador no muestra las extensiones, el fichero simulará ser un archivo de texto y tomaremos menos precauciones frente a él.

Otro tipo de fichero potencialmente peligrosos son los ficheros generados con el procesador de textos Word, y con extensiones **.doc**. Aunque básicamente estos ficheros contienen texto, la potencia de este programa permite insertar en estos ficheros una serie de comandos (las llamadas macros), que pueden ser diseñados para que efectúen operaciones similares a los virus. Si queremos enviar ficheros de Word adjuntos en mensajes de correo es recomendable que guardemos el fichero (con la opción **guardar como** de Word) en formato .rtf en lugar del .doc. El formato .rtf no permite la adición de macros potencialmente peligrosos, y es además compatible con la mayor parte de procesadores de texto.

Por último, el tercer tipo de mensajes de correo electrónico que podemos recibir son los que contiene páginas web, o mensajes en formato html. Estos, aunque en principio no son tan peligrosos como los que llevan ficheros adjuntos infectados, pueden esconder en su código html (en forma de *scripts*) algunas ordenes con potencial peligrosidad. Frente a este tipo de mensajes los programas de correo electrónico modernos suelen detectar las acciones peligrosas e impedirlas, o al menos, dar mensajes de aviso. Los desarrolladores de programas están continuamente revisando sus versiones para que no se produzcan fallos de seguridad a través de este tipo de mensajes.

En cualquier caso, siempre puede ser de ayuda **disponer de un antivirus actualizado**, que nos proteja de los virus, que potencialmente puedan llegar en nuestro correo electrónico.

13.1.2.- Confidencialidad

El correo electrónico es una herramienta de utilidad inmensa y conociéndola bien podremos sacarle el mayor rendimiento. Una función poco empleada es la de envío de *copias ciegas.* Todos los programas de correo electrónico permiten enviar copias de mensajes además de a un destinatario concreto, a otro u otros múltiples. En las versiones en español de Outlook, por ejemplo, encontramos un campo **Para**, a rellenar con la dirección donde queremos enviar el mensaje, y otro campo marcado como **CC:** para especificar copia o copias donde enviar también el mensaje. Existe otro tercer campo llamado **CCO:** (copias ocultas) (si nuestro programa de correo no lo muestra podemos activarlo en el menú **Ver**, de un mensaje nuevo, marcando la opción **Todos los encabezados**), con una peculiaridad y es que las copias que enviemos a través de este campo no quedarán reflejadas para el resto de los receptores del mensaje. Es decir quienes reciban el mensaje no conocerán si se han enviado otras copias, y a quién o quiénes. Es fácil percibir el interés de esta opción. Por otro lado, es frecuente que necesitemos enviar un mismo mensaje a un número elevado de receptores. Si utilizamos la opción de copia CC, cada receptor, recibirá además del mensaje, la identidad y la dirección de correo de todo el resto de destinatarios del mensaje. Como es posible que muchos de nuestros posibles receptores no deseen que su dirección de correo se divulgue a terceros, la alternativa de enviar copias a través de la opción CCO: tiene gran interés.

Los mensajes de correo electrónico que recibimos vienen generalmente perfectamente identificados, con el nombre del remitente y su dirección de correo electrónico. Esta información, sin embargo, puede borrarse o alterarse con facilidad, ya que refleja los datos que nosotros mismos hemos introducción de las **propiedades** de la cuenta de correo al configurarla. Evidentemente, si alguien nos está enviando virus, mensajes no solicitados, o simplemente no quiere que conozcamos su identidad, alterará esos datos. A pesar de ello, los mensajes de correo llevan todos incluida una cabecera que contiene información sobre la procedencia del mensaje, y los servidores por donde ha pasado, lo que nos va a permitir obtener una valiosa información.

