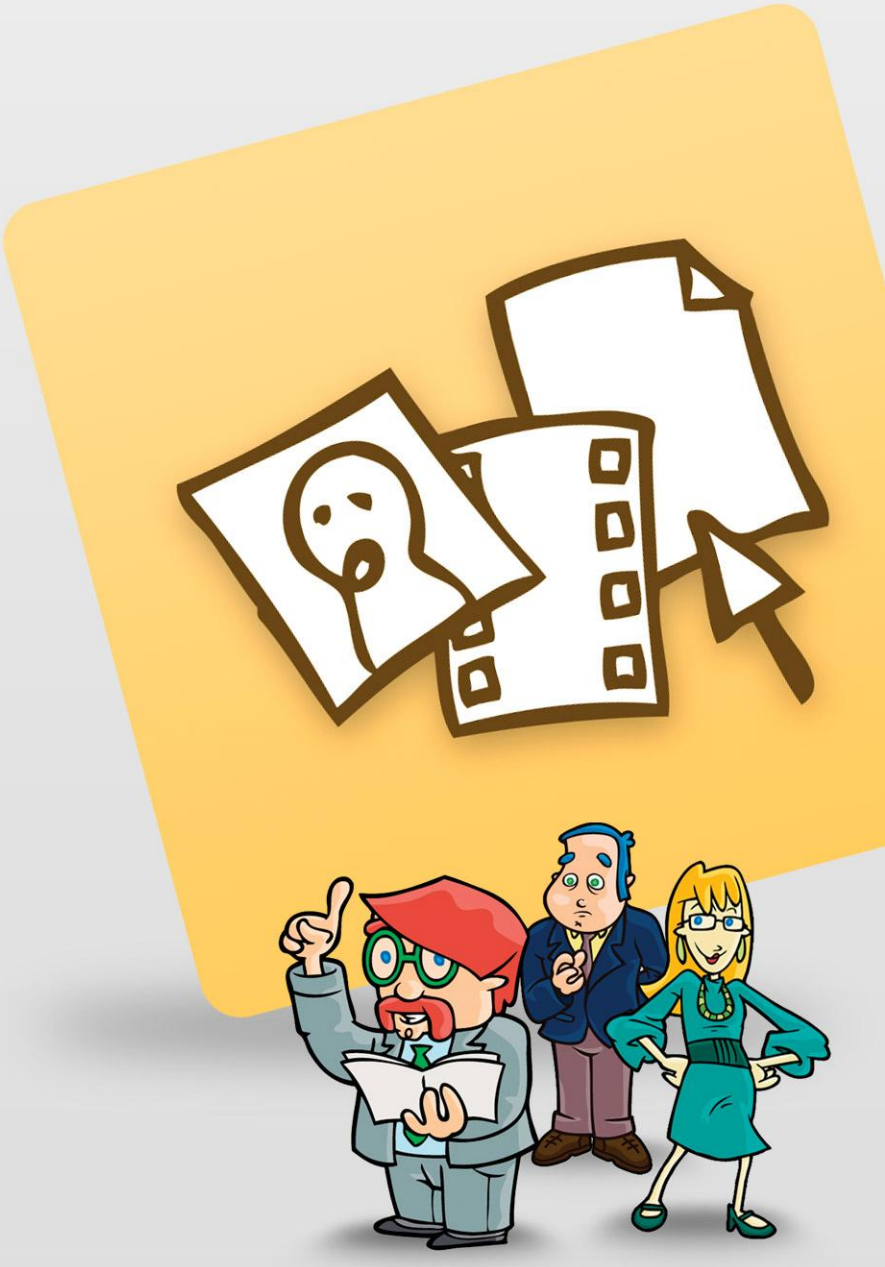
03

Imagen en los Servicios Web 2.0.



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ÍNDICE

I. OBJETIVOS

Concienciar del uso adecuado de la imagen (fotos y videos) en los servicios que componen el entorno Web 2.0 y sus consecuencias. Las imágenes muestran directa o indirectamente determinados atributos de la personalidad del usuario que pueden escapar de su control cuando son utilizadas en los servicios de Internet, poniendo en riesgo su privacidad.

