>>> Gestión: nuevas tecnologías >>>>>>>>>>>>>>>>>>>>>>>>>>>>

Despachos de abogados en redes sociales: sí, pero con precauciones y responsabilidad

Hace unos meses que paralelamente al auge de la web 2.0 se han oído voces de alarma que advertían de la falta de privacidad de las herramientas que forman la web social y el peligro que podía suponer para los usuarios si se hace un uso indebido.

Muchas de estas herramientas, como Facebook, Flickr o Twitter, son actualmente utilizadas no sólo por particulares, sino también por empresas, colectivos, instituciones públicas y despachos de abogados para ganar presencia en la red y mejorar su posicionamiento, incluso para llevar a cabo campañas de marketing on-line.

En este sentido, la responsabilidad es la mejor respuesta a la creciente preocupación por la protección de los datos de carácter personal y profesional. En primer lugar, es importante **conocer bien el entorno** para determinar qué herramienta es la más adecuada para satisfacer las necesidades comunicativas del bufete (ganar visibilidad en los buscadores, realizar una campaña de promoción de un nuevo servicio, difundir comunicación corporativa en un entorno online, etc.), así como evaluar las implicaciones de cada una de las decisiones tomadas.

Asimismo, en la puesta en marcha de proyectos con estas herramientas es primordial **analizar a fondo la conveniencia de la plataforma a utilizar, tanto para sacarle el máximo rendimiento, como para difundir la marca y el prestigio del despacho con total seguridad.**

No se debe olvidar que Internet es un interesante escaparate comercial, por lo que debemos tener claro qué datos se quieren potenciar y cuáles son preferibles de preservar fuera de las herramientas 2.0. En otras palabras, **es aconsejable evitar los datos de carácter económico, aquellos excesivamente personales o que pudieran derivar en un uso fraudulento por parte de terceros, así como aquellos relativos a asuntos y clientes**. Es importante recordar que el buen uso de la web 2.0 no sólo implica al despacho, sino también a sus contactos, clientes y proveedores. También es recomendable leerse a fondo las condiciones de uso de cada servicio, y ante la duda, dejarse asesorar por un profesional.

Es aconsejable evitar los datos de carácter económico, aquellos excesivamente personales o que pudieran derivar en un uso fraudulento por parte de terceros, así como aquellos relativos a asuntos y clientes

Por otro lado, en el momento de establecer nuevos contactos y socios comerciales en las redes sociales (Facebook, LinkedIn, Xing, Viadeo), también se deben tomar **precauciones**: en primer lugar, asegurarse de que la persona que nos contacta es realmente una persona conocida y de confianza, y en segundo lugar, restringir los datos que los demás usuarios de una red y contactos propios pueden ver sobre el bufete y uno mismo. Asimismo, **es preferible no aceptar invitaciones de aplicaciones realizadas por terceros, la identidad e intenciones de los cuales desconocemos**.

Así pues, **un tratamiento profesional de la presencia del bufete en las redes sociales y otras herramientas 2.0 garantiza una correcta gestión de la identidad virtual del despacho y posibilita una evolución positiva de acuerdo con sus intereses**. En otras palabras, el conocimiento profundo del entorno online, la precaución y la responsabilidad son los mejores avales para evitar casos de phishing (robo de identidad) o apropiación indebida de datos confidenciales.

Iuris.doc

Dpto. Servicios Internet

>>> Opinión: protección de datos >>>>>>>>>>>>>>>>>>>>>>>>>>>

Cámaras y privacidad: Convivencia necesaria

El debate está servido, cada día son más frecuentes las noticias de actualidad referidas a situaciones relacionadas con cámaras de vigilancia, vídeos colgados en la Red que emiten imágenes en tiempo real desde videocámaras, cámaras instaladas en colegios, empleados cuyos movimientos se ven controlados constantemente, etc. La casuística es muy diversa y de lo más variopinta y la regulación actualmente aprobada en España no alcanza a clarificar todas estas situaciones.

Cada vez hay más denuncias originadas en la captación de imágenes a través de cámaras de videovigilancia, ello no es de extrañar por cuanto que, la instalación de sistemas de esta naturaleza se ha triplicado en el último año llegando hasta la elevada cifra de **15.000 cámaras instaladas en España con fines de vigilancia**. Un dato relevante y cuanto menos significativo es que **más del 90% de las mismas corresponden al sector privado y están orientadas a la seguridad privada**.