Para acceder a la cabecera del mensaje, seguimos este procedimiento:

Abrimos el mensaje que queramos identificar, menú de **archivo**, opción **propiedades**, solapa **detalles**, y casilla, **código fuente del mensaje**. Allí vamos a encontrar antecediendo al texto del mensaje, la cabecera del mismo, con gran cantidad de información. La forma como está escrita resulta un poco difícil de interpretar pero fijándonos podrá entresacar muchos detalles. La siguiente es una cabecera de un mensaje tomado al azar:

```
Received: from correo.fercl.es ([196.119.29.141])
       by correo.ctv.es (8.9.3/8.9.3) with ESMTP id MAA10169
       for <lalfaro@ctv.es>; Tue, 3 Apr 2001 12:26:33 +0200 (MET DST)
Received: from y7i4e8 ([195.235.225.241]) by correo.fercl.es  with Microsoft
SMTPSVC(5.5.1877.537.53);
        Tue, 3 Apr 2001 12:53:26 +0200
Message-ID: <20010406121755.640$f1e1ebc3@y7i4e8>
From: "Carlos García" <carlgo@mail.es>
To: "Luis Alfaro" <lalfaro@ctv.es>
Subject:
Date: Tue, 3 Apr 2001 12:17:55 +0200
MIME-Version: 1.0
Content-Type: multipart/alternative;
       boundary="----=_NextPart_000_0012_01C0BC38.1CDE6020"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4133.2400
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4133.2400
X-UIDL: c16620532a6ffae8d8d39c7a999a3e72
```

En la primera parte encontramos información del servidor de correo desde donde nos llega el mensaje (**Received: from**) y su dirección IP. Estos datos son suficientes para poder identificarlo con facilidad.

Existe en Internet servidores Whois, que proporcionan a partir de la dirección IP los datos informativos básicos del servidor de correo desde donde nos ha llegado un mensaje concreto: el nombre de la organización o institución emisora, la dirección física, el teléfono, el nombre y correo electrónico de la persona responsable, etc. La siguiente dirección corresponde, como ejemplo, a uno de estos servidores Whois:

http://www.ripe.net/cgi-bin/whois

A continuación, en la cabecera del mensaje consta la dirección de nuestro servidor de correo que ha recibido el mensaje, y nuestra dirección particular de correo, hasta donde nos lo ha transmitido.

Viene también escrito el nombre y la dirección del remitente (aunque estos datos pueden alterarse modificándolos en la configuración de nuestra cuenta de correo).

Cuando el mensaje ha pasado por varios servidores veremos una relación de los mismos, antecedidos por las palabras *received from* y *received by* que nos indican que ordenadores han transmitido y recibido el mensaje. Cada servidor intermedio añade su cabecera al principio del mensaje, por lo que veremos antes la parte final de la trayectoria y después el punto de origen.

Una parte importante es la que queda expresada en el apartado de Message-ID. Los caracteres que se recogen aquí expresan en la primera parte, el año, el mes, el día, la hora, los minutos, y los segundos, del momento en el que se emitió el mensaje. A continuación tras un punto hay una serie de caracteres que expresan el código con el que el servidor de correo origen ha registrado la procedencia del mensaje, después viene una arroba @ y otros caracteres que identifican el *nombre* ordenador de origen. Estos últimos datos los podemos también modificar en la configuración de nuestro ordenador. Pero el código que registra el servidor de correo de origen, permite identificar sin ninguna duda la procedencia del mensaje. Este código queda almacenado en los servidores de correo, y aunque no es de acceso público, en caso de actividades delictivas a través del correo electrónico, serviría para encontrar al autor del mensaje delictivo.

Otra información que proporciona la cabecera del mensaje es el programa de correo electrónico empleado, y su versión.

A pesar de toda esta información que nos otorga cierta seguridad y protección frente al correo electrónico, hemos de tener en cuenta que existe forma de eludir estos mecanismos de identificación, como son la existencia de servidores de correo anónimo. Estos servidores funcionan de la siguiente manera. Los mensajes que reciben llevan una dirección de destino y una cabecera con los datos de identificación de origen, como hemos visto. Al recibirlos borran la cabecera y lo envían a otro servidor intermedio (probablemente localizado en países diferentes) que actúa de la misma manera (borra la cabecera, aunque ésta ya no contenía información de origen, sino del servidor anterior remitente) y lo envía a un tercer servidor que sigue el mismo procedimiento. Cuando el mensaje llega a su destino ha pasado por unos cuantos servidores intermedios, cada uno de los cuales ha borrado la cabecera del mensaje, lo que hace casi imposible determinar el origen inicial del mensaje y la trayectoria que ha seguido.