II. CONCEPTOS

1. LA IMAGEN EN EL ENTORNO WEB 2.0.

La imagen es un dato de carácter personal, lo que supone otorgarle la protección y garantías que para éstos establece la normativa aplicable. Recuérdese que se considera dato personal **cualquier información concerniente a personas físicas identificadas o identificables.** Por eso, en la medida en que se puede establecer la identificación de una persona, el uso de la imagen puede afectar directa o indirectamente a su privacidad.

La imagen en Internet es uno de los elementos de la identidad digital que más caracterizan a la persona, puesto que muestra el aspecto físico y permite a los demás reconocerle. Ésta es una información especialmente sensible, puesto que una foto o vídeo sacados de contexto o en manos de terceros pueden influir negativamente en la identidad y reputación en la Red y, además, son susceptibles de manipulaciones.

Las consideraciones expuestas respecto a la privacidad del usuario en buscadores, páginas Webs y redes sociales, son plenamente aplicables al uso de las imágenes en el entorno Web 2.0.

a) Las plataformas online de publicación e intercambio de contenidos en formato de vídeo.

Servicios como Youtube, Dalealplay.com, Vimeo, etc. se caracterizan por la puesta a disposición de los usuarios de herramientas gratuitas y sencillas para el intercambio y la publicación de contenidos digitales (vídeos, fotos, textos, etc.).

Permiten el alojamiento de contenidos para que el resto de usuarios puedan visionarlos, y la interacción entre los usuarios añade la posibilidad de incluir comentarios respecto a los contenidos y otorgarles puntuaciones, así como enlazar los contenidos y publicarlos directamente en el perfil de la red social utilizada por los usuarios.

Los vídeos contienen mucha información que no se percibe directamente, como, por ejemplo, la matrícula de un coche, el nombre de una calle, el equipo de futbol donde entrena un menor, el colegio o instituto al que acude cada día,… En el caso de los adolescentes la situación se complica porque muchas veces cuelgan información sin tener en cuenta que lo que están poniendo en la Red puede identificarles y asociarles con comportamientos no adecuados (peleas, actos vandálicos, situaciones de acoso,…).

Como cualquier red social, las plataformas de publicación de videos se caracterizan por la viralidad (esto es, se propagan tan rápido como los virus) en la expansión de sus contenidos y la pérdida de control por parte del autor del video. A esta circunstancia hay que añadir que en los videos que se suben a dichas plataformas puede haber terceras personas cuya privacidad puede verse comprometida. En este sentido es preciso tener en cuenta el consentimiento o autorización de las personas que aparecen en el video subido a la red y las posibles consecuencias de dicha acción. Una buena medida de evaluación consistirá en preguntarse si supone algún riesgo que cualquier persona, y en cualquier momento, puedan ver esas imágenes. En el caso de una respuesta afirmativa es mejor no subirlas. Las imágenes se difunden de forma rápida y extensa y esas personas que no queremos que las vean, en el momento menos oportuno, pueden llegar a recibirlas.

Igualmente, hay que tener en cuenta que los contenidos puestos en la Red van a estar publicados durante mucho tiempo y, por lo tanto, un vídeo que hoy puede ser inocuo o incluso gracioso, dentro de un tiempo puede ponernos en una situación comprometida. Las propias plataformas recomiendan que en el caso de querer subir un vídeo con imágenes de carácter personal es mejor hacerlo privado. De esta forma sólo van a poder acceder a él las personas a las cuales el usuario invite a verlo.

El usuario es el único responsable de su comportamiento en la página. El prestador de servicios sólo es responsable desde el momento en el que recibe un aviso o notificación de la violación de sus normas de uso o la normativa vigente y no actúa al efecto.

En la "Política de privacidad" y en las "Condiciones de uso" de las páginas Web de estos servicios se especifican los derechos y deberes del usuario. Sin embargo, en la práctica, es normal encontrar usuarios que desconocen su responsabilidad. En el momento del registro muchos internautas aceptan directamente esas condiciones sin leer ni informarse de su contenido.