La inquietud por la seguridad y por la protección de bienes y personas por un lado y la necesidad en el ámbito empresarial de verificar que los empleados cumplen con sus funciones laborales por otro, conlleva la demanda de medios tecnológicos avanzados que permitan acabar con la inactividad laboral o erradicar la delincuencia allá donde la vigilancia privada no alcanza.

Se ha demostrado que los sistemas de videovigilancia suponen de por sí, un **elemento disuasorio** para persuadir al que "se siente observado" o "se sabe vigilado" ante la posible comisión de cualquier tipo de ilícito, así como de comportamientos que pudieran resultar inapropiados. Asimismo, de no conseguir evitar tales prácticas pueden ciertamente contribuir a su persecución.

Los sistemas de videovigilancia captan, graban, transmiten o almacenan las imágenes de los espacios públicos o privados que vigilan. En este sentido, es fundamental plantearse si al tratamiento de tales imágenes se aplican las normas sobre protección de datos de carácter personal.

La respuesta es sencilla, cuando tales grabaciones, con independencia de su almacenamiento o no, capten imágenes de personas físicas identificadas o que sean identificables a raíz de las mismas, esta información constituye un **dato de carácter personal** a los efectos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD).

En este mismo sentido y una vez sentado que la imagen constituye un dato personal sometido a los derechos y a las obligaciones de la normativa de protección de datos personales, habrá que precisar cuándo podemos instalar o utilizar cámaras de videovigilancia.

A este respecto, señalar que **para que exista legitimación respecto de su uso, no será suficiente con que el sistema reúna los requisitos técnicos que lo permitan funcionar sino que además, en principio, será necesario contar con el consentimiento de las personas objeto de captación**.

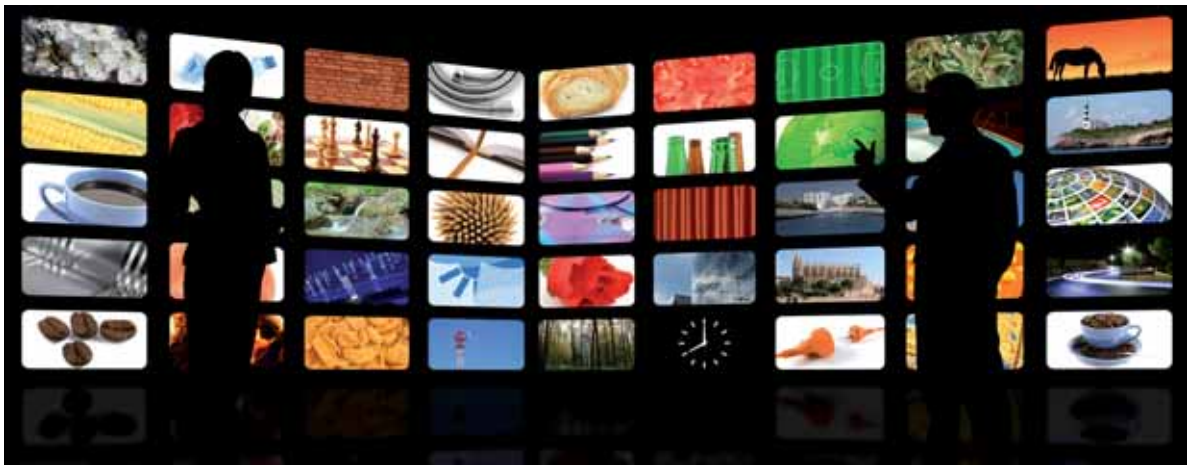
Si bien, la Agencia Española de Protección de Datos (AEPD) que es el órgano específico cuya misión es velar por el cumplimiento de la normativa referida, ha indicado que los supuestos en los que se requiere el consentimiento de las personas a las que vigilan es, en la actualidad, un supuesto todavía infrecuente.