13.1.3.- Encriptación y Firma Electrónica

Otra de las peculiaridades del correo electrónico, es la naturaleza abierta de los mensajes. Como toda información que se transmite a través de Internet, el correo electrónico circula por la red atravesando una serie de nodos intermedios hasta llegar a su destino, y a lo largo de esta trayectoria es susceptible de ser interceptado y leído. Para garantizar la confidencialidad de los mensajes se emplean métodos de encriptación.

Existen muchos sistemas de claves para codificar los mensajes. En la actualidad entre los más utilizados destacan los que emplean dos claves complementarias, una pública y otra privada (secreta). Estas claves funcionan de forma que los mensajes encriptados con una de las claves sólo pueden descifrarse con la otra, su complementaria. La clave pública, como indica su nombre, puede divulgarse con toda libertad ya que es la que se utilizará por terceros para enviarnos mensajes codificados. Estos mensajes sólo pueden descifrarse con nuestra clave privada, su complementaria, (la cual sí debe ser conocida únicamente por nosotros para garantizar la confidencialidad). A la inversa cuando queramos enviar a alguien un mensaje encriptado, buscaremos o le pediremos su clave pública y con ella generaremos un fichero codificado sólo descifrable por medio de la clave privada del receptor.

En ocasiones los mensajes por su contenido no necesitan ser encriptados, pero si se *autentifican* igualmente con el sistema de claves, para garantizar que no han sufrido alteraciones o cambios durante su transmisión. Estos mensajes se “firman” electrónicamente con nuestra clave privada, y a su recepción nuestro interlocutor aplicando nuestra clave publica, que conocerá o le habremos hecho llegar, y gracias a su complementariedad, sabrá que el mensaje no ha sufrido manipulaciones. Por lo tanto, las daves publicas deben ser conocidas por todos aquellos que quieran enviarnos mensajes. A menudo están disponibles en las páginas web personales, pues no hay ningún inconveniente en que cualquiera disponga de ellas. Sólo hay que preservar el secreto de la clave privada.

Muchos programas de encriptación utilizan este sistema. Quizá el más conocido es el llamado PGP (*pretty good privacy*), que tiene versiones de libre distribución (http://www.pgpinternational.com). También el Outlook de Microsoft dispone de un sistema de encriptación y firma digital, en el menú **Herramientas**, sección **Opciones**, solapa **Seguridad**, sin embargo, en este caso para hacerlo funcionar es necesario disponer antes de un identificador digital que otorgan otras instituciones, que sirve como garantía para que quienes reciben nuestros mensajes sepan que proceden realmente de nosotros y no han sido suplantados o falsificados por otros.

13.2.- Seguridad en el entorno de trabajo

Otra cuestión importante, relativa a la seguridad, corresponde a la de nuestro ordenador de trabajo. En este caso debemos considerar si se trata de un ordenador de uso personal y exclusivo, al que nadie más tiene acceso, y por tanto no es necesario disponer de medidas de protección y seguridad especiales; o bien si utilizamos un ordenador compartido, o en un entorno de trabajo en el que múltiples usuarios utilizan el mismo ordenador, o al menos tiene posibilidad de accesos a él. Por último es importante tener en cuenta las conexiones en red de nuestro ordenador. Es decir si forma parte de una red dentro de un hospital, y los niveles de acceso que existen desde el interior (intranet), y también los posibles accesos a través de red desde el exterior (Internet).

Los niveles de seguridad de que disponemos dependen en gran medida del sistema operativo que utilicemos. Así en sistemas como Windows 2000, o las versiones previas de NT, existen habilitados numerosas posibilidades y mecanismos de protección, ya que son sistemas operativos especialmente diseñados para el funcionamiento en red, donde hay que cuidar especialmente estas medidas de seguridad. Otros sistemas operativos más orientados al funcionamiento doméstico como Windows 95, 98 o ME, contienen menos recursos de seguridad. En estos últimos por ejemplo, aunque al iniciarlos podemos encontrarnos con un recuadro que nos solicita una contraseña, el desconocerla no impide acceder al sistema, ya que incluso pulsando sobre el botón de cancelar tenemos acceso completo a todo el sistema.