La Agencia Española de Protección de Datos ha sancionado en numerosas ocasiones a usuarios que han subido en plataformas de este tipo videos en los que terceras personas aparecían sin haber expresado el consentimiento para la utilización de su imagen con dicho fin. Por tanto, es preciso recordar que los usuarios pueden ostentar una doble cualidad, en unas ocasiones como víctima y en otras como infractor, de lo que se deriva el especial celo y rigor que hay que tener cuando se suban contenidos al entorno Web 2.0..

b) El uso de la Webcam.

Hoy día el uso de plataformas basadas en la transmisión de imágenes en tiempo real captadas a través de Webcam ha aumentado exponencialmente (por ejemplo la aplicación Skype). Asimismo, las redes sociales y plataformas colaborativas incluyen entre sus servicios la comunicación a través de videoconferencia. Es por lo que debe recordarse la importancia de un correcto uso de la Webcam en el entorno del Web 2.0.

Es recomendable restringir el uso de la Webcam a los menores para que no la puedan utilizar sin el permiso de los padres. La persona que nos ve, además del rostro, puede observar la edad aproximada, el estado de ánimo, el lenguaje corporal y muchos datos sobre nuestra forma de vida, la ropa, cómo es la casa, si hay otras personas cerca,... La información es muy detallada y se puede analizar bien.

Las situaciones de riesgo que pueden comprometer la privacidad del usuario pueden concretarse en las siguientes:

- **La Webcam puede dar de forma accidental información** que no se pretendía mostrar. Por ejemplo, que alguien a quien no se pretendía enseñar pase por detrás de la cámara.
- **Se puede grabar la escena** que se ve en la cámara y por lo tanto, cualquiera podría llegar a verlo.

- **Las imágenes se pueden trucar**. Esto quiere decir que si el objetivo de activar una cámara Web es conocer la identidad de la otra persona, puede que nos engañen con alguna grabación para hacernos pensar que es alguien que no es en realidad.
- A veces se hacen cosas irresponsables e imprudentes delante de una Webcam en un momento de excitación o euforia que, de manera reflexiva, jamás se harían.
- **Puede existir el riesgo de ser objeto de bromas y engaños en los chats** con cámara, que después pueden ser grabados y publicados en Internet.
- La Webcam es el medio más utilizado para llevar a cabo los chantajes, las extorsiones y el acoso sexual: *grooming*, *sexting*,…

c) Plataformas para publicar e intercambiar fotografías.

Entre los servicios de la Web 2.0 relacionados con las imágenes, destacan plataformas diseñadas para compartir imágenes por parte de los usuarios (por ejemplo, Flickr, Instagram, Picasa, etc.,..) que van desde servicios online hasta software que se descarga e instala en el dispositivo del usuario permitiendo la organización de la información en formato de imagen, ya sea a través de álbumes, mediante tags, colecciones, etc.

Es importante destacar la posibilidad de añadir metadatos a las imágenes en estas aplicaciones, por ejemplo, se pueden añadir mapas (geolocalización) y comentarios a las imágenes publicadas, lo que va a permitir extraer información adicional más allá de la propia fotografía.

Muchas de estas plataformas pueden considerarse como verdaderas redes sociales debido a la estructura de la participación del usuario y otras son directamente vinculables a dichas redes. Incluso al registrarse en estas plataformas, o descargar el software necesario para su uso, puedes otorgarles permisos para la utilización de la Webcam con la finalidad de actualizar datos del usuario, identificación, etc.

Por eso hay que tener muy presente los riesgos para la privacidad que conlleva la "**correlación entre servicios Web**", que los prestadores de servicios ofrecen, cuando puedan modificar la política de privacidad que inicialmente el usuario aceptó de forma individual para cada servicio.

d) Servicios de reconocimiento facial en servicios de la Web 2.0 y en dispositivos móviles.

La disponibilidad y precisión de la tecnología de reconocimiento facial ha sido integrada en los servicios en línea y móviles para la identificación, autentificación/verificación o la categorización de las personas. Entre los servicios en línea y móviles que la utilizan se encuentran las redes sociales y los fabricantes de teléfonos inteligentes o smartphones.

Se considera que el reconocimiento facial está incluido en el ámbito de la biometría y que en muchos casos contiene los detalles suficientes para identificar a una persona de manera inequívoca.