Los sistemas de videovigilancia captan, graban, transmiten o almacenan las imágenes de los espacios públicos o privados que vigilan. En este sentido, es fundamental plantearse si al tratamiento de tales imágenes se aplican las normas sobre protección de datos de carácter personal

En este sentido, **puede existir una norma con rango de Ley que exima de la necesidad de obtención del consentimiento de los titulares de los datos personales, tal como, entre otros, es el caso previsto por la Ley 23/1992, de 30 de julio, de Seguridad Privada**. En esta Ley se establece que no se requerirá el consentimiento de dichas personas siempre que la instalación y el mantenimiento de las videocámaras las haya realizado una empresa de seguridad autorizada.

En relación con lo anterior, la resolución emitida por la AEPD en el Procedimiento Sancionador Nº PS/00071/2008 determina que **únicamente se está legitimado para instalar cámaras de videovigilancia cuando se cumplan los siguientes requisitos**:

- Que la instalación, el mantenimiento de los siste-



mas de seguridad, así como el tratamiento de las imágenes captadas se realice por empresas de seguridad privada.

- Que se disponga de un contrato que cumpla los requisitos establecidos en la normativa de seguridad privada.
- Que la empresa de seguridad que realiza la instalación y/o el mantenimiento se halle inscrita en el Registro de Empresas de Seguridad gestionado por el Ministerio del Interior.

Para que exista legitimación respecto de su uso, no será suficiente con que el sistema reúna los requisitos técnicos que lo permitan funcionar sino que además, en principio, será necesario contar con el consentimiento de las personas objeto de captación

Aún con todo lo anterior, será necesario firmar con las empresas de seguridad que lleven a cabo la instalación y el mantenimiento de las videocámaras un contrato de prestación de servicios que contenga los requisitos establecidos en el **artículo 12 de la LOPD** referido al acceso a datos por cuenta de terceros, así como los extremos que fueran necesarios contemplar respecto de su normativa de desarrollo.

Adicionalmente a lo indicado, el Responsable del uso o de la instalación de sistemas de esta naturaleza deberá tener en cuenta que:

- Su uso debe ser **proporcional**, entendiendo este principio como, la inexistencia de un sistema menos intrusivo o, de una medida menos moderada, para la consecución del mismo objetivo, así como, la imposibilidad de grabar imágenes a un alcance mayor al que realmente resulte necesario.

En este sentido, es importante señalar que toda la normativa reguladora de la materia coincide en la forzosa existencia del **principio de proporcionalidad o de mínima intervención** como justificación del recurso a esta tipología de sistemas.

- Se deberá **informar a las personas que transiten dentro del alcance de las cámaras sobre la captación y/o grabación de las imágenes**.

A este respecto, **la Instrucción 1/2006, de 8 de noviembre**, de la AEPD establece la obligación de ubicar un **cartel informativo** que identifique o alerte las zonas videovigiladas aunque sin la oportunidad de conocer la ubicación concreta de las cámaras puesto que, de este modo, se acabaría con la esencia misma de este método de seguridad.

- En caso de ubicarse en espacios privados, no podrán obtener imágenes de la vía pública sin la debida **autorización**.

En este caso, podría darse la circunstancia antedicha cuando resultara totalmente imprescindible para la finalidad de vigilancia que se persiga o por la imposibilidad de evitar tal extremo debido a la ubicación de las cámaras.

- Su uso deberá respetar los derechos de las personas y del resto del Ordenamiento Jurídico, tales como, los **derechos de acceso, rectificación, oposición o cancelación de las imágenes o el derecho al honor, a la intimidad y a la propia imagen**.
- **Las imágenes**, tal y como se establece en la Instrucción 1/2006, de 8 de noviembre, de la AEPD, **no se conservarán por un plazo superior a un mes**, considerado éste como el tiempo máximo de tenencia de las imágenes captadas.

En base a lo anterior, indicar que recientemente ha sido presentada y publicada por la AEPD la **"Guía sobre videovigilancia"**, documento de obligada lectura para todos aquellos que pretendan la instalación o el uso de videocámaras con fines de vigilancia,

puesto que, la misma ofrece indicaciones precisas y criterios prácticos que permiten el adecuado cumplimiento de la legislación vigente en este ámbito.

Asimismo, la Agencia Catalana de Protección de Datos, ha aprobado y publicado la **Instrucción 1/2009, de 10 de febrero**, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, como instrumento que delimita el marco jurídico aplicable en esta materia en el ámbito de actuación del órgano autonómico.

Esta Instrucción prevé la posibilidad de solicitar un informe a la Agencia Catalana de Protección de Datos en el proceso de implantación del sistema de videovigilancia, como una medida de mayor garantía a la hora de asegurar el cumplimiento de la normativa en materia de protección de datos en los tratamientos que se realicen.

En definitiva, el recurso a este tipo de dispositivos de seguridad requiere que, además de los requisitos técnicos necesarios para su instalación, se tengan en cuenta inevitablemente otros factores o condicionamientos en orden a conseguir mitigar o, por lo menos minimizar, el impacto que tales medidas pueden causar en derechos fundamentales de las personas, procurando la menor intromisión posible en su intimidad o en sus vidas privadas.

En base a todo lo expuesto, es inevitable cuestionarse hasta qué punto las personas estamos dispuestas a ceder un espacio de nuestra vida en beneficio de nuestra propia seguridad e integridad o incluso, en beneficio de la seguridad común.

Por **Esmeralda Saracíba**.
Consultora de Compliance de Ecija

>>> Contenidos web >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Cómo mejorar el uso del correo electrónico

Muchas veces, lo primero que hacemos al llegar al despacho es abrir el correo electrónico y ver los mensajes recibidos. Esta tarea que no debería llevarnos demasiado tiempo, se convierte a veces en un verdadero calvario si a los correos atrasados se unen los numerosos spam y mails no deseados que cualquier usuario suele recibir. Por ello, **se aconseja**:

- **Limpiar el buzó**n de correo nada más llegar, borrando sin demora y sin abrirlos los mensajes que claramente parecen indeseados.
- **No dilatar las respuestas**, contestarlos cuanto antes.
- **Evitar** en la medida de lo posible el envío de mensajes con ar**chivos adjuntos**
- Al finalizar la jornada, repetir la misma operación: **dejar la bandeja de entrada limpia de correo**s.

>>> Empresas >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Empresas: hay que controlar gastos, riesgos e implantar un sistema de recobro especializado

La crisis económica está suponiendo un aumento considerable de los **procedimientos concursales**, lo que está contribuyendo de una manera rotunda al colapso de los juzgados mercantiles que no dan abasto. Esto, por su parte, afecta negativamente a las empresas concursadas que ven reducidas sus posibilidades de viabilidad, dado que en la actualidad de cada diez concursos, nueve finalizan en liquidación, justo lo contrario de lo que pretendía originariamente la vigente Ley Concursal. Por ello, **se recomienda a las empresas** reforzar sus sistemas de control de gastos, seleccionar los riesgos y asumir ante el aumento de los impagados, un sistema de recobro especializado. En la coyuntura actual, lo importante es subsistir al margen del concurso.

>>> Recursos Humanos >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Sobre la importancia del buen ambiente en la empresa o en el despacho

Una organización con un clima laboral agradable, buenas relaciones interpersonales entre sus empleados y en la que **el manejo del recurso humano** sea una realidad siempre contará con trabajadores más motivados, integrados, colaboradores, creativos y con un nivel de rendimiento superior al promedio. Los recursos humanos son **una herramienta de gestión** muy importante para una organización. Bien utilizada, puede crear ventajas comparativas y competitivas en una compañía, pero lo principal es reconocer que **las organizaciones son el reflejo de sus trabajadores**; una empresa eficiente posee trabajadores eficientes y un buen clima laboral. La salud física y mental de los empleados, a su vez, también son el reflejo de una compañía.

Fuente: *"Puede ser un buen día"*
Por **Claudio Gregorio Pino**

Libros hechos por profesionales para los profesionales

www.tecnos.es

Legislación sobre Construcción
Edición de Editorial Tecnos

Legislación sobre pequeña y mediana empresa (PYME)
Edición de Editorial Tecnos

Legislación sobre Auditoría Pública
Edición de Belén González Díaz (coord.)

Legislación sobre el cambio climático
Edición de M.ª Ángeles González Bustos, Miguel Ángel González Iglesias y Dionisio Fernández de Gatta

Legislación sobre Fuerzas y Cuerpos de Seguridad
Edición de Carmen Chinchilla y Francisco José Alés (5.ª ed.)

La nueva Ley del Libro
Edición de Editorial Tecnos (2.ª ed.)

Legislación del Cuerpo Nacional de Policía
Edición de Editorial Tecnos

Lecciones del contrato de trabajo
Luisa Vicedo Cañada