Con estos sistemas operativos existe, sin embargo, una posibilidad de modificar este recuadro de acceso con contraseña de forma que si no la tecleamos correctamente se rechace nuestro acceso. Esta puede ser una primera medida que incremente el nivel de seguridad de nuestro ordenador.

Para hacerlo hay que modificar el registro con el siguiente procedimiento:

[*El registro es una base de datos que guarda la configuración, las propiedades y opciones de funcionamiento de nuestro sistema operativo. La modificación del registro nos permite obtener y variar importantes posibilidades en nuestro ordenados, pero es esencial hacerlo con cierto conocimiento y cuidado ya en el caso de modificar equivocadamente algunas opciones, podemos alterar gravemente el funcionamiento de nuestro sistema operativo e incluso, perder toda capacidad de funcionamiento. Por todo ello antes de modificar el registro se recomienda efectuar copias de seguridad de sus ficheros (user.dat y system.dat), de forma que ante algún error de configuración podamos restaurarlos para volver a la configuración previa. La importancia del registro es tal que el propio sistema operativo realiza copias de seguridad automáticamente. Para restaurar algunas de las copias de seguridad por problemas con el registro, debemos iniciar el sistema operativo en modo DOS y teclear:* ***scanreg/restore***].

La edición del registro se hace pulsando sobre el botón de **inicio**, opción **ejecutar** y tecleando **regedit**.

Para que nuestra contraseña de entrada impida el paso a quines no la conozcan (en Windows 95/98/ME) hay que modificar:

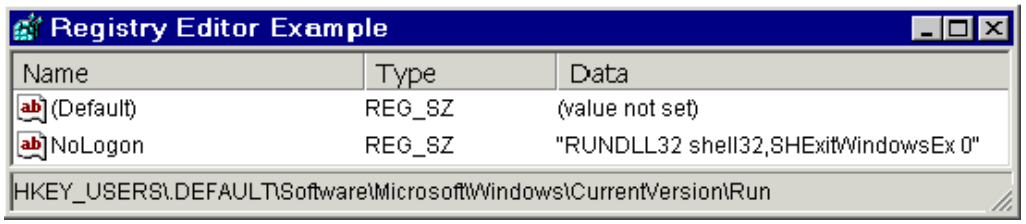
1.- Acceder al panel de control (**inicio, panel de control**) y en el apartado de **usuarios** crear un nuevo usuario, indicando nombre de usuario y contraseña.

2.- Reiniciar el ordenador entrando con el usuario y contraseña que acabamos de crear

3.- Acceder al registro (**inicio, ejecutar**, y teclear **regedit**) y en la sección [HKEY_USERS], localizar este apartado:

[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run]

y allí crear un nuevo valor de la cadena llamado "NoLogon", y al que daremos el siguiente valor: "RUNDLL32 shell32,SHExitWindowsEx 0"



Tras este procedimiento cada vez que iniciemos de nuevo nuestro ordenador se nos pedirá la contraseña y en el caso de no rellenarla, o hacerlo incorrectamente el sistema no permitirá el acceso.

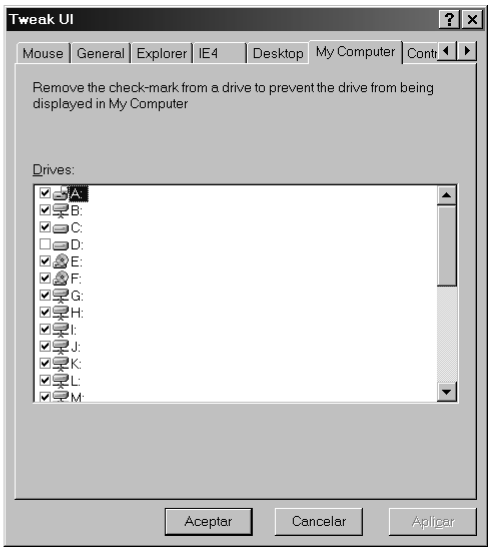
Una opción más sencilla es configurar nuestro protector de pantalla con una contraseña. Esta posibilidad es útil y cómoda si queremos proteger nuestro ordenador momentáneamente, cuando nos hemos apartado de él por un periodo breve. Incluso podemos hacer que al arrancar el ordenador se nos solicite esta contraseña, si colocamos el fichero del protector de pantalla al que le hemos configurado la contraseña en el directorio de inicio (es decir el directorio que ejecuta todos lo programas que hemos colocado en él cada vez que arrancamos el ordenador). Para colocar allí el fichero del protector de pantalla pulsamos con el botón derecho del ratón sobre el botón de **inicio** de la barra de tareas, elegimos **abrir**, y dentro veremos el directorio de

programas que contiene dentro el subdirectorio de **inicio**. Colocamos allí el fichero del protector de pantalla. (estos ficheros se encuentran habitualmente en el directorio Windows o en el directorio windows/system y tiene la extensión .scr)

El nivel de protección que da esta medida no es demasiado bueno, pues para saltar la contraseña, cualquier usuario con algunos conocimientos de informática, puede reiniciar el ordenador en modo a prueba de fallos y desactivarla.

Otra forma muy sencilla de proteger, aunque sea de forma superficial nuestro ordenador se basa en el empleo de una opción contenida en el sistema operativo de Windows 9x que no se instala por defecto. Se trata de una serie de utilidades y recursos del sistema que pueden resultarnos muy valiosas. Se encuentran en este directorio TOOLS\RESKIT\POWERTOY (para Windows 98) del CD-ROM de instalación, y para instalarlas hay que localizar el fichero denominado Tweakui.inf, y pulsando sobre él con el botón derecho del ratón escogemos instalar.

Una vez instalado. En el panel de control de Windows (**inicio, configuración, panel de control**), encontraremos un nuevo icono denominado Tweak UI, pulsando sobre el accedemos a todas las opciones.



De especial utilidad puede servirnos la que se encuentra en la solapa My Computer. Allí podemos des-seleccionar las unidades de disco que no queremos que aparezcan al pulsar sobre el icono de Mi PC. Por ejemplo en el caso de disponer de dos discos duros (C: y D:) Podemos seleccionar el D: en el que podríamos guardar los datos más importantes de modo que si alguien se sienta ante nuestro ordenador y realiza una exploración superficial, no percibirá que existe un segundo disco duro oculto.

Windows 2000 y NT tienen un buen sistema de seguridad para proteger nuestros programas y datos. Existen distintos niveles de acceso con diferentes contraseñas, de modo que sólo el administrador con su contraseña, tiene acceso a todo el sistema y posibilidades de instalar o desinstalar programas y cambiar configuraciones. A cada usuario se le habilita una contraseña y se definen sus niveles de acceso, por ejemplo, a algunos usuarios, puede permitírsele el manejo de programas y acceso a datos pero no la instalación de nuevos programas.

La tercera posibilidad de funcionamiento, es que nuestro ordenador esté conectado a una red (intranet). En ese caso podemos definir si los otros miembros de la red tienen acceso a nuestros datos de forma parcial o total, y si pueden únicamente tener acceso de lectura o también puede escribir en nuestro disco duro. Estas opciones pueden modificarse y establecerse una contraseña para ellas.

En el caso que estemos conectados a una red, tendremos instalados los protocolos de funcionamiento de la misma, y pulsando con el botón derecho del ratón por ejemplo en nuestro disco duro (unidad c:) veremos una opción denominada **compartir**. Allí seleccionamos si queremos compartir nuestro disco. En el cuadro de diálogo podemos escoger para el resto de la red sólo acceso de lectura o total, y podemos proteger estas opciones con una contraseña. Si

sólo queremos compartir un directorio del mismo, efectuamos esta operación exclusivamente en ese directorio.

De la misma manera también podemos tener accesos a otros ordenadores de la Intranet en que nos encontremos, para ello pulsamos sobre el icono de entorno de red del escritorio y allí veremos los ordenadores conectados a la red, pulsado sobre cada uno de ellos podemos acceder a sus datos (si en dichos equipos está configurada la opción de compartir) e incluso imprimir con las impresoras conectadas a tales equipos (igualmente, en el caso de que hayan configurado esta opción)

13.3.- Aspectos legales aplicables a la Telepatología

La Ley de Propiedad Intelectual (Real Decreto 1/1996 de 12 de abril, BOE de 22 de abril) [5/98 de 6 de marzo] protege entre otras cosas las imágenes fotográficas, aunque distinguiendo las creaciones originales de carácter artístico, que tienen un plazo de protección durante toda la vida del autor, y de los 70 años posteriores a su muerte (art. 26); y las imágenes que reproducen escenas, figuras y acontecimientos de la realidad cotidiana, las cuales tienen un plazo de protección de 25 años desde su realización (art. 128). Aunque podría ser sujeto de interpretación y discusión, a cual de estas dos categorías pertenecerían las imágenes de telepatología, en cualquiera de los dos casos, el autor dispone en esos periodos del derecho a autorizar su reproducción, distribución y difusión. El hecho de encontrar imágenes en páginas web, con la consiguiente facilidad para su copia, no autoriza por ello hacer libre uso de las mismas.

Por otro lado, la misma ley de Propiedad Intelectual establece que los derechos sobre cualquier creación (imágenes de telepatología, en nuestro caso) se obtienen simplemente por su creación, sin que sea necesario una inscripción en Registros de Propiedad Intelectual.

Como excepción la Ley dispone (art. 32) que se pueden utilizar fragmentos de obras sujetas a propiedad intelectual, a modo de citas ó para su análisis, comentario o juicio critico, siempre que tal utilización se haga con fines docentes o de investigación, lo cual podría entrar en la materia de la telepatología. (en este caso debe siempre indicarse la fuente y el autor de la obra utilizada).

Otro aspecto de la Ley de Propiedad Intelectual es la que hace referencia al uso privado de cualquier tipo de obras, publicadas, o ya divulgadas; ya que en este caso, está permitida la copia y reproducción de fotografías, o imágenes macro o microscópicas en nuestro caso, para uso particular, siempre que la copia no sea objeto de utilización lucrativa (art 31.2).

Aunque la legislación intenta adaptar las cuestiones de protección de datos a las diferentes posibilidades de transmisión y divulgación; en los entornos de redes digitales, resulta difícil que encontrar soluciones a cada unas de las múltiples posibilidades que existen.

Así, aunque descargar imágenes a partir de páginas web y hacer uso de ellas resulte ilegal, salvo en las excepciones citadas, más difícil de adaptar a la legislación resulta el hecho de reproducir imágenes a partir de enlaces directos con otras páginas, de modo que las imágenes susceptibles de interés no estén físicamente en la página en cuestión, sino que permanezcan en el servidor original, al que accedemos mediante un enlace en el código html. Incluso con este tipo de enlace, la autorización para el empleo de estas imágenes es conveniente.

En la práctica, y pese a las garantías legales, resulta difícil restringir en medios como Internet la descarga indiscriminada de imágenes, u otro tipo de documentación publicada en páginas web. Debemos pues, tener en cuenta esta consideración cuando coloquemos imágenes o cualquier otra información en páginas web, en ámbitos de Telepatología.

Ante esta situación, siempre se puede incluir un mensaje en nuestras páginas con referencia a las cuestiones de copyright. Por ejemplo, el siguiente *script* incluido en el código html de una página web actúa desactivando la función del botón derecho del ratón, que utilizamos de forma preferente en los navegadores de Internet para descargar imágenes (con la opción **guardar como**). En su lugar muestra un mensaje con el texto que hayamos incluido (en nuestro ejemplo: "*Esta imagen está sujeta a derechos de autor. Para su descarga solicitar autorización*").

```
<script language="JavaScript">
<!--
 function click() {
   if (event.button==2) {
```

```
     alert("Esta imagen está sujeta a derechos de autor. Para su descarga
solicitar autorización");
   }
 }
 document.onmousedown=click
// -->
</script>
```

Este *script* puede complementarse con otro, que a partir de un enlace, abra nuestras imágenes en una nueva ventana con tamaño predefinido, y al que hemos suprimido las barras de menús, de navegación, y la capacidad de ampliarla o reducirla. Este nuevo enlace podría conectar a otra página web distinta, en lugar de ir directamente a la imagen, con la posibilidad de anular en esa segunda página enlazada, la función de descargar con el botón derecho del ratón empleando el *script* anterior :

```
<script language="JavaScript">

function NAME_IT() {

window.open('foto1.htm','EANITHING','toolbar=no,location=no,directories=no,sta
tus=no,menubar=no,resizable=no,copyhistory=no,scrollbars=no,width=400,height=3
00');
}

</script>

<a href="javascript:NAME_IT()">Foto 1</a>
```

De esta manera el enlace a una imagen conduce a una nueva página web (foto1.htm, en nuestro ejemplo), que se despliega en una ventana predefinida (de 400x300 en nuestro caso), que puede incluir el nombre de la imagen xxxx.jpg, y su *path* situado en otro directorio. Ello combinado con el *script* que suprime el menú del botón derecho del ratón hace más difícil localizar y descargar la imagen.

Aunque ninguna de estas medidas evita por completo que nuestras imágenes colocadas en páginas web puedan obtenerse sin autorización, si al menos pone ciertas trabas a las descargas.

Otra cuestión legal referida a imágenes fotográficas, no sólo de telepatología sino en cualquier otro ámbito medico, es la relacionada con aquellas imágenes de pacientes, que reproducen parcial o totalmente a estos, y que deben respetar los derechos de intimidad y propia imagen, y por tanto independientemente que reflejen una lesión de interés médico, deben ser tratadas de manera que no permitan la identificación del paciente. En este caso es de aplicación la:

Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD) (BOE 14 de diciembre de 1999)

Entre los presupuestos de esta ley, se plantea el limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos, siguiendo el mandato del artículo 18.4 de la Constitución.

Recoge las medidas de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, entendiendo como tal, cualquier información concerniente a personas físicas identificadas o identificables

La ley establece una serie de medidas de seguridad técnica de los ficheros automatizados que contengan datos de carácter personal. El establecimiento de las medidas de seguridad, para garantizar los derechos reconocidos en la Ley, se configura como una de las obligaciones por las que, de no verificarse, se incurriría en responsabilidades administrativas.

Se establecen tres niveles de seguridad en función de la información tratada.

El nivel básico se configura como el aplicable por defecto a cualquier fichero.

El nivel medio se encuentra formado por los relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los de solvencia patrimonial y crédito.

El nivel alto lo forman los ficheros con datos sobre la ideología, religión, creencias, origen racial, salud o vida sexual, y los recabados para fines policiales sin consentimiento del afectado.

La legislación intenta resolver problemas que surgen del empleo de las nuevas tecnologías digitales. Aunque parece necesaria la elaboración de criterios normativos para regular nuevos aspectos de la sociedad derivados de la implantación de las tecnologías de la información. Los intentos legislativos suelen encontrar criticas y resistencia por parte de usuarios, al tiempo que despiertan recelos, por ser entendidos como elementos de control, y de restricción de libertades. Un ejemplo de ello es la próxima Ley de Servicios de la Sociedad de la Información y Comercio Electrónico. Esta Ley se encuentra en fase de anteproyecto, y puede ser consultada en la página web del Ministerio de Ciencia y Tecnología:

http://www.setsi.mcyt.es/

En ella se regulan las responsabilidades en las que incurren quienes ofrecen servicios de comercio digital, y si bien esas responsabilidades suponen garantías para los usuarios de dichos servicios frente a abusos y conductas fraudulentas, el catalogo de infracciones de la ley es también fácilmente interpretable como un cúmulo de restricciones y de amenazas a la libertad de expresión, con riesgos de extensión a otras páginas web no comerciales.

Por ello, quizá para moverse en los entornos digitales -que desde sus comienzos se han caracterizado por un crecimiento y una expansión muy por delante de las leyes reguladoras, posiblemente un tanto caóticos, pero enormemente provechoso- haya que compaginar la protección que ofrece la legislación frente a delitos evidentes, junto a una propia autoprotección con mecanismos de seguridad ante los riesgos de compartir un misma e inmensa red con los más variados y diversos habitantes.