El reconocimiento facial es el tratamiento automático de imágenes digitales que contienen las caras de las personas con fines de identificación, autenticación o categorización de dichas personas. Está compuesto por una serie de subprocesos diferenciados como la obtención de la imagen, la detección de la cara, la normalización, la extracción de características, el registro y la comparación.

Los riesgos para la intimidad de las personas que pueden plantear los sistemas de reconocimiento facial dependen del tipo de tratamiento y de los objetivos de que se trate. No obstante, existen riesgos que tienen mayor relevancia en fases concretas del reconocimiento facial.

La privacidad del usuario puede verse comprometida dependiendo de la ubicación de las plataformas implicadas en cada fase del reconocimiento facial. Puede suceder que cada actor implicado en las distintas fases (obtención, detección, extracción de características, registro y comparación) tenga que realizar una comunicación de datos para pasar a la siguiente fase, con el riesgo que puede conllevar dicha comunicación a través de la red. Es muy importante que a través de las políticas de privacidad del servicio de reconocimiento facial se informe del destino, almacenamiento, plataformas implicadas y medidas de seguridad empleadas.

También puede suceder que un usuario haya optado por el reconocimiento facial como medida de identificación y acceso a una plataforma determinada, pero que no quiera que su imagen se asocie a su perfil en dicha plataforma, por lo que deberá conocer previamente a dicha elección, el tratamiento concreto y la finalidad de su imagen en dicha red social.

Asimismo, cuando ocurren fallos de seguridad o uso malintencionado de información de la imagen digital, por parte de terceros, pueden darse situaciones incómodas para aquellos usuarios que inicialmente optaron por el sistema de reconocimiento facial y que observan como su imagen es utilizada en el entorno del Web 2.0 para finalidades que no consintieron inicialmente.

e) El etiquetado de imágenes por terceros.

Cada vez es más frecuente en los servicios de la Web 2.0 la posibilidad de utilizar tecnologías de etiquetado que permiten añadir metadatos a dichas imágenes. **El etiquetado de imágenes permite añadir comentarios y otros datos a imágenes y vídeos subidos a la red**.

Tradicionalmente la vulneración de la privacidad suponía la salida inconsentida de información de la esfera intima de la persona, con el etiquetado de imágenes se produce el proceso inverso: son terceras personas las que añaden valoraciones subjetivas a la esfera privada de la persona, alterando y modificando su identidad, pues dichos atributos se relacionarán con un usuario determinado con independencia de la aceptación de éste.

Los riesgos del etiquetado de imágenes para la reputación de la persona ocurren cuando, por ejemplo, el uso de los buscadores puede implicar que las imágenes etiquetadas traspasen el círculo de contactos autorizados, llegando a disposición de terceros, que pueden utilizarlas de forma inadecuada. Sirva a modo de ejemplo la siguiente situación: *Susana ha sido etiquetada junto a más gente en una foto de la fiesta de su facultad. La foto aparece en un post con el título "Botellón en la facultad". Susana acude a una entrevista de trabajo y el entrevistador le confiesa que ha visto esa foto al buscar más detalles sobre su formación académica, lo que le supone un gran bochorno y la pérdida de una oportunidad de trabajo. Susana quiere que la des-etiqueten de la foto.*

2. CONSEJOS.

- **Leer atentamente las políticas de privacidad de los servicios del entorno Web 2.0.** Es muy importante saber qué datos son necesarios para la utilización de un determinado servicio, quién los va a tratar, para qué y hasta cuándo van a ser tratados. En caso de duda respecto del tratamiento que se vaya a dar a nuestros datos, valorar la posibilidad de no utilizar dichos servicios.
- Al utilizar servicios que impliquen la descarga de software en el dispositivo del usuario, **analizar detalladamente los permisos que se otorgan para modificar o acceder al contenido del dispositivo**. En caso de duda, valorar la posibilidad de no instalar el programa o aplicación sugerida.
- Evitar el envío de imágenes o videos a usuarios en los que no se confía si un desconocido nos solicita vídeo o foto, o encender la Webcam.
- Utilizar Webcam con indicadores que permitan saber si se está grabando o no.
- Respecto de la Webcam, **usarla sólo con personas de máxima confianza** y no hacer delante de ella nada que no se haría en público.

