consultas jurídicas

Carmen Perona
Abogada de CCOO

Imágenes en Internet

¿Qué puede ocurrir si publicamos imágenes de terceros en Internet?

B.B.M. (Valencia)

La Agencia Española de Protección de Datos ha hecho publico un decálogo de recomendaciones, apelando a la responsabilidad de los usuarios de Internet.

Así, en el ámbito de las redes sociales aconseja no grabar ni publicar imágenes o videos sin el consentimiento de quienes aparecen. Recuerda que cuando se publica una foto o escribe en un foro se puede estar incluyendo información sobre otras personas, lo que puede acarrear responsabilidades personales y jurídicas.

En este sentido, advierte, además, de que las redes sociales son una importante fuente para la obtención de información sobre las personas. Por ello, se debe garantizar la seguridad mediante una configuración adecuada del perfil y utilizando contraseñas apropiadas, sin olvidar que los buscadores pueden permitir a cualquier tercero obtener la información pública de los perfiles. Desaconseja publicar en ellos excesiva información personal y familiar (ni datos que permitan la localización física) así como aceptar solicitudes de contacto de forma compulsiva.

A este respecto, pide a las empresas que están detrás de las redes sociales, que pongan a disposición del usuario herramientas para el control absoluto de la información que publica en la red, con medios que limiten la posibilidad de etiquetar a otros usuarios recibiendo automáticamente una solicitud de aceptación o rechazo.

Cree que lo conveniente sería establecer, por defecto, el máximo grado de seguridad en el perfil del usuario, al contrario de lo que sucede ahora.

Asimismo, la Agencia alerta de otros riesgos en la red y previene ante el hecho de que en Internet no todo el mundo es quien dice ser, por lo que no hay que dar los datos si no se dice para qué los van a usar.

En cuanto a los mensajes de correo electrónico, si se envían a una variedad de destinatarios, se debe utilizar el campo Con Copia Oculta (CCO), y no hay que contestar nunca al spam. De hecho, se recomienda desactivar la opción que envía un acuse de recibo al remitente de los mensajes leídos del sistema de correo electrónico, ya que si un spammer recibe dicho acuse sobre que la dirección esta activa, enviará más spam.

Para evitar prácticas fraudulentas como el phishing, antes de aportar ningún tipo de datos personales en el comercio y banca electrónica conviene asegurarse de que se ha establecido una conexión segura con el portal y desconfiar de los correos que informan de cambios en las políticas de seguridad y solicitan datos y claves de acceso. Al suscribirse a un servicio on line o contratar un producto, hay que revisar la política de privacidad.

Tampoco los menores están a salvo. Por eso, se aconseja navegar con ellos, ayudarles a distinguir los riesgos y asegurarse de que no intercambien datos personales ni fotografías con desconocidos.