- **Enfocar la Webcam a un ángulo muerto cuando no se esté usando**, evitaremos que, por descuido o error, se active y se transmitan imágenes que no se desea. Si viene integrada en el equipo portátil, basta taparla con cinta adhesiva o similar.
- Mantener actualizado permanentemente el antivirus y cortafuegos para evitar su activación desde el exterior. No permitir el uso de una Webcam en un equipo donde no estén activado antivirus y cortafuegos.
- Si se pretende conocer la identidad del interlocutor y se intercambia con él la imagen de la Webcam por unos instantes, es recomendable pedir en esos momentos que realice alguna acción particular (por ejemplo, tocarse una oreja) para poder comprobar que no está mostrando una grabación.
- **Pedir permiso a las personas que vayan a salir en una foto** para poder subirlas a la red. Igualmente, pedir permiso antes de etiquetar fotografías subidas por otras personas.
- Si tienes permiso para publicar fotos **no incluyas otros datos personales como nombre, dirección, teléfono, etc.** También se ha de **ser respetuoso** con los comentarios que se añadan a las imágenes a través del etiquetado.
- Si descubres una foto comprometedora tuya en el perfil de otra persona **ponte en contacto con el administrador del sitio Web** si consideras que el contenido no es adecuado.
- **No es aconsejable publicar fotos atrevidas porque nunca se sabe dónde pueden ir a parar**. La foto puede estar en la Red para siempre. No publiques imágenes que realmente no estés dispuesto a que llegue a verlas todo el mundo, ni tampoco cuando no estés dispuesto a que circulen para siempre por Internet. Ambas cosas pueden suceder con cualquier foto que subas a la Red.
- El uso irresponsable de las imágenes en Internet puede dar lugar a situaciones desagradables cuando terceras personas las utilizan malintencionadamente, pudiendo llegar a situaciones de riesgo (*ciberbullying, grooming, sexting,…*).

3. PARA SABER MÁS.

› Cuidado con la webcam. Pantallas Amigas

www.cuidadoconlawebcam.com

› Cinco consejos básicos para un uso seguro de la webcam. Pantallas Amigas

www.pantallasamigas.net/proteccion-infancia-consejos-articulos/cinco-consejos-basicos-para-un-uso-seguro-de-la-webcam.shtm

III. ACTIVIDADES

1. ETIQUETADO.

El profesor podrá leer el siguiente supuesto:

Ana ha sido etiquetada, añadiendo su nombre en una foto sin su permiso. Esta foto se hizo en una fiesta a la que acudió con algunos amigos. En dicha foto sale disfrazada, muy alegre y con un vaso en la mano. Además, en esta foto se han puesto algunos comentarios, y entre ellos:

"¡¡¡ Vaya pintas que llevabas!!!".

Ana ha acudido a una entrevista de trabajo y su entrevistador le confiesa que ha accedido a esta fotografía. Ana siente mucha vergüenza.

1. ¿Creéis que el hecho de que el entrevistador haya visto la foto de Ana influyó en que no la contrataran?

2. Ana quiere que quiten la etiqueta de la foto. ¿Cómo puede hacerlo?

3. ¿Qué puede hacer para evitar que la etiqueten la próxima vez?.

2. USO DE LA WEBCAM

El profesor propone formar grupos de 4 ó 5 alumnos:

El uso de la webcam ha traído grandes ventajas como poder hablar y ver a amigos o familiares que se encuentran lejos y que de otra manera únicamente podríamos escuchar su voz. Sin embargo, también ha traído más de un disgusto a muchos. Cuando mantenemos una conversación a través de la webcam, nos pueden estar grabando al mismo tiempo, e incluso puede ser que estemos hablando con una grabación sin que lo sepamos. Por ello, se invitará a los alumnos a que inventen una pequeña historia para concienciar a los demás del problema que puede tener asociado un mal uso de la webcam e intercambio de información con terceros sin estar seguros de su identidad.

Más tarde se podrán leer y comentar entre